# 第１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６月３日（水）　１０：００～１２：００

２．場所　経済産業省別館１階　１０１－２会議室

３．出席者（敬称略）

構成員：松本勉（座長）、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、森安隆、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１　「CRYPTREC の在り方に関する検討グループ」開催要綱（案）

資料２　CRYPTREC に関する現状について

参考資料１　暗号技術検討会における小グループの設置について

参考資料２　CRYPTREC の在り方に関する検討グループ　構成員・オブザーバ名簿

５．議事概要

１　開会

事務局から開会の宣言があり、構成員の欠席（上原構成員）の報告があった。

２　議事

（１）「CRYPTEC の在り方に関する検討グループ」開催要綱について

資料１に基づき、事務局より説明が行われた。質疑はなし。原案どおり承認された。

続いて、構成員の互選により松本勉構成員が座長に選出され、ご挨拶があった。

（２）CRYPTEC に関する現状について

資料２に基づき、事務局より説明が行われた。続いて行った自由討論の内容は以下のとおり。

○自由討論

奥山オブザーバ：マイナンバー等、政府として重要なシステムの構築がこれから行われるところ、暗号技術について考え方を整理し、示すことができる場は CRYPTREC しかないのではないかと考えている。また、近年量子計算機などの新しい技術の研究が進んでおり、現行暗号が効力を失うことも想定されるが、その際の移行をどうすればよいか不安がある。ぜひ構成員の方々の知見をいただきたい。

近澤構成員：「政府機関の情報セキュリティ対策のための統一基準」（以下「統一基準」

という。）では、使用可能な場合には「電子政府推奨暗号リスト」に掲載された暗号技術を使用することとなっているが、リストに掲載されていない暗号が使用される場合もあると考えてよいか。

奥山オブザーバ：知っている限り無い。

松本座長：安全なシステムを構築するためには、適切に実装されていることが重要。統一基準では、暗号プロトコル等について具体的な基準はないと考えてよいか。

奥山オブザーバ：一般論としての記載はあるが、具体的な基準はない。

松本座長：昨年度 CRYPTREC が作成した「SSL/TLS 暗号設定ガイドライン」のような文書は、NISC から見て有用だと思うか。

森安オブザーバ：有用だと思う。

松本座長：CRYPTREC として政府システムの安全性向上に貢献できたらと考えているが、NISC としてどのような成果物があると望ましいと考えるか。

奥山オブザーバ：提案できるほど暗号技術に関する知見がないので、ぜひ CRYPTREC から提案してもらいたい。

松本座長：CRYPTREC と NISC が今後も継続的にコミュニケーションを取っていく枠組みが必要。属人的なつながりに依存するのではなく、長く続く仕組みを作りたい。

奥山オブザーバ：そのとおり。CRYPTREC 事務局（総務省、経済産業省、NICT、IPA）の４者は NISC と密に連携を取っており、その関係性を活用してほしい。

手塚構成員：政府システムを構築するにあたり、必要な要素の全体像を明確化し、どこまでが CRYPTREC の担当範囲で、それ以外の範囲を誰が担当するのかといった、俯瞰的な立場に立った議論が必要。現状では、暗号技術のうち、どの部分について基準がないためにベンダ依存になっているのかといったことが分からない。また、NISC には政府システム全般のリスト化、現状把握を行っていただきたい。どのような暗号技術を使用しているのか把握しておくことは、危殆化などの問題が生じた際に大変重要。政府内にシステムに熟知した人材が乏しくベンダへの依存度が高いが、安全なシステムを構築するために、基準や使用するべき規格などを定めることが必要。

松本座長：何についてどの程度基準を決めるべきか、という点は使う側と技術を提供する側で意見が異なっている。CRYPTREC として統一基準にどのようなインプットを行うか、本検討グループにおける重要な論点。また、CRYPTREC の範囲をどの程度広げるかという論点もある。

松本泰構成員：２点ある。１点目は、統一基準に関して、米国においてよく見受けられるデータセキュリティに基づく分類が議論の参考になるということ。移動中のデータ、保管中のデータ、利用中のデータ、消去されたデータの４つの状態に基づき分類され、どういった技術・文書があり、何が不足しているか分かり易い。２点目は、暗号研究の出口戦略が不明確であること。暗号がセキュリティのための技術であるというイメージが強いが、トラストのための技術としての意味合いの方が重要である。今後の IoT

社会においてイノベーションを起こすための技術として暗号技術を位置づけ、暗号技術の出口を考え直すべき。

松本座長：暗号研究に関して、CRYPTREC としてどのようにコミットしていけば良いか。

松本泰構成員：暗号政策全体の観点になるが、日本に足りないものは米国の NIST に相当する組織。基礎研究と実社会を結び付ける NIST のような組織がないため、暗号技術の社会への還元が不足している。CRYPTREC が NIST 相当の機能を担うべきかという点には様々な意見があると思うが、NIST 相当の機能の必要性は広く認められているところ。

太田構成員：信頼性の高いシステムを構築するという観点では、電子政府のみならず、例えば医療系システム等の重要なシステムも適用先としてアプローチできないか。医療系システムであれば厚生労働省の所管であるが、NISC ではこのような分野にもアプローチしているのか。

大川オブザーバ：医療分野は重要インフラの１分野であり、NISC として安全基準等の策定指針を示したりしているが、NISC が政府統一基準への遵守を求められるのは政府機関のシステムまでである。セキュリティに限らず医療分野を含む各業界のルールは各所管省庁等で作っており、セキュリティだけを切り出して NISC が各業界を直接担当するという形にはなっていない。

松本座長：その点、米国の NIST は連邦情報セキュリティマネジメント法による位置づけがあり、豊富な標準規格を用意することで、各業界、世界各国から参照されている。日本でもかなり参照されているが、日本が自ら規格を定めることも必要。広く使われるような魅力ある成果物を作る必要がある。

事務局（経済産業省）：経済産業省では「IT 製品の調達におけるセキュリティ要件リスト」を作成している。現在は世界で標準的な基準に基づいて審査を行っているが、将来的に日本から基準そのものを発信していきたい。

事務局（経済産業省）：情報セキュリティ全体における暗号の位置づけを明確化し、さらに政府における役割分担も明確化するべきだと思う。法律上の所掌では、NISC が総合調整機能を果たし、総務省及び経済産業省が、暗号に関する取組を提案していく形だと思われる。

手塚構成員：CRYPTREC の活動を考えるうえで、技術と実装を分けて考えることが必要。従来の CRYPTREC は暗号技術の評価・監視など技術的な観点からの取組が中心であった。製品やシステムといった実装のレベルとは異なる段階である。技術から実装まで全体の流れを俯瞰し、それぞれの範囲をどの組織が担当するか、整理することが重要。その点、JCMVP 等も連携先として十分考えられるのではないか。

松本座長：技術に関する取組には必要な人的リソースの確保が CRYPTREC の重要な課題の１つ。とはいえ、人的リソース等の体制面での議論はひとまず置いておき、CRYPTREC としてやるべきことについて、最初に議論したい。現時点での CRYPTREC の取組は、

暗号技術の一部の側面しか対象となっていない。何が必要で何を作るべきか、改めて検討するべき。今日、実装やプロトコルレベルでの脆弱性への対処が重要な課題。また、CRYPTREC が電子政府や電子政府以外の領域でどのように貢献できるかも論点の１つ。

盛合構成員：CRYPTREC はこれまで、提案者から評価の申し出があった技術について評価し、結果を公表してきた。政府に近い立場である CRYPTREC が、勝手に個別の実装に対して問題点を指摘することになるというのがこれまでと異なる点である。また、現状の国内の脆弱性関連情報の届出の体制は、暗号技術に関する脆弱性等の情報に対応していない。さらに、現状の CRYPTREC の人的リソースは限られているので、より製品に近い部分については、既存の団体との連携を強化することが必要。

松本座長：ユーザ側の立場から判断する内容を示すだけなので、特段問題ないのではないか。

盛合構成員：製品レベルで推奨・非推奨といった評価を行う場合、全ての製品を評価対象とすることは出来ないので、限られたリソースに基づき調査をするとやはり不公平感が生じてしまい、中立性の担保が難しいのではないか。

手塚構成員：ご意見もっともだが、解決方法もある。例えば、基準となるガイドラインを作り、その基準に従って評価する制度を作るという方法が考えられる。

事務局（経済産業省）：懸念点はあっても、必要なことであれば解決策を探るべき。

松本座長：人材リソースに関する論点は重要だが、CRYPTREC のミッションに関する議論の後に議論したい。

近澤構成員：暗号技術に関して脆弱性などの問題が明るみになった際、CRYPTREC のホームページにその問題に関する見解等が記載されていると、活動の存在意義が高まって良いのではないか。IPA は電子政府に限らず全ての領域を対象としており、全ての領域を対象とすることの重要性は認識しているが、CRYPTREC で扱うべきかという点は議論が必要。また、ISO/IEC JTC1 で標準化活動にも関わっているが、利用者に近いテーマの規格文書やガイドラインでないとあまり読んでもらえないという実感がある。

松本座長：ホームページを通じた情報発信はぜひやっていきたい。情報の早さではマスコミ等のサイトに敵わないが、信頼性のある情報を素早く出すことに意義がある。ユーザに活用してもらえる情報を出すためには、リソースを考慮しつつ、どの分野で何を出すがという点が重要。

３　閉会

事務局から、次回会合の詳細については別途連絡する旨の説明が行われた。

以上