第２回　重点課題検討タスクフォース　議事概要

１．日時　平成27年12月21日（月）　19:00～21:00

２．場所　経済産業省　本館１階　共用西会議室

３．出席者（敬称略）

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

事務局：総務省（中西悦子、筒井邦弘、丸橋弘人、今野孝紀）、経済産業省（瓜生和久、上坪健治、中野辰実、中村博美）、情報通信研究機構（大久保美也子）、情報処理推進機構（神田雅透）

４．配付資料

（資料番号）	（資 料 名）
資料１	第１回重点課題検討タスクフォース議事概要（案）
資料２	CRYPTREC 暗号技術活用委員会の今後の活動に向けて
資料３－１	暗号アルゴリズムの脆弱性に関する情報伝達フローについて
３－２	暗号アルゴリズムの脆弱性に関する情報伝達フロー（案）
資料４	暗号プロトコルのセキュリティ確保に向けた活動
参考資料１	「CRYPTREC の在り方に関する検討グループ」における議論結果報告書（2015 年度第１回暗号技術検討会 資料２）
参考資料２	急激な安全性の低下における CRYPTREC の対応について（2011 年度第１回暗号技術検討会　資料２　別紙１）

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

タスクフォースの名称について、前回会合の配付資料に一部誤記があったところ、「重点

課題検討タスクフォース」である旨、事務局より伝えられた。また、資料のミス等の修正について、説明があった。前回欠席だった菊池構成員より挨拶があった。

前回会合の議事録について、確認が行われた。その後、資料の説明が行われた。

（１）暗号技術活用委員会の今後の活動に向けて

資料２の前半部に基づき、事務局より説明が行われ、暗号技術活用委員会の活動内容案が承認された。主な質疑応答は以下のとおり。

○松本座長　　今年度の暗号技術活用委員会は一度開催し、来年度につなげるという形になると思うが、活動内容について意見はあるか？

○近澤構成員　　今年度の審議内容として、暗号技術活用委員会の活動ポリシーと、運用ガイドラインのメンテナンス体制検討の２点挙がっているが、２つ目にある運用ガイドラインのメンテナンスの検討を１回で終わらせることは可能なのか？

○事務局（IPA）　１回で決めることはできないと考える。とりあえず考え方の整理について意見をもらい、扱うか扱わないか判断をし、扱うとなれば来年度早々にＷＧを作ることになる。また、実機での製品設定調査などに関しては、次回から業界団体やＪＮＳＡのような団体に任せるやり方を検討せよ、という判断になった。

○盛合構成員　　例えばAppendixにその製品についての調査結果を載せたとして、それを更新することはできないということか？

○事務局（IPA）　　更新できないというより、更新対象から外す、もしくは切り離して別のドキュメントにする等の対応をとることになる。

引き続き資料２の後半部について事務局より説明が行われた。主な質疑応答は以下のとおり。

○松本（泰）構成員　　米国では政府調達のためのFIPSは当然として、SP800シリーズもNISTが自主的に作成しているというよりは、FISMAのような法的な要求から作りなさいという命令の下で作成しているものが多い。日本でのCRYPTRECが作成する文書にはそういう強制力のある構造はなく、調達で使いやすい文書や強制力のある文書にはなっていないと認識している。

○上原構成員　　他にないという理由で、他機関が作った文書が参照されることはある。

○満塩構成員　　統一基準に関わっているのは政府機関のみであり、統一基準を具体化

したものはあるが、それはあくまでもNISCが手順書化したもので、SP800と比べてベンダもきちんと関与しているというレベルのものがない。

○松本座長　　体系化が進んでいないということがはっきりした。できるところからか、必要なところからか、どちらから対応していけば良いかについて意見はあるか？

○手塚構成員　　両面だと思う。体系をきっちり考えなければいけないのは当然として、喫緊で必要とされる例として、マイナポータルへアクセスする個人番号カードの認証方法のプロトコルが非常に気になっている。今後、個人番号は携帯電話や、リモコン等でも使われるというように、かなりデバイスに広がりをもたせようとしている。そのときのプロトコルが統一されており、CRYPTRECで行うか、もしくはCELLOSのような民間で行うのか、やり方はいくつかあるとしても、その安全評価が行われているべき。理想論としてはJISなどの標準化などで決定されているべきだが、体系の中で重要な部分を順々に埋めていく作業をしていくしかない。

○上原構成員　　政府調達を含め、非機能要件にセキュリティ要件を書きなさいといわれたときに、参照すべきものが全くないという状況が指示書を書く立場の人にとって一番困ることであるため、歯抜けでも良いので、とりあえずリストを作ることが大切である。

○松本座長　　ある種、網羅的な枠組みだけは少なくとも整備するということか？

○上原構成員　　ここは参照されている、ここは参照されていないということがわかれば作業もやりやすくなる。

○松本座長　　大変な作業になることが予想されるが、まずは全体的な体系をつくり、その中で優先順位を決めて作業していくことになる。

○事務局（総務省）　　あくまでもCRYPTRECが行うのは暗号に根差したものという理解で良いか？

○上原構成員　　セキュリティに関しては、暗号に絡んだプラクティスがたくさんあるはずで、それを含んだところはできるだけ網羅したい。

○手塚構成員　　CRYPTRECが取り組むべき範囲を、どこまで、どのように広げていくかという議論と関係しており、非常に重要である。また、どのようなフレームワークでどのような組織構成になるかも考えなければいけない。

○松本座長　　ある程度議論ができるメンバーがそろっているという点では、ここは非常に有力な組織である。セキュリティ全般を考慮しつつ対応する必要があるが、まず

は我々ができるところから動かしていくのが良い。

（２）暗号アルゴリズムの脆弱性に関する情報伝達フローについて

資料３－１，３－２に基づいて、事務局より説明が行われた。主な質疑応答は以下のとおり。

○松本（泰）構成員　　暗号アルゴリズムの脆弱性に対して本当に緊急な対応が必要なものがあるのか疑問がある。実際、暗号アルゴリズムの移行には非常に時間がかかる。例えば、SHA-1であってもNISTにおいて署名以外は使えるとしており、また代替する手だても少ない。現状、暗号技術に関する緊急な対応が必要なものの多くは、暗号プロトコルの脆弱性の話し等であり暗号アルゴリズム自身ではない。暗号アルゴリズムの脆弱性化の多くは、本当の意味での緊急性を要しているわけではない。

○松本座長　　例えばこの前、MISTYに対して今まで知られていない攻撃方法があるということが出てきた。そういう様々な情報に対してどう考えれば良いのかということを、混乱を避ける為に、CRYPTRECからきちんとした情報を発信できるようにはすべきである。

○満塩構成員　　速報や安全結果の事実関係だけを並べられても現場はかなり混乱する。どういうアクションかはケースバイケースだが、何らかのアクションを現場でどうとるべきかという情報を入れてほしい。

○松本座長　　直ちにセキュアでなくなることはないというようなことを書きたいが、具体的なアクションも伴うので書き方が難しい。

○松本（泰）構成員　　アルゴリズムの評価の話で、SHA-1が徐々に安全性が低下するといったときに、既存のSHA-1を使った署名文書をどうするのかという問題がある。今のところ、こうした観点でのCRYPTRECでの評価は行っていない。SHA-1の使用を止めなさいとは言っているが、いつまでその署名文書が安全かということに関しては何も言明していない。

○松本座長　　そういうことに対する技術的な検討はたくさんされているが、CRYPTRECではまだ対応ができていない。

○手塚構成員　　CRYPTRECでは、各所から上がってきた速報を踏まえてどうするかを検討することに意味があると思っている。あえて速報のところで競争する必要はなく、CRYPTRECが最終的にピン留めすることが重要。また、どこにどの暗号が使われているか

というデータベースを構築しなくてはならない。何か問題が起きたときに、政府システムに対して手を打てるのはCRYPTRECのみであり、暗号のデータベースをしっかり管理することで、CRYPTRECで扱うべき問題か、民間に任せるかの割振りも可能となる。

○上原構成員　　暗号プリミティブが突然危殆化するというのはほぼないので、余り心配する必要はないが、この活動はパニックを抑えるために必要。危殆化が進んだことが学術的にわかっているものに対して「大丈夫です」というのは責任論にもなりかねないため、政府機関はこう判断しましたといえる機関はここしかない。このため、速報を出して安全性を評価して必要な情報を整備することは良いものだと考える。

○手塚構成員　　米国やヨーロッパなどがこういうことをどのような伝達方法で、どこの組織が担当しているか参考にしたい。

○事務局（IPA）　　NISTは、FIPSの更新のタイミングで次回の更新はないと発表し、次回更新までに移行する対策を進めさせ､その後はレガシーのみの使用を認めるように、移行の期限を決めている。実際にDESのものは全数探索のアタックがあっても、移行の期限内ではほとんどのアプリケーションで大丈夫だとNISTは発表している。

○松本座長　　NISTは法律に基づいて活動を位置づけられているのでNISTの判断を明言できる仕組みになっているが、ここは検討会でしかないので、これから整備していくことである。

○菊池構成員　　NISTにはこういう評価委員会みたいなものはあるのか。

○事務局（IPA）　　あるかどうかはわからないが、リサーチチームは当然いる。

○菊池構成員　　CRYPTRECで速報を出すとしても、２～３日で暗号技術評価委員内の同意をとるのは難しいのではないか。ただCRYPTRECは年度ごとに報告書を出している。それで民間を含め多くの方々に信頼されているので、信頼できるリソースを速報という形で出さなくても、定期的に発信することで十分存在意義を増しているとは考えている。

○手塚構成員　　速報について、競争のような世界に入る必要はない。速報を出せるのが一番理想ではあるが、CRYPTRECの活動は世の中を安定させることにあり、常日ごろ様々な情報に対してCRYPTRECの名で対応する必要はないと考える。

○松本座長　　CRYPTREC内部に速報や安全性評価結果を出す等、公式ステートメントに相当するような重みのあるものを作成する作業が必要になるため、内部での作業はそもそも大変なものであると認識すべきである。民間でも非常に困っているわけなので、

公的なところがそれをやってくれれば、省力化にもなるのではないか？

○手塚構成員　　そのときには体制やクレジット等をしっかりと整理する必要がある。

○盛合構成員　　今の体制だと、暗号技術評価委員会が監視活動をしている。安全性に対してCRYPTRECのお墨付きの対象にそういう報道が出たときに、CRYPTRECとしてはこう考えるというのをなるべく早い時期に外に示すというのは、それを出している立場上必要なことだと考える。

○手塚構成員　　それに越したことはないが、体力的に大丈夫か？また、MISTYの速報は何日ぐらいで出せたのか？

○太田構成員　　私と盛合構成員で２週間ぐらいのうちに２回緊急的なアナウンスをつくった。２～３日を維持しようとすると常時戦時体制でないといけない。

○松本座長　　何のためにこういう活動をするのか、どのくらい人とお金と時間をかけてよいのか、というそもそものところにもつながる話である。

○菊池構成員　　盛合、太田をオーサーとして速報を出しては駄目なのか？

○太田構成員　　その作業をやっているときに、ここで大丈夫だと発表すること自体にどれぐらいの責任を負うのかということも含めて、非常に難しい話だと感じた。

○満塩構成員　　ぜひ今回のMISTYの件をケーススタディとして、どう回したかというのを比較すると現実的なリアリティな議論ができると考える。

（３）暗号プロトコルのセキュリティ確保に向けた活動

資料４に基づき、事務局より説明が行われた。主な質疑応答は以下のとおり。

○近澤構成員　　盛合構成員が紹介したNICTの安全性評価と、CELLOSでの活動はかぶらないのか？

○盛合構成員　　CELLOSの活動について詳しいわけではないが、CELLOSの中でも、プロトコルの安全性評価をZooの中でためていく作業はしている。ホームページに公開されているのはSSL/TLSのレベルのもので、こちらのCPVPの活動は、もう少し下のレベルになると考えている。住み分けは難しいが、CRYPTRECは電子政府向けと整理すれば、お互いにぶつからない。

○手塚構成員　　CRYPTRECは国がバックアップする組織なので、信頼度の高さが重要。それに対してCELLOSというのはもっと軽く、さっと動いて研究者魂でやれる世界、そういう研究者の思いが一番根底にあり、民間活動の中のone of themだと思っている。

○太田構成員　　モチベーションの高い人、属人的になってしまうと組織として永続性がない可能性もあるので、皆が幸せになるような仕掛けを作ることがポイントだと考える。また、お金がつくかわりに責任もある、というところをうまくコーディネートできればいいと考える。

○手塚構成員　　研究者と一緒にやっている各社も、どちらかというとボランティアで動いている。

○松本座長　　フォーマルメソッドを使って、厳密に計算機の力も借りてプロトコルのセキュリティを評価するという話と、SSLなどの現実に使われていて社会的にも影響度の大きいものについての速報を出すというのと、CELLOSは２つ活動している。

○近澤構成員　　万が一かぶっているのであれば、リソース的にもったいないので、切り分けたほうがいいと考える。

○太田構成員　　研究者魂でやっているので、切り分ける必要はないと考える。

○松本座長　　問題は、CRYPTRECがポータルになるという考え方だとすると、そこから仕事をお願いできる場合と、できない場合がある。気が向いたときだけやってもらうという緩い感じでの連携ももちろんあると思うが、相談したいときに頼りにしているので必ず反応してという約束があったほうが本来はいい。

○手塚構成員　　CRYPTRECは全てを対象にするのが理想だと考えるが、政府システムに責任を持つことが最も重要である。どういう政府システムで使われているか、どういう暗号や暗号プロトコルが使われているかわかっていれば、その範囲について対応しやすくなる。政府以外に対してもサポートすると相当大変になるため、CRYPTRECのメンバーだけでやれないところは民間の組織も活用するとなれば、いろいろなやり方はある。一方で、政府にないプロトコルまでサポートするには相当大変となる。

○松本座長　　例えばプロトコルといっても、世の中のいろいろな人が普通に使っているプロトコルが政府系のシステムの中にも入っている。CRYPTRECが十分な予算や人員などをもっていれば、別にCELLOSの力をかりなくても良い。しかし、CELLOSという非常にアクティブな方々がいるため、そこと連携できれば良いと考えている。

○手塚構成員　　CELLOSのメンバーには、CRYPTRECとしてピン止めの役割を担う場合だと速報を出しにくいというのを感じている人たちがいる。決して悪い意味ではなく、CRYPTRECというのは最終的に相当重要なところであるため、研究者として自由に発信するのとはわけが違う部分があるためである。

○松本座長　　つまり研究者が主体的に行動しているかについて違いがあり、CRYPTRECからのお願いに対し、必ずしも受ける体制にないということか？

○手塚構成員　　どちらかというとそうである。要は、明確に仕事として予算もつけてもらうとなれば研究者たちもやりたいが、企業ではそこに予算がついているわけではない。

○松本座長　　研究者群としてはCELLOSでアウトプットをしている方々がいるので、仕事が振れるのであれば、CRYPTRECに協力してくれるかもしれないという期待はある。もう１つは、脆弱性情報を早く見つけて解説をする活動について、それもお願いできるのか、あるいはCELLOSから発信されたものをCRYPTRECで判断する等、いろいろなチャネルがあると思うが、具体的にどういう方法をとることができるのか、具体的にしたい

○手塚構成員　　CELLOSも、もともと国家プロジェクトで動いていたので、予算があればきちっとアウトプットを出していた。それが延長できればそのままツール類もやれたが、今はボランティアになって活動している。

○太田構成員　　予算がつけばうまく回るということか？

○手塚構成員　　研究者たちは、そのツールをさらに良くしようというのは当然思っている。もしCRYPTRECと連携するならば、CELLOSで出す速報をうまく活用するなり、CRYPTREC側にパスを渡して、しっかりとやってもらうなりある。または、CRYPTRECのほうで見つけたものをCELLOSが速報で出し、CRYPTRECへ返して、CRYPTRECできちんとまとめて出すというような双方向の連携はあるのではないか。

○太田構成員　　予算をつけて、網羅性などの義務が入るとかなり難しいだろう。

○手塚構成員　　そこは本当に難しく、今の体制ではできないと思う。

○松本座長　　予想どおり、大変な議論ではあるが、先ほどのアルゴリズムの脆弱性情報のフローの話とプロトコルのセキュリティ評価、確保に向けてどうしていくかということについては、次回、第３回である程度のめどはつけたい。

３　閉会

次回第３回重点課題検討タスクフォースについて、平成28年２月３日（水）19:00～開催する旨の連絡があった。その後、閉会の宣言があった。

以上