第１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１１月２０日（金）　１８：００～２０：００

２．場所　経済産業省別館３階３０１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、満塩尚史、盛合志帆

オブザーバ：NISC（奥山剛、久保山拓）

事務局：総務省（大森一顕、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．配布資料

（資料番号）	（資 料 名）
資料１	「重点課題検討タスクフォース」開催要綱（案）
資料２	重点課題検討タスクフォースの設置について
資料３	ハッシュ関数 SHA-2,SHA-3 の取扱いについて
資料４	CRYPTREC 活動方針についての論点 ～活用委員会の活動ポリシーの見直し～
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について（2015 年度第１回暗号技術検討会 資料２）
参考資料２	重点課題検討タスクフォース　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、参考資料２に基づき、構成員の紹介が行われた。新しく構成員に加わった満塩構成員より挨拶があった。

２　議事

（１）「重点課題検討タスクフォース」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。質疑応答は以下のとおり。議論内容を反映させたものを後日事務局より構成員にメールにて展開することとなった。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、挨拶があった。

〇質疑応答

松本(泰)構成員：開催の趣旨・目的で「今後の情報システム全体のセキュリティ基盤」とある。「情報システム」に対しては「情報セキュリティ」という言葉が対応しているが、現在は「セキュリティ」というと「情報セキュリティ」よりも「サイバーセキュリティ」を指すことが多く、多少のニュアンスの違いがあると思うので「情報システム」の代わりに「サイバー空間全体」と変更してはどうか。

松本座長：もう少し広く「情報社会」としてはどうか。

満塩構成員：目的は広く読めた方がよいと思うので、「情報社会」への変更に賛同する。

松本(泰)構成員：「情報システム」よりいいと思う。

事務局（総務省）：ご指摘を踏まえ、開催の趣旨・目的にある「今後の情報システム全体のセキュリティ基盤」を「今後の情報社会全体のセキュリティ基盤」に修正する。

（２）重点課題検討タスクフォースの設置について

資料２に基づき、事務局より説明が行われた。質疑応答は以下のとおり。本年度及び来年度の主な議題案と本年度のスケジュール案は承認された。資料２で用いている用語についてコメントがあり、事務局にて修正の上、後日構成員にメールにて展開することとなった。

〇質疑応答

満塩構成員：資料２の５ページの「③来年度以降の議論方針等」のような、広い視野にたった活動の議論はどのタイミングで行うことを想定しているのか。

松本座長：できるところをまず固めることから始める。今年度に関しては、第１回に暗号技術活用委員会がどういう仕事をすべきかの議論をまず行い、SHA-3 の取扱いについても早く議論したいと考えている。現状検討が必要な課題は５ページ①～⑥。①と②にある情報発信方法及び暗号プロトコルセキュリティ確保に向けた活動については、検討を急ぐものであるので第２回に議論したい。さらに広い視野にたった活動である③については、第２回で結論づけることは難しく、第３回での議論となってしまうことも想定している。

事務局（経産省）：①、②は在り方検討グループでも議論があり、新たに対象としたもの。広い視点で議論いただきたい。⓪は基礎的なもの、その他は直近の課題であることを補足する。

（３）ハッシュ関数 SHA-2,SHA-3 の取扱いについて

資料３に基づき、事務局より説明が行われた。意見交換内容は以下のとおり。資料３の課題が古い内容であったことにコメントがあり、事務局にて修正の上、後日構成員にメールにて展開することとなった。

〇意見交換

手塚構成員：資料に承認案と記載があり、暗号技術評価委員会では、どこまで審議・承認されたのか。

事務局（NICT）：資料３の２ページ前半の３点について暗号技術評価委員会にて審議し、承認が得られている。

手塚構成員：暗号技術評価委員会での審議結果を受けて、タスクフォースで議論すべきことは何か。

松本座長：暗号技術評価委員会では、ハッシュ関数 SHA-2、SHA-3 の実装性能及びセキュリティ面に問題がないことを確認し、現在のルール上、推奨候補暗号リストに掲載する資格は満たした。タスクフォースでは、SHA-2、SHA-3 をどのような形で載せるかどうかを検討したい。タスクフォースで原案を作成し、暗号技術検討会で承認を得ることを想定している。

満塩構成員：新しくて良い暗号を使いたいという実装者の足かせにならないように議論してほしい。システムインテグレーター側に、CRYPTREC 暗号リストに記載されていないため安全でないと判断されないように、推奨候補暗号リストでもよいので、少なくともどこかのリストに載せた方がよいと思う。また、ハッシュ関数の種類ごとに並べる案１と、まとめる案２について、どちらが良いかについて意見はあるのか。

松本座長：議題１では、ビット長に関しては、256 ビット以上のものは掲載して良い方針があり、当該方針に基づき、256 ビット以上のもののみ推奨候補暗号リストに追記することで良いかという確認をしたい。資料３の背景についての補足だが、JCMVP は CMVP と足並みをそろえるという基本方針があり、かつ、電子政府推奨暗号リストに記載される暗号アルゴリズムは「承認されたセキュリティ機能」に入れることとしている。電子政府推奨暗号リストに記載されていないが実装された製品が社会に出ている暗号アルゴリズムについては、「承認されたセキュリティ機能」に入れるかどうか JCMVP が主体となって決めている。SHA-3 についてはこれから JCMVP でも審議を行うことになるが、CRYTPTREC 暗号リストにも掲載されていない場合でも、「承認されたセキュリティ機能」に追加されるものもある。推奨候補暗号リストから電子政府推奨暗号リストへ昇格し、JCMVP で認証した製品が政府調達に利活用されるスキームは適切なものとなっている。セキュリティを重視した場合であっても、CRYPTREC 暗号リストへの追加対象となる暗号アルゴリズムは、暗号技術評価委員会での審議を踏まえた考え方としてもよいと思う。

太田構成員：問題ないと思う。

松本座長：議題１に関するタスクフォースの結論は、事務局案のとおりハッシュ長が 256 ビット以上のアルゴリズムのみとする。

議題２の追加先リストについては、推奨候補暗号リストに掲載し、然るべきタイミングで様子を見てから電子政府推奨暗号リストへ昇格させる案２が妥当だと思うが、いかがか。

手塚構成員：案２が一番妥当だと思う。

松本座長：案１は先走りすぎだと思う。
盛合構成員：SHA-512/256 はすでに実装されていると思うが、SHA-3 と同じ扱いでよいか。
松本座長：SHA-2 は利用されているのか。
盛合構成員：１パラメータのみ実施する意味があるのか考える必要はある。
太田構成員：SHA-512/256 は利用実績調査がまだ行われていないが、この追加した１項目のみ行う建前は理解するが、単独で行うのではなく、あるタイミングで SHA-3 とあわせて利用実績調査をするのがよいのではないか。
松本座長：利用実績調査をするとすれば、次回の暗号技術検討会の後になるので、早くても 3 月以降になるのではないか。
事務局（IPA）：利用実績調査は、1 アルゴリズムをやるのも 10 アルゴリズムをやるのも労力としては同じ。調査では利用するアルゴリズムの選択肢が１個増えるのか 10 個かの違いであり、労力の差がない。NIST の SHA に関してのバリデーションルールでは、暗号アルゴリズムの部分のチェックの仕方の対象として、SHA-512/256 はない。あくまで SHA は、SHA-224、SHA-256、SHA-384、SHA-512 というように、FIPS 180-3 で記載されているものであり、512 の中に SHA-224、SHA-256 を含んでいると解釈するか、含んでないと解釈するかは非常に微妙。
松本座長：今の CRYPTREC 暗号リストの SHA-512 は、SHA-512/256 がない時に定めたものだが、SHA-512、SHA-512/256 ともに、暗号技術評価委員会にてセキュリティ上は問題ないことが確認されている。SHA-512/256 の利用実績がどれくらいあるか把握していないが、SHA-512 はすでに電子政府推奨暗号リストに掲載されているので、あとは整理の問題。
松本(泰)構成員:SHA-512/256 は 1024 ブロックにて利用する場合効率的だったためだろう。
事務局（IPA）：SHA-256 は 32 ビット、SHA-512/256 は 64 ビットを演算単位としている。64 ビットの CPU で使う際に SHA-512 を使った方が、処理が早いためだと思う。
松本(泰)構成員：多分、今は SHA-512/256 が利用されていないだろう。掲載を急ぐ必要はないが、性能の問題で話題にあがると思う。
手塚構成員：利用実績調査はいつ実施することができるのか。
事務局（IPA）：暗号技術検討会にて利用実績調査を行うことの承認を得られた後に、予算確保を確保して発注を行い、半年かけて調査を行うとすると、調査結果が出るのは早くて来年末だと思われる。
手塚構成員：結局、暗号技術検討会で審議してから決定するので、やはり来年度末か。
満塩構成員：ならば、SHA-512/256 と SHA-3 を分ける理由はない。作業ステップ・効率を考えれば、SHA-3 の利用実績調査とまとめてやることがよいと思う。
松本座長：これまでの議論から、議題２については、SHA-3、SHA-512/256 合わせて案２とし、利用実績調査の実施に当たっては、同時に行うこととする。議題３の表記方法については、各々のアルゴリズムを列挙する案１しかないように思う。
満塩構成員：政府統一基準では、新規システムを導入する場合は、やむを得ない場合を除

き電子政府推奨暗号リストに記載された暗号アルゴリズムを採用することと書かれているが、安全性・実装性に問題がなければ推奨候補暗号リストに記載の暗号アルゴリズムも採用してもよいという理解でよいか。

オブザーバ(NISC)：推奨候補暗号リストが技術的にどういう位置づけなのか明示してほしい。

松本座長：推奨候補暗号リストに掲載されている暗号アルゴリズムは、セキュリティ上問題はなく、実装性能において普通の用途には問題なく使えるというもの。

オブザーバ(NISC)：政府統一基準は、基本的に性能基準を示したものであるため、技術的な性能基準を満たされているものであれば、採用することを妨げるものではない。

松本座長：議題３の表記方法については、案１とする。４ページ最後に記載されている形で第２回暗号技術検討会に提案し、承認を仰ぐこととする。

太田委員：２ページ目の配慮すべき点について、「一部分のみがリストの対象となる。」とした場合、SHA-2 のほんの一部のみが掲載されているように解釈され、修正すべき。

松本座長：では、「全てがリストの対象となっているわけではない。」と修正したい。

（４）CRYPTREC の活動方針についての論点

資料４に基づき、事務局より説明が行われた。意見交換内容は以下のとおり。

〇意見交換

太田構成員：暗号技術活用委員会と暗号技術評価委員会とでは立場が違うということは理解したが、CRYPTREC の活動に協力してくれる企業とタイアップし、生産性を上げて情報発信していく方向に舵を変更していくということでよいか。

事務局（IPA）：結果的にそうなることはあるかもしれないが、個別企業とべったりつきあうというところまでは踏み込めないと思う。そのリスクを考慮して市販製品の設定などは行わないとか、暗号技術評価委員会と暗号技術活用委員会のポリシーを分けて設定してポリシーに基づき運用するようにするか等の線引きをタスクフォースで議論してほしい。

松本座長：CRYPTREC の活動範囲を広げるにあたり、５ページの下にあるような主体的判断の要素をどこまで想定するのか、９ページにある成果物をどのように展開していくのか、このような観点で議論したい。

松本(泰)構成員：在り方検討グループでは、成果物に附番することの必要性について議論した。NIST では、SP-800 シリーズをもとに、SP-1800 シリーズというベストプラクティス集を次々と出している。日本でも、技術的にエンドユーザが求めているのは、電子政府推奨暗号リストに則ったベストプラクティス集であると思う。また、サービス事業者等では、暗号アルゴリズムの強度だけでは解決しないトレードオフが幾つもあるのが現状である。例えば、SHA-1 しか使えない機器等もありその場合、SHA-1 の使用をやめるとするとしたら、何も暗号が使えなくなるといった悩みがある。このようなことへの説明を含めたベス

トプラクティス集が望まれている。そういった実態も踏まえ、SP-1800 シリーズではベンダーも一緒に作成している。

手塚構成員：CRYPTREC がこれまで行ってきた暗号アルゴリズムの客観的な安全性の確認はこれからも続けていく必要があるが、暗号を利活用することを検討する次のステップにおいては、成果物を政府統一基準に掲載されることが理想だと思うが、まずは必要こと・やりたいことを効率的なやり方で行い、得られた成果物をまとめたり発表したりする段階で製品名の出し方や CRYPTREC のクレジットのことを議論すればよいのではないか。

松本(泰)構成員：手塚構成員の意見に賛同する。

松本座長：何でも柔軟に対応するということではなく、セキュリティの評価はしっかりと行うこと、それが揺らぐことのないよう留意することは大前提。

満塩構成員：客観的なセキュリティ評価という基準は残しつつ、主体的な基準で判断することもあるところは賛成。海外のドキュメンテーションなどでもそうなっているが、主体的な基準で判断される場合、仮説を明確にしておく必要がある。仮説は客観的な基準も考慮しつつ位置づけられるものであり、組織の戦略などによって変化させていくものでもよいと思う。そういう意味では、CRYPTREC として Appendix を追加していくというよりは、企業自身がどのような設定を行って、どのような評価しているか、ということを CRYPTREC のドキュメントをベースに行っていくことが理想だと思う。CRYPTREC としての仮説や判断を示して、企業側にそのような活動をしてもらうことが良いのではないか。

松本座長：Appendix を別文書として、ベンダーを交えた議論の場を設け、ベンダーが案を出していくこととし、おかしい議論とならないようにチェックしていく体制も考えられる。それを附番するなどで文書体系をしっかりと固めておくことが必要。例えば、今議論している Appendix とは、SSL/TLS 暗号設定ガイドラインの Appendix に相当するものであり、このような成果物はどのように発信していくかという整理も必要だと思う。CRYPTREC としては大枠を決めて、動きやすいように Appendix を分けて整理するのが適当か。

手塚構成員：政府統一基準とうまくリンクできるようにするためのパスをどうやって見つけるかが重要。

松本座長：良いものがあれば政府統一基準に掲載するではなく、SSL/TLS 暗号設定ガイドラインなどを事例として、どうすれば政府統一基準に掲載できるのか具体的な意見を NISC から挙げてほしい。

オブザーバ(NISC)：NISC としては、暗号利用で重要なポイントを CRYPTREC から教えてほしい。鍵管理の方法も重要だと思っているほか、データ通信のための暗号活用や、データ保存のための暗号利用も重要だと思う。

松本座長：今 NISC から挙げてもらった鍵管理やデータ保存時の暗号利用などのような事例をうまく集めて、ドキュメントやガイドラインを作成し、それを政府統一基準と体系づけられたリンクができればよいということだと思う。

手塚構成員：CRYPTREC では、SSL/TLS 暗号設定ガイドラインのように、通信時の暗号設定

方法は示してきたが、データ保存や鍵管理といった運用面での暗号利用についての検討を行っていなかったので、今後、その点をうまくレポートとしてまとめていけるようにすることが理想。

オブザーバ(NISC)： NISC からは事務局にいくつかテーマの候補は連絡しているので、CRYPTREC からも盲点になりうることがあれば共有してほしい。

上原構成員：政府統一基準はこれまで、政府調達の仕様書に、「電子政府推奨リストに記載されている暗号を選ぶこと。」という記載を要求するレベルであったが、これからは、この書きぶりを入れ込んでくれというレベルまで書き下す必要がある。NISC や業界から、仕様書にはどのくらいの粒度で記載したいといったひな形を挙げてもらうと、CRYPTREC としてはどのような仕様書への記載方法が適当か提案しやすい。

松本座長：SP-800 に影響を与えるような良いものとしたい。

オブザーバ(NISC)：仕様書に書く技術的要求は非常に多いので、記載したい粒度を示すことは難しい。細かく定めれば定めるほど直接参照となっていくので、結局政府統一基準を参照することなどを記載することとなり、有名無実化するおそれがある。

満塩構成員：SSL/TLS 暗号設定ガイドラインのチェックリストのように、調達担当者が確認すべきポイントと対応方法法をまとめることも重要であり、そうした議論が必要だと思う。

上原構成員：調達と運用は分けて考えられる。調達はあまり柔軟な対応ができないものなので、仕様書のひな形を用意して進める必要があるが、運用は通達一つで柔軟な対応を行っており、NISC から通達を出しつつ、調達対応も図っていくなど両面での対応を行うのが良いかと思う。調達要件を十分に記載していない場合、調達できないこともあるため、そうした場合への担保も必要だと思っている。

満塩構成員：５ページにある設定ガイドラインとマネジメントガイドラインの中間のものを具体的に議論し、活動を広げていくポイントを随時議論していくことがよいのではないか。

松本座長：今回の議論をまとめると、政府統一基準を始めとして、調達や運用に活用されるドキュメント群を CRYPTREC として構築していくことが重要ということになると思う。具体的に、昨年度までの成果物をリバイスしていく場合、来年度には SSL/TLS 暗号設定ガイドラインと同等以上のものをいくつか作成していくことになると思う。データ保存や鍵管理の議論があったが、この２点は難しいテーマであるので、緊急度や重要度等を踏まえ、優先順位をつけて対応・展開していくことになる。今後の進め方については、事務局での宿題とさせてほしい。論点①については、新しい方針を定義するという結論とするが、この点につき事務局から確認事項があればお願いしたい。

事務局(IPA)：第２回タスクフォースでは、SSL/TLS 暗号設定ガイドラインのアップデート内容の確認と暗号技術活用委員会の次年度以降の活動方針を議論してほしい。

松本座長：ちなみに９ページにある冊子のニーズが想像以上に大きいとはどういう状況か。

事務局(IPA)：管理職あるいは経営層からは、PDF データは見づらいという意見、展示会で

配付されたから読んでおいてくれと目に見える形で渡せるという、利便性の観点から冊子の需要があった。

松本座長：海外のドキュメントは有料。本当に必要なら、有料として財源を確保することもできるのではないか。

事務局(IPA)：NICT や IPA の普及活動の一環で冊子の作成を行うことも考えられる。しかしその場合は、CRYPTREC のクレジットの取扱いについて整理が必要。

（５）その他

盛合構成員：１４ページにある SSL/TLS 市販製品での暗号設定状況の調査は、今年度の暗号技術活用委員会の活動対象となるのか。

事務局(IPA)：調査結果が出るのが来年の夏頃になる見込みなので、今年度の活動対象とはならない。しかし、来年中には Appendix に掲載するかどうかを決める。仮に CRYPTREC としての成果物としない場合は IPA の報告書だけが公開されている状態になる。

盛合構成員：CRYPTREC の方針が固まる前に成果物ができた場合、IPA の成果として公表した後で CRYPTREC の成果として改めて公表することになるのか。

松本座長：混乱を招くことがないように、その時に全体最適化を考慮して議論していく。

上原構成員：TLS1.3 において、ChaCha20 というストリーム暗号が唯一のストリーム暗号となりつつある。KCipher-2 を入れ込むことのコメントを行ったが、反応は薄く苦戦している。ChaCha20 を CRYPTREC 暗号リストに追加するために、次の小改定を検討することになる可能性がある。暗号技術評価委員会にて、安全性・実装性の調査をお願いしたい。

上原構成員：国税庁がマイナンバー法に基づき、法人番号をインターネット上のサイトに公表することとしているが、このサイトへのログインの際の認証に用いる鍵が無期限有効のものとされており、セキュリティ確保の観点から問題であると感じている。詳細は把握していないが、GPKI の安全性確保ということになると、CRYPTREC でも何かすべきことがあるのではないかと思っている。

松本座長：本件の対応については、事務局にてどのように対応すべきか検討してほしい。

３　閉会

事務局から、第２回重点課題検討タスクフォースは１２月２１日（月）１９：００～開催し、第２回で積み残した議題があれば、第３回を平成２８年２月３日（水）１９：００～開催する予定である旨の連絡があった。

以上