第４回　重点課題検討タスクフォース　議事概要

１．日時　平成２９年２月２２日（水）　１５：００～１７：００

２．場所　経済産業省本館１階西共用会議室

３．出席者（敬称略）

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

事務局：総務省（酒井雅之、上東孝旭、今野孝紀）、経済産業省（師田晃彦、森川淳）、
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．配布資料

（資料番号）	（資 料 名）
資料１	CRYPTREC の今後の体制（案）について
資料２	文書番号体系（案）について
参考資料１	「重点課題検討タスクフォース」開催要綱
参考資料２	委員名簿

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）CRYPTREC の今後の体制(案) について

資料 1-1、1-2 に基づき、事務局より説明が行われ、重点課題検討タスクフォースのミッションを終了し、今後、暗号技術検討会やその下の両委員会にまたがる検討事項が出てきた場合には、適宜 4 者事務局打ち合わせで調整の上、必要に応じて暗号技術検討会やその下の両委員会に付議すること、および、暗号技術検討会を従来、年 2 回開催していたが、年 1 回の開催とし、他はメールベースの審議とすることについて基本合意され、来年度から運用されることとなった。

質疑応答は以下のとおり。

○松本(泰)構成員　昨年やっていたときに、課題 3 に挙がっていた「新たな社会ニーズを見据えた新規活動」は、前年度はやらず、今年度検討の予定となっていた。「新たな社会ニーズを見据えた新規活動」の中で CRYPTREC の体制や活動内容が少し変化するべきではないかなと思ったので、そこを議論してないのが少し残念である。

〇松本座長　変革期にあり、体制が整わなかった。そういった活動は必要であろうという認識については共有されていたが、具体的な検討・実施は資料 1-2 に示された体制で検討していくということである。

〇事務局(経産省) 今までは日本のサイバーセキュリティというのは、日本のサイバーセキュリティを高める、むしろ防衛力を高めるというところにかなり主眼を置いて取り組んできたが、今後は、むしろ産業競争力という観点に力を入れて取り組むべきである。セキュリティ産業を強めるというだけではなくて、産業にセキュリティをインボルブさせることでどう競争力を上げるかという観点が重要であると考えている。

〇盛合構成員　産業化ということで、CRYPTREC がこれまで全く何もやっていなかったかというとそうでは必ずしもなくて、例えば軽量暗号に関しては、4 年前からWGを設置して、さまざまな IoT の応用先に対して軽量暗号の果たし得る役割などの観点からガイドラインを作成し今年度末公開予定となっている。ガイドライン読者層としては、情報システム、あるいは IoT システムを設計する立場にある人など、必ずしも暗号の専門家ではない方などを想定している。

〇満塩構成員　暗号技術検討会の開催回数を減らすとのことだが、暗号技術評価委員会・暗号技術活用委員会については、従来通りの開催形態であるとの認識で合っているか。

〇松本(勉)座長　両委員会については、今までと基本的に同じような形で進めていくという認識である。

〇事務局(経産省)　事務局側の変革もあり、そのような変革に併せて暗号技術検討会の進め方についても効率化を図るというのが一つ目的としてある。検討会としてのアクティビティが低下しないということは原則である。

(2)文書番号体系について

資料 2 に基づき、事務局より説明が行われた。以下については合意され、暗号技術検討会にて審議されることとなった。また、付議資料については、本日の議論を踏まえ事務局が修正を行い、ML 上で委員が確認したものをあげることとなった。

・現行の CRYPTREC が公表している文書類は、全て CRYPTREC 文書と位置づける
・現在存在している文書だけが CRYPTREC 文書だとはしない
・今後 CRYPTREC 文書に含める文書は、暗号技術検討会、暗号技術評価委員会、暗号技術活用委員会で承認された文書とする
・暗号技術検討会、暗号技術評価委員会、暗号技術活用委員会の委員会配布資料は CRYPTREC 文書に含める
・暗号アルゴリズムの仕様書そのものは CRYPTREC 文書には含めない
・CRYPTREC 暗号リストと仕様書の対応関係表は CRYPTREC 文書に含める
・他の組織で作られた文書の参照関係などを示す文書は CRYPTREC 文書に含める

質疑応答は以下のとおり。

○手塚構成員　実際これをやっていくときに一番気になるのは他組織と組むというところで、何をもって他組織がこの CRYPTREC と組める相手か否かといった判断をどのように行うか、が今後大変重要になる。検討会で審議されるべき内容である。他組織が作ったものを CRYPTREC の名前を使って出すということをどのように考えていくか、これを運用していくときのルール化など、実施の運用に落とし込んでいくときにどうするかというところが非常に気になる。
○松本(勉)座長　「CRYPTREC 主導」の行の中で、「アウトソーシングで作成させた内容をベースに、CRYPTREC としての成果物を作成」とある行については、作業として従来 WG 等で実施していたものをどこかに発注するというようなことか。
○事務局（IPA）そうである。
○松本(勉)座長　それらの場合であっても、最終的には暗号技術評価委員会、暗号技術活用委員会で責任を持って出す、という認識で合っているか。
○事務局（IPA）　合っている。表に記されている全ての場合について、文書の内容については、暗号技術評価委員会、もしくは、暗号技術活用委員会で議論し、承認されたものに対して付議をする、という案である。

○松本(勉)座長　議論の仕方が複雑なので、まず、CRYPTREC 文書というものの中に何を入れるかということ、そのつくり方とアップデートの仕方について共通の認識をもちたい。 各アルゴリズムの仕様書自体は、番号を振る文書には含めないということでよろしいか。
○満塩構成員　仕様書そのものには番号が無くてもいいが、暗号アルゴリズムの名称と仕様書との対応表は、CRYPTREC 文書 として番号を付けた方がよい。
○松本(勉)座長　暗号アルゴリズムの名称と仕様書との対応表は必要であり、CRYPTREC 文書として、番号を付けた方がよい。その対応表は CRYPTREC 文書に位置づける、仕様書そのものは CRYPTREC 文書ではない、ということでよろしいか。
○全構成員　異議なし

○手塚構成員　対象文書は今後増えていくと考えている。
○松本(勉)座長　これしかない、と限定してしまうのはよくない。
○手塚構成員　今後増える文書に柔軟に対応できる文書体系にしておくべき。
○盛合構成員　3 ページの「CRYPTREC 文書に該当しない代表的な文書類」に書いてある外部評価レポートについては、おそらく、現在 CRYPTREC のホームページで参照できるドキュメントの中で一番数が多い。これらのレポートは、例えばリストの暗号技術の安全性の評価・実装性能評価などが含まれており、委員会で行われるリストへの掲載に関する、適切/不適切の審議の判断材料として用いられている。そのような位置づけの文書に番号を付与する必要はないか否か、ご意見頂きたい。また、外部評価レポートは、毎年、暗号技術評価委員会などで、評価・調査対象および、外部評価依頼先について委員会で審議し、承認を頂いた上で外部評価を実施し、

レポートを提出頂いている。そのように委員会で審議・承認された結果出来あがった文書に番号を付けなくてよいのか、という点についてご意見頂きたい。
〇松本(勉)座長　外部評価レポートについては、私も番号はつけたほうがいいと思う。

〇満塩構成員　CRYPTREC 文書にするか否かに対して、著作権の有無は判断基準にならない。今ここでもともと議論をしようとしているのは、外からみて参照するときの文書体系である。
〇松本(勉)座長　外部評価レポートは、我々が CRYPTREC 文書の 3 ページの上に書いてあるようなものをつくるに当たって素材にしただけであって、そのもの自体にはあまり責任はもっていない。そういう位置づけの違いは識別できるべき。
〇菊池構成員　外部評価レポートは、現在でも通し番号がある。これをそのまま活用してもかまわないのではないか。
〇満塩構成員　同感である。現在の番号を活かして番号付けすればよいのではないか。技術報告書というカテゴリとして扱えばよいのではない。
〇松本(勉)座長　技術報告書というカテゴリがあって、その中で発行順に番号をつけてしまえばいいのではないかということか。
〇満塩構成員　はい。それでどのレポートかは一意に特定できる。
〇松本(勉)座長　それは一案であると思う。委員会資料についても番号を付けた方がよい。
〇満塩構成員　委員会資料についても番号を付けて良いと思う。現在は、年度ごとに分かれているようなので、その番号体系を活かして、シリアル番号を付けるなどして一意に特定できるようにしておけばよいであろう。
〇松本(勉)座長　委員会報告書はそういうカテゴリがよいであろうということか。
〇満塩構成委員　はい。委員会報告書というカテゴリを作るのがよいと思う。
〇松本(勉)座長　これまでに議論を整理する。現行の CRYPTREC が公表している文書類は、全て CRYPTREC 文書と位置づける。また、今後の活動で現れる文書があるかもしれないので、今あるものだけが CRYPTREC 文書だとはしない、とする。

〇松本(勉)座長　8 ページで、「CRYPTREC 主導」と書いてある作成段階のところで 1 番、2 番、とあるが、1 番と 2 番は特に区別しなくてよいか。
〇盛合構成員　作成時に WG を立ててやる場合は 1 番、立てない場合が 2 番とあるので、違いはあるのではないか。6 ページでも、1 番のほうは、「CRYPTREC 内部で作る」ということで、2 番はそれ以外、「WG も設置しない」と書いてある点も、1 番と 2 番には違いがある。
〇松本(勉)座長　アウトソーシングをするという形態について、皆さんと共通のイメージを持ちたい。 WG を作ったとしても、委員会でそれを承認している。 作業をアウトソースし作っても、委員会で承認している。
〇松本(泰)構成員　CRYPTREC で一番重要なのは、やはり CRYPTREC 暗号リストであり、様々なところで参照され、更新されることが保証されていると考えられている。一方、WG 設置で

作った文書は、 WG 解散後、実際には更新できないという問題が根本的にある。しかし、今の CRYPTREC の暗号リストだけでは共通として参照される文書は少な過ぎると思っている。もっと幅広くなるべきだと思っている。例えば、個人情報保護ガイドラインの高度な暗号化については、暗号アルゴリズムは電子政府推奨暗号リストを参照するが、他の要件に関しては参照するべき文書がない。このような場合に参照できる文書を作れるところは、CRYPTREC しかないのではないか。

〇手塚構成員　その議論はもっともだと思う。 しかし、本日の審議から外れている。番号体系化については、ユーザーから見たときに、どのように見られる番号体系なのか、というところが今一番のポイントと思う。どんな作り方をしようと、 CRYPTREC としてこういうガイドラインを出しました、こういう体系で出しています、ということが外から見えることが重要な観点であって、それがどんな作られ方をしようとも、CRYPTREC でのクレジットであるということに基づいて番号体系は作るべきである。他組織の名前をもし、そこに入れていくとなれば、それは、非常によく考えなくてはいけない。CRYPTREC だけのクレジットでやるのだったら、それは CRYPTREC できちんと体系化を考えて出していけばいいと、そういう整理になる。

〇松本(勉)座長　まず、1 番と 2 番の区別をなくして議論したい。その他については、3 番と 4 番があるが、3 番は CRYPTREC と他組織との成果物だということか。

〇事務局 (IPA)　どこかの団体、コミュニティなどと一緒につくったものを想定している。

〇松本(勉)座長　4 番は、作る段階では何も関わっていない、ということか。

〇事務局 (IPA) そのとおり。他の組織で作られたものをみて、CRYPTREC に持ち込み、審議・承認したものに、クレジットを与えるというケースを意図している。

〇上原構成員　基本的には、CRYPTREC の名前で出すかどうかという観点が、番号をつけるか否かの一番重視すべき判断基準であって、出どころや誰が作ったか、というのとはちょっと違う話だと思う。他の組織で作成された文書を、ほとんどコピペしたような文書を CRYPTREC の名前で出すというのはなさそうな気がする。

〇松本(勉)座長　他の組織が作成した文書を参照する文書はあってもいいと思うが、その文書そのものを、表紙をつけて CRYPTREC 文書とするというのは、かなり慎重にやるべきである。

〇 菊池構成員　これを 3番、4番、C、D のあたりを拡大するという考えを事務局が提案したのは、例えば自動車業界とか、あるいは制御システム系など、これまで暗号やセキュリティの概念があまりなかったところで、なおかつ正しくガイドラインや系がつくれていない組織が多いのではないかという想定に対して、CRYPTREC から専門家としてある程度指針や助言をし、よりよいガイドラインを目指す意図があるものと推察した。 一方、スムーズに受け入れられないのではないかという懸念もあり、難しそうだという印象を持った。

〇手塚構成員　階層化してものを見るような仕掛けができているかというところだと思う。 その観点からも、この番号体系もそういう意味では非常に大事だと思う。

〇松本(勉)座長　2番はとりあえずなしにして、3番、4番というのがあるという前提で話をしたほう

がよい。また、「他組織が作成した文書をベースに作成」というのは、ベースに作成とあるので、そのままもってくるのとは違うという解釈になるのか。
○事務局（IPA）　極力少ない変更にとどめ、変更の必要がなければそのまま取り入れる。
○松本(勉)座長　　全く同じだったら、それはこちらで、その参照する文書に番号をつけているだけであって、その文書自体には番号をつけないのではないか。
○事務局(IPA)　はい。他の組織が作成した文書自体に番号を付けるわけではない。参照するインデックスとして番号を振ることを想定している。
○松本(勉)座長　　一枚表紙をつけるではなくて、表紙だけなのではないのか。
○事務局(IPA)　そうである。
○松本(勉)座長　　つまり、中身がなく、一枚だけで、これこれに関しては何とかという団体がつくったXという規格があり、これはこのように使ってもいいのではないか、とかいうことが書かれているという文章が CRYPTREC 文書としてある、というようなイメージである。
○満塩構成員　　今の話は重要。暗号アルゴリズムの仕様と参照先リストの関係と同様に、やはり構成を示す文書は必要なので、それを作るという発想。
○事務局(IPA)　インデックスを示した文書に付番をする。
○手塚構成員 その考え方は CRYPTREC が中心で全て暗号系は見ていることが前提である。そこにちゃんと CRYPTREC のクレジットを付けて、番号体系にはめるということをやるというのを想定しているのか。
○事務局(IPA)　はい。
○手塚構成員　　日本の場合、それをやってどうかというのは今後の課題の部分はあるけれども、そういうことをしたいということか。了解した。
○事務局(IPA)　CRYPTREC に来れば、必要なドキュメントなどが、他の組織で作成した文書も含め、探せるというスタイルを想定しているのが4番である。
○松本(勉)座長　　それをやるには相当精査が必要である。
○上原構成員　　文書の中身の精査が必要である。また、更新に関する情報がちゃんと CRYPTREC に情報が上がってくるような仕組みが必要になる。
○手塚構成員　　そこは完全にリエゾンを組む必要がある。 CRYPTREC で引き取るというのは難しい。 CRYPTREC 側でそれだけの体制をつくらなければいけなくなる。
○松本(勉)座長　4 番は、「他組織が作成した文章に対して参照関係を示す文書」か。
○手塚構成員　先ほどの，対応表のことか。
○満塩構成員　そのイメージだ。
○上原構成員　CRYPTREC 文書の定義を正確に表現することが難しい。 すごくざっくりした定義で、CRYPTREC において承認した文書ぐらいしかできない。
○松本(勉)座長　3 番目の他組織と共同で成果物作成といっているのは、自分たちは作っていることを想定しているか。
○事務局(IPA)　はい、一緒に作成することを想定している。

〇松本(勉)座長　つまり、共著ということか。
〇事務局(IPA)　はい。
〇松本(勉)座長　「アウトソーシングベースでのアップデート」というのと「自前でのアップデート」というのは、やり方の違いだけなのかと思われるので、これも C と D はマージでよろしいか。
〇手塚構成員　いいと思う。
〇松本(勉)座長　D は、他組織がつくった文書がどう変化していっているか、というのを常時把握しておく必要があるということか。
〇事務局(IPA)　はい。

〇松本(勉)座長　2 ページに戻って、冒頭につける文字列はどのような表記が適切か。CRYPTREC 文書というのだから、CRYPTREC とついていればわかりやすい。

〇松本(勉)座長　カテゴリ案について、審議する。
〇太田構成員　案 1 と案 2 の本質的な違いは、案 1 はエに相当するカテゴリが、案 2 では、コとサに分かれているということか。
〇事務局(IPA)　はい。
〇太田構成員　コ、サに分けた案 2 の理由は何か。
〇事務局(IPA)　案 1 は、比較的少ないカテゴリを意図し、案 2 は、現在のホームページの区別を踏襲したものとなっている。特に、技術ガイドラインには複数の文書が混在しているが、それでよいか否か議論頂きたい。
〇太田構成員　現状は、コとサに分かれているということか。
〇事務局(IPA)　はい。
〇太田構成員　レポートの内容は、外部評価者の責任において記述されているという意図である。そのレポートに対して、委員会で審議をして、委員会としての結論として年次報告書が作られている、というステップを踏んでいるので、委員会の活動として、入力(外部評価者のレポート) と、出力(年次報告書) が両方並べられることになるので、案 2 のほうがよい。
〇松本(勉)座長　コやサと外部評価レポートは別カテゴリにする必要はあるか。
〇松本(勉)座長　ガイドラインには複数の種類の文書があるが、いずれも推奨はしているのか。
〇事務局(IPA)　運用ガイドラインは、ベストプラクティスなやり方を示す文書を想定している。技術ガイドラインは、選ぶ際の技術的指針等が記されている文書を想定している。
〇盛合構成員　例えば、今、SHA-1 の暗号技術ガイドラインなどは、SHA-1 は基本的には移行を推奨するが、HMAC で使う場合は何年まで使えるなどの内容が記されている。
〇松本(勉)座長　ガイドラインは、判断する際に参照されるものなので、重みがある。異なる種類のガイドラインを同じカテゴリにしてよいか、それとも、 分けるべきか。
〇満塩構成員　ガイドラインというカテゴリだけでもいいような気もする。
〇松本(勉)座長　分解能が悪過ぎるのかどうなのか。

〇満塩構成員　ガイドライン全般にまとめてもいい気がする。また、システム運用の人たちからみると、運用という言葉から違うことを連想してしまう懸念もあるので、運用ガイドというよりは、普通にガイドラインまとめるのがよい。
〇松本(勉)座長　CRYPTREC リストは LS、レポートは RP 、注意喚起レポートは ER、ガイドラインは GL、技術ガイドラインは TR。
〇事務局(IPA)　TR に 調査 WG 作成文書と外部評価レポート文書が混在することになるが分けるべきか否か、分けるとした場合、いずれを TF にすべきか。
〇事務局（事務局）　暗号技術評価委員会の外部評価レポートは、調査を始める前に、暗号技術評価委員会で外部評価を実施するおよび具体的な評価依頼先について承認をいただき、提出レポートを改めて暗号技術評価委員会で審議し、承認されたレポートのみが公開されている。
〇松本(勉)座長　WG 報告書を TR とし、外部評価者レポート を EX とする。

〇事務局(IPA)　残っている議題として、カウントの付け方を議論頂きたい。特にガイドラインでは、GL100 番台、GL 200 番台は、種類が異なるという識別をできるようにするか否か。
〇松本(勉)座長　したほうがいいというご意見が多かったように思う。

〇松本(勉)座長　本日の議論を受けて、事務局が修正したファイルについては、一度私が確認するが、構成委員の皆様にもご確認頂きたいので、検討会に出す前に皆様にもう一回ご意見を伺うという最終確認のプロセスを設けることにさせていただく。

〇太田構成員　暗号技術評価委員会の委員長をしている立場として申し上げたいことがある。ER を作成するケースなど、緊急時に非常事態が生じたときにレポートを上げるというのが暗号技術評価委員会の仕事だと認識している。これは、非常事態が起きたとき、そのスキルをもった人に迅速に、的確に依頼が行えるか、どれほどの時間で緊急レポートとして、速報を出せるかということに対して、不確定要因があまりに多い。非常事態に備えて常にマンパワーを確保することは不可能であり、予測不可能である。非常に深刻な事態が発生した場合は、日本チームとしてはギブアップ状態になる可能性も含まれている。そういう責務を CRYPTREC の中で、暗号技術評価委員会が抱えているということは認識頂きたい。理想的には、何らかの意味で、有識者をプールできるような仕掛けをつくっておいて頂きたいと、個人的には思っている。
〇松本(勉)座長　非常に重要な、重たい課題である。すぐには、解決できないが、必ず検討会でも入れておきたい。

3 閉会

松本(勉)座長から閉会の宣言があり、予定していた審議事項がすべて終了した旨が告げられた。

以上