第 2 回重点課題検討タスクフォース

日時：平成 27 年 12 月 21 日(月) 19:00～21:00
場所：経済産業省 本館 1 階　西共用会議室

議　事　次　第

１．開　会（資料確認等）

２．議　事
(1) 前回議事概要確認と本日の議論の進め方について
(2) CRYPTREC 暗号技術活用委員会の今後の活動に向けて
(3) 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
(4) 暗号プロトコルのセキュリティ確保に向けた活動について
(5) その他

３．閉　会

（資料番号）	（資　料　名）
資料１	第１回議事概要（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
資料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時における 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）

資料１

第１回　重点課題検討タスクフォース　議事概要（案）

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、技術的な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。一方で、事業者では、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 しか使えない機器の場合、SHA-1 の使用をやめることで、暗号化できなくなる悩みがある。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

資料2

CRYPTREC暗号技術活用委員会の今後の活動に向けて

平成27年12月21日

重点課題検討タスクフォース事務局

第1回TFで議論された活動方向性（論点の再整理）①

暗号技術活用委員会で取り扱う可能性があるテーマの質・対象が
従来とは大きく異なってくることが想定されることから、
暗号技術活用委員会の運営スタイルの考え方自体を再整理

「中立性・客観性」の意味合いを広げた従来とは異なる運営スタイル
での**「セキュリティ向上に役立つドキュメント類」の作成**まで
活動対象範囲を拡大する

CRYPTREC暗号
リストの改定
（利用実績調査）

※おおむねこの範囲に拡大

暗号設定ガイドライン
（具体的設定例なし）
（OSS設定例あり）
（市販製品設定例あり）

マネジメント関連の
ガイドライン
（鍵管理、リスク管理等
コンセプトガイドライン）

政策的課題・社会
ニーズ的課題の議論
（合理的な仮説提示）

- Best Practiceのドキュメント類の作成に当たっては（利害関係者でもある）**ベンダの協力**を仰いでもよいのではないか
- 大枠としての**セキュリティ評価の基本線が揺らいでいるように対外的に見えない**（＝ベンダの言いなりにならない）ようにコントロールすることが重要
- CRYPTRECとしてやるべき範囲と別組織がやるべき**範囲の切り分け**を検討
- 作成にあたった**運営スタイルの違いを考慮**し、**適切な文書体系に整理したうえで公開**すべき

論点

- 文書体系の在り方
  - 成果物の区分の仕方・構成をどう考えるか？
  - 読者の主対象をどこに置くか？
  - CRYPTRECが扱うべき範囲と
    別組織が扱うべき範囲の切り分けをどこに置くか？
  - CRYPTRECクレジットをどういう方針で扱うべきか？
  - どのような文書体系が使いやすいか？

今後の詳細検討を
どこで継続するか
要検討
（TF or 暗号技術活用
委員会？）

- 運用ガイドラインのメンテナンス方法
  - 整備すべき運用ガイドラインの対象
  - 内容更新のメンテナンスの仕組み
  - 他組織との連携方法

暗号技術活用
委員会にて検討
（暗号技術活用委員会
活動方針案）

（2015年度）暗号技術活用委員会活動内容案

- 委員をコアメンバに限定した形（10名程度）で開催
- 審議予定の内容は以下の通り
  - 2016年度暗号技術活用委員会の活動方針案の審議・承認
    - 作成すべき運用ガイドライン対象の検討
    - 委員の追加について
  - 運用ガイドライン（「SSL/TLS暗号設定ガイドライン」をモデルケース）のメンテナンスの検討
    - SSL/TLS市販製品での暗号設定状況の調査結果の採用是非
    - ①暗号技術活用委員会で確認・承認、②WGを組織、③CRYPTRECとしては取り扱わない、といった切り分けに関する考え方の整理

最新動向の追記・更新	ガイドライン本体の更新	Appendixの更新・扱い
• 最近のIETF動向反映	• セキュリティ例外型見直し	• 記載内容範囲の切り分け

- 2016年度に持ち越しの論点
  - CRYPTRECとしては直接活動しないが、運用ガイドラインに関連が深いテーマについて扱い
    - 他組織との連携体制（例：NCCoEのようなもの）の検討
  - 文書体系の検討（暗号技術活用委員会で扱うことになれば）

成果物の作成目的からみた区分例

成果物の作成目的からみた区分		具体的な成果物（例） ※下線部は作成したことがある成果物
①	**政府統一基準から参照**される文書	• CRYPTREC暗号リスト
②	攻撃の内容（影響範囲・対処方法等）を**早期に公開し、注意喚起**することを目的とした文書	• 注意喚起レポート
③	安全性／実装性についての特定の基準に基づき、**中立性を重視した客観的な技術評価**を実施した結果をまとめた文書	• 技術報告書 • 暗号技術調査WG報告
④	安全性／実装性についての特定の基準に基づき、**中立性を重視した客観的な判断**を行った結果をまとめた文書	• 暗号技術ガイドライン
⑤	委員の技術知見や外部状況等も考慮して、**主体的な判断**を行った結果をまとめた文書	• （仕様書を補完する）推奨セキュリティパラメータ設定 • 暗号運用ガイドライン（主に暗号設定に関する）
⑥	委員の技術知見や外部状況等も考慮して、セキュリティ向上のための**誘導的要素を主体的に組み入れた**文書	• 暗号運用ガイドライン（主にマネジメントに関する）
⑦	委員の技術知見に基づき、**セキュリティに係る情勢等を主体的に分析・考察**した結果をまとめた報告書	• 調査報告書
⑧	実用性を向上させるための**具体的な設定方法を紹介**した文書	• 暗号運用ガイドライン（主にAppendix / Best Practiceに関する）
⑨	**外部機関が作成・公表**する同系列の文書へのリンク	• 報告書、ガイドライン等

暗号運用ガイドラインの構成からみた区分例

汎用性が高い ⟷ 固有要件の反映が可能

抽象度が高い

詳細

General Guidelines
（政府向け、民間向けの明確な区分けをしない）

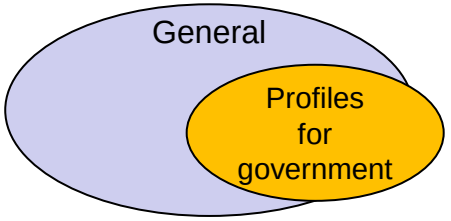
Framework
汎用的・抽象的な検討項目の提示
（※要件というより検討項目・考え方の列挙）

Introduction
ガイドラインの目的や最近動向の説明

General Requirements
必須の検討項目の提示

General Recommendations
汎用的に利用できる推奨要件の提示
（※特定の条件や環境等は考慮しない）

Best Practices
推奨要件に基づく実現例の提示
（※実現例として特定の条件や環境等を設定）



Profiles
特定の条件や環境等（政府向け、民間向け、特定用途向け等に限定）を考慮したうえでの要求項目の提示

Specific-purpose Requirements
要求項目に対応する必須要件の提示

Specific-purpose Recommendations
要求項目に対応する推奨要件の提示

Checklists
推奨要件の実装確認
（※具体的な製品・システムに関する）

NIST文書類作成の関連組織

NIST National Institute of Standards and Technology
Information Technology Laboratory
SEARCH CSRC: GO
CONTACT SITE MAP
Computer Security Division
Computer Security Resource Center

PUBLICATIONS

NIST publishes standards, guidelines, recommendations and research on computer/cyber/information security and privacy using the following NIST technical series. Publication drafts are available for public comment

- Federal Information Processing Standards (FIPS): security standards;
- NIST Special Publications (SPs): security and privacy guidelines, recommendations and reference materials. These include SP 800 subseries (computer security), SP 1800 subseries (NIST Cybersecurity Practice Guides) and selected SP 500-series (information technology) publications directly relevant to computer/cyber/information security and privacy;
- NIST Interagency or Internal Reports (NISTIRs): reports of research findings and background information for FIPS and SPs; and
- Information Technology Laboratory (ITL) Bulletins: monthly overviews of NIST's security and privacy publications, programs and projects.

Sponsored by DHS/NCCIC/US-CERT
NIST National Institute of Standards and Technology
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking

National Checklist Program Repository

NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD

The National Checklist Program (NCP), defined by the NIST SP 800-70 Rev. 2, is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications. NCP is migrating its repository of checklists to conform to the Security Content Automation Protocol (SCAP). SCAP enables standards based security tools to automatically perform configuration checking using NCP checklists. For more information relating to the NCP please visit the information page or the glossary of terms.

Search CVE and CCE Vulnerability Database

(Advanced Search)
Keyword search: Search

Try a product or vendor name
Try a CVE standard vulnerability name or OVAL query
Only vulnerabilities that match ALL keywords will be returned
Linux kernel vulnerabilities are categorized separately from vulnerabilities in specific Linux distributions

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE
NIST National Institute of Standards and Technology U.S. Department of Commerce

Projects

Overview

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available and open source technologies. The NCCoE collaborates with industry, academic, and government experts to build modular, end-to-end reference designs that are broadly applicable and repeatable.

Use Cases Versus Building Blocks

The center works on use cases, which are sector-specific cybersecurity problems, and building blocks, which address technology gaps affecting multiple sectors.

Final Products

When a project is completed, the NCCoE facilitates rapid, widespread adoption of secure technologies by publishing NIST Cybersecurity Practice Guides (Special Publication series 1800), which include all of the information and instructions needed to deploy a reference design.

Partners

The NCCoE has joined with a variety of U.S. companies through a formal initiative called the National Cybersecurity Excellence Partnership (NCEP). These partners have pledged to provide hardware, software and expertise to our mutual efforts to advance the rapid adoption of secure technologies. In addition to contributing equipment and other products to the NCCoE's test environments, companies may designate guest researchers to work at the center in person or remotely.

We are pleased to work with:

Akamai, ca technologies, cisco, FireEye, hp, HYTRUST, IDW, intel, JUNIPER, Lookout, Lumeta, McAfee, Microsoft, NEXTLABS, paloalto, Ping identity, Pulse Secure, redhat, RSA, splunk>, Symantec, tripwire, VANGUARD, VENAFI

参考：NIST文書類での予想分類例(1)

※ NIST文書類の一部をタイトル名からP.3の区分に当てはめて分類した時の予想分類例

成果物の作成目的からみた区分		予想分類例
①	**政府統一基準から参照**される文書	• **（必須）FIPS** • **（ガイドライン）Special Publication (SP)**
②	攻撃の内容（影響範囲・対処方法等）を**早期に公開し、注意喚起**することを目的とした文書	• なし（あえていえばNews／Announcement）
③	安全性／実装性についての特定の基準に基づき、**中立性を重視した客観的な技術評価**を実施した結果をまとめた文書	• **NIST Internal/Interagency Report (NISTIR)** NISTIR7427 6th Annual PKI R&D Workshop "Applications-Driven PKI" Proceedings NISTIR7539 Symmetric Key Injection onto Smart Cards NISTIR7896 Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition
④	安全性／実装性についての特定の基準に基づき、**中立性を重視した客観的な判断**を行った結果をまとめた文書	• **FIPS Appendix／change notice** FIPS186-4 Appendix D: Recommended Elliptic Curves for Federal Government Use • **NIST SP800シリーズ** SP800-22 A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications SP800-107 Recommendation for Applications Using Approved Hash Algorithms SP800-108 Recommendation for Key Derivation Using Pseudorandom Functions
⑤	委員の技術知見や外部状況等も考慮して、**主体的な判断**を行った結果をまとめた文書	• **NIST SP800シリーズ** SP800-133 Recommendation for Cryptographic Key Generation SP800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths SP800-52 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations SP800-77 Guide to IPsec VPNs SP800-97 Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i SP800-111 Guide to Storage Encryption Technologies for End User Devices
⑥	委員の技術知見や外部状況等も考慮して、セキュリティ向上のための**誘導的要素を主体的に組み入れた**文書	• **NIST SP800シリーズ** SP800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach SP800-53 Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans SP800-114 User's Guide to Securing External Devices for Telework and Remote Access SP800-128 Guide for Security-Focused Configuration Management of Information Systems SP800-130 A Framework for Designing Cryptographic Key Management Systems SP800-152 A Profile for U. S. Federal Cryptographic Key Management Systems (CKMS)

参考：NIST文書類での予想分類例(2)

※ NIST文書類の一部をタイトル名からP.3の区分に当てはめて分類した時の予想分類例

成果物の作成目的からみた区分		予想分類例
⑦	委員の技術知見に基づき、**セキュリティに係る情勢等を主体的に分析・考察**した結果をまとめた報告書	• **NIST Internal/Interagency Report (NIST IR)** NISTIR7816 2011 Computer Security Division Annual Report NISTIR7956 Cryptographic Key Management Issues & Challenges in Cloud Services NISTIR7966 Security of Automated Access Management Using Secure Shell (SSH) NISTIR8014 Considerations for Identity Management in Public Safety Mobile Networks • **NIST SP800シリーズ** SP800-145 The NIST Definition of Cloud Computing SP800-176 2014 Computer Security Division Annual Report • **White paper（NIST NCCoE Program）** DATA INTEGRITY - Reducing the impact of an attack
⑧	実用性を向上させるための**具体的な設定方法を紹介**した文書	• **SP800シリーズ（National Checklist Program）** SP800-70 National Checklist Program for IT Products: Guidelines for Checklist Users and Developers • **SP1800シリーズ（NIST NCCoE Program）** SP1800-1 Securing Electronic Health Records on Mobile Devices (DRAFT) SP1800-5 IT Asset Management (DRAFT)
⑨	**外部機関が作成・公表**する同系列の文書へのリンク	• **National Vulnerability Database (NVD)**

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3541 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

FIPS

13. Waiver Procedure: The Federal Information Security Management Act (FISMA) does not allow for waivers to a FIPS that is made mandatory by the Secretary of Commerce.

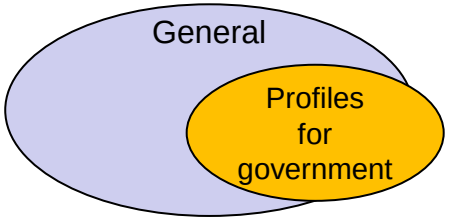
SP

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

参考：ガイドラインの構成例（米国）

For General
（政府・民間の区分けなし）
- SP800-153 Guidelines for Securing Wireless Local Area Networks (WLANs)
- SP800-144 Guidelines on Security and Privacy in Public Cloud Computing
- SP800-119 Guidelines for the Secure Deployment of IPv6
- SP800-88 Guidelines for Media Sanitization
- SP800-52 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations

For Non-federal
（民間向け）
- SP800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
- SP800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise



For Federal
（政府向け）
- SP800-53 Security and Privacy Controls for Federal Information Systems and Organizations
- SP800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations

Framework
- SP800-130 A Framework for Designing Cryptographic Key Management Systems

General Recommendations
- SP800-57 Recommendation for Key Management: Part 1: General

Profiles
- SP800-152 A Profile for U. S. Federal Cryptographic Key Management Systems (CKMS)

Best Practices
- SP800-57 Recommendation for Key Management: Part 2: Best Practices for Key Management Organization Part 3: Application-Specific Key Management Guidance
- SP1800-1 Securing Electronic Health Records on Mobile Devices
- SP1800-5 IT Asset Management

Checklists
- SP800-70 National Checklist Program for IT Products: Guidelines for Checklist Users and Developers
- SP800-69 Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist

参考：ガイドラインの構成例（米国）

■ Practice Guide（SP1800シリーズ）

NIST Special Publication 1800-1b

SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES

Health IT Sector

DRAFT

Gavin O'Brien
Nate Lesser
National Cybersecurity Center of Excellence
Information Technology Laboratory

Brett Pleasant
Sue Wang
Kangmin Zheng
The MITRE Corporation
McLean, VA

Colin Bowers
Kyle Kamke
Ramparts, LLC
Clarksville, MD

Leah Kauffman, Editor-in-Chief

340 **4.6 Technologies**

341 In January 2013, the NCCoE issued a call in the Federal Register to invite technology providers
342 with commercial products that could meet the desired security characteristics of the mobile
343 device use case to submit letters of interest describing their products' relevant security
344 capabilities. In April of 2013, the center hosted a meeting for interested companies to
345 demonstrate their products and pose questions about the project. Companies with relevant
346 products were invited to sign a Cooperative Research and Development Agreement with NIST,
347 enabling them to participate in a consortium to build a reference design that addresses the
348 challenge articulated in the use case.

349 Table 3 lists all products and the participating companies and open-source providers used to
350 implement the security requirements in Table 2. The CSF aligns with existing methodologies
351 and aids organizations in expressing their management of cybersecurity risk. The complete
352 mapping of representative product to security controls can be found in NIST SP 1800-1d,
353 Standards and Controls Mapping, Section 5.

ACKNOWLEDGEMENTS

We gratefully acknowledge the contributions of the following individuals and organizations for their generous contributions of expertise, time, and products.

Name	Organization
Curt Barker	NIST
Doug Bogia	Intel
Robert Bruce	Medtech Enginuity
Lisa Carnahan	NIST
Verbus Counts	Medtech Enginuity
Sally Edwards	MITRE
David Low	RSA
Adam Madlin	Symantec
Mita Majethia	RSA
Peter Romness	Cisco
Steve Schmalz	RSA
Ben Smith	RSA
Matthew Taylor	Intel
Steve Taylor	Intel
Jeff Ward	IBM (Fiberlink)
Vicki Zagaria	Intel

Table 3: Participating Companies and Contributions Mapped to Controls

CSF Function	Company	Application/Product	Use
Identify (ID)	RSA	Archer GRC	centralized enterprise, risk and compliance management tool
Protect (PR)	MedTech Enginuity	OpenEMR	web-based and open source electronic health record and supporting technologies
	open source	Apache Web Server	
	open source	PHP	
	open source	MySQL	
	open source	ModSecurity	Apache module extension, web application firewall (supporting OpenEMR)
	open source	OpenSSL[34]	cryptographically secures transmissions between mobile devices and the OpenEMR web portal service
	Various	mobile devices	Windows, IOS and Android tablets
	Fiberlink	MaaS360	Cloud-based mobile device policy manager
	open source	iptables firewall	stateful inspection firewall
	open source	secure configuration manager / Puppet Enterprise	creation, continuous monitoring, and maintenance of secure server and user hosts
	Cisco	local and remote mobile NAC (Identity Services Engine)	radius-based authentication, authorization and accounting management server
	Cisco	VPN server (ASAv 9.4)	enterprise class virtual private network server based on both TLS and IPSEC
	open source	URbackup	online remote backup system used to provide disaster recovery
	Cisco	wireless access point (RV220W)	Wi-Fi access point

参考：CRYPTRECシンポジウム2013公開資料（抜粋）

5. 将来に向けた展望：文書番号体系の確立とCRYPTREC暗号リストの改定に伴う修正

文書番号体系の確立

- リストガイドを参照しやすくするため、統一的な番号体系を採用し文書番号を付与する

＜文書番号＞::=＜略称＞”-”＜カテゴリ＞”-”＜連番＞
例：CUG-A-003

- 一度付与された連番は，文書の改訂では変更しない
- 改訂における考え方
  - 改訂年度などの情報を入れる（ISO方式）⇒　例：CUG-A-003-2013
  - バージョンを文書に付与する（NIST SP800方式）⇒　例：CUG-A-003 Rev.1

CRYPTREC暗号リスト改定に伴う修正

- CRYPTREC暗号リストの改訂に伴い、これまでに作成したリストガイドを修正する
  - 新しい体系（電子政府推奨暗号リスト、推奨候補暗号リスト、運用監視暗号リスト）に対応した内容の追記

参考資料１

資料２

「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

平成 27 年 10 月５日

暗号技術検討会事務局

資料２

目次

資料２

１.「CRYPTREC の在り方に関する検討グループ」設置の経緯

2001 年に CRYPTREC が発足した当初の目的は、安全でない暗号アルゴリズムが乱立する中で、電子政府において利用が推奨される安全な暗号アルゴリズムを確定させることであり、活動成果として 2003 年に「電子政府推奨暗号リスト」を策定した。

その後、CRYPTREC は、その発足の趣旨に鑑み、電子政府推奨暗号リスト掲載の暗号アルゴリズムについて安全性低下などの問題（暗号危殆化）の監視、注意喚起等を実施など、安心な暗号利用について貢献してきた。一方で、国際標準規格の策定などの要因により、国際的に利用できるデファクト暗号アルゴリズムへの集約が進み、安全でない暗号アルゴリズムが混在するという懸念は激減した。このような外部環境の変化を踏まえ、市場性や利用状況等を加味して評価した結果 2012 年度末に「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト)」を策定（以下「リスト改定」という。）した。

また、リスト改定後は、従来からの「CRYPTREC 暗号リストの安全性維持に係る取組」に加え、「新しい暗号技術の調査」、「暗号技術の普及促進に係る取組」、「中長期的視点に立った暗号政策に係る検討」等を行ってきた。

上記活動を通じて、暗号技術を取り巻く環境、サイバーセキュリティ基本法の施行といった社会情勢の変化等に鑑み、CRYPTREC が果たすべき役割は、CRYPTREC 暗号リストの策定及び維持に限られるものではなく、より柔軟に活動することが望ましいといった意見があった。

このため、今後、社会ニーズ等を踏まえた柔軟な活動を図るべく、CRYPTREC で対象とする暗号技術の見直しや、活動範囲、また安全性確保等にかかる活動の在り方（緊急時対応、必要な体制の見直し）等の議論を行うことが望ましいと考えられ、暗号技術検討会に「CYPTREC の在り方に関する検討グループ」（以下「検討グループ」という。）を設置し、議論を行った。

本報告書では、2015 年 6 月より合計４回開催した検討グループの議論の結果と、今後の CRYPTREC の体制について報告することとする。

資料２

2.「CRYPTREC の在り方に関する検討グループ」概要

2.1 体制（事務局・構成員）

検討グループは、暗号技術検討会の構成員を中心に、学識経験者、暗号ユーザー、暗号研究者により構成することとし、オブザーバーに NISC の参加を得つつ、総務省、経済産業省が事務局として開催した。構成員は表１の通り。

表１　CRYPTREC の在り方に関する検討グループ　構成員名簿

	委員氏名	所属
座長	松本　勉	国立大学法人横浜国立大学　大学院環境情報研究院 教授
構成員	上原　哲太郎	立命館大学　情報理工学部情報システム学科 教授
構成員	太田　和夫	国立大学法人電気通信大学　大学院 教授
構成員	近澤　武	独立行政法人情報処理推進機構 セキュリティセンター 暗号グループグループリーダー（ISO/IEC JTC 1/SC27/WG2 Convenor（国際主査））
構成員	手塚　悟	東京工科大学 コンピュータサイエンス学部 教授
構成員	松本　泰	セコム株式会社 IS 研究所コミュニケーションプラットフォーム ディビジョンマネージャー
構成員	盛合　志帆	国立研究開発法人情報通信研究機構 ネットワークセキュリティ研究所 セキュリティ基盤研究室 室長
オブザーバー	内閣官房内閣サイバーセキュリティセンター	

事務局

総務省　情報流通行政局　情報セキュリティ対策室

経済産業省　商務情報政策局　情報セキュリティ政策室

2.2 開催実績

検討グループは、表２のとおり、合計４回開催した。各会合の開催日及び主な議題は以下のとおり。

表２　CRYPTREC の在り方に関する検討グループの開催

回	年月日	議題
第１回	2015 年 6 月 3 日	(1)「CRYPTREC の在り方に関する検討グループ」開催要綱について (2)CRYPTREC に関する現状について
第２回	2015 年 6 月 24 日	(1)前回議事確認と本日の議論の進め方について (2)CRYPTREC に関する問題意識 (3)暗号プロトコル評価技術コンソーシアム(CELLOS)の概要 (4)サービス視点からの暗号技術(の重要性) (5)全体を通しての意見交換
第３回	2015 年 7 月 3 日	(1)前回議事確認と本日の議論の進め方について (2)CRYPTREC で取り組む新しい暗号技術 (3) これからの CRYPTREC について (4)第１回、第２回の発言ポイントまとめ (5)全体を通しての意見交換
第４回	2015 年 8 月 3 日	(1)前々回の議事確認と今回の進め方について (2)CRYPTREC の在り方に関する検討グループまとめ案 (3)全体を通しての意見交換

資料２

3.「CRYPTREC の在り方に関する検討グループ」議論概要

3.1　全体俯瞰図に関する議論

CRYPTREC が担うべきタスクに関する議論にあたって、以下の論点を踏まえた検討が必要との方針がまず示された。

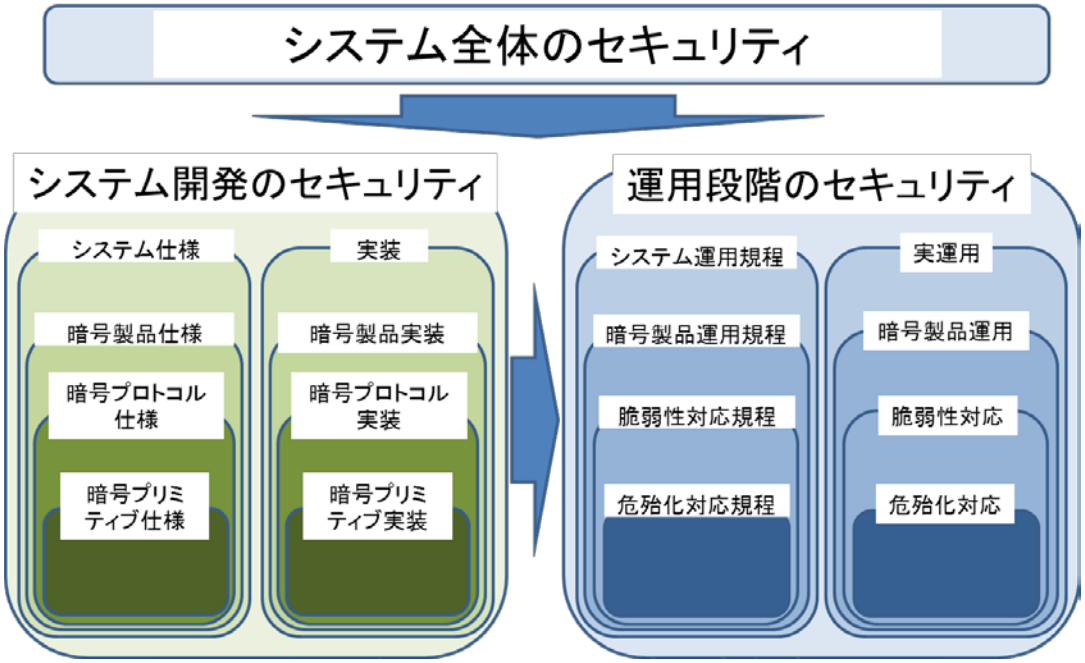
・目的：従来のミッションから変更すべきか、何を追加すべきか
・対象とする活動領域：暗号アルゴリズム等従来に加えて何を対象とするか
・主な適用範囲：電子政府に加えて一般向けの情報システムも対象とするか
・成果物：CRYPTREC 暗号リストに加え、どのような成果物が考えられるか

ただし議論の過程において、「情報システムにおける暗号技術のセキュリティ確保の全体俯瞰図を共通認識として持ち、それを踏まえた上で議論をすべき」との意見が多くの構成員より提出された為、以下の観点から全体俯瞰図を整理した。

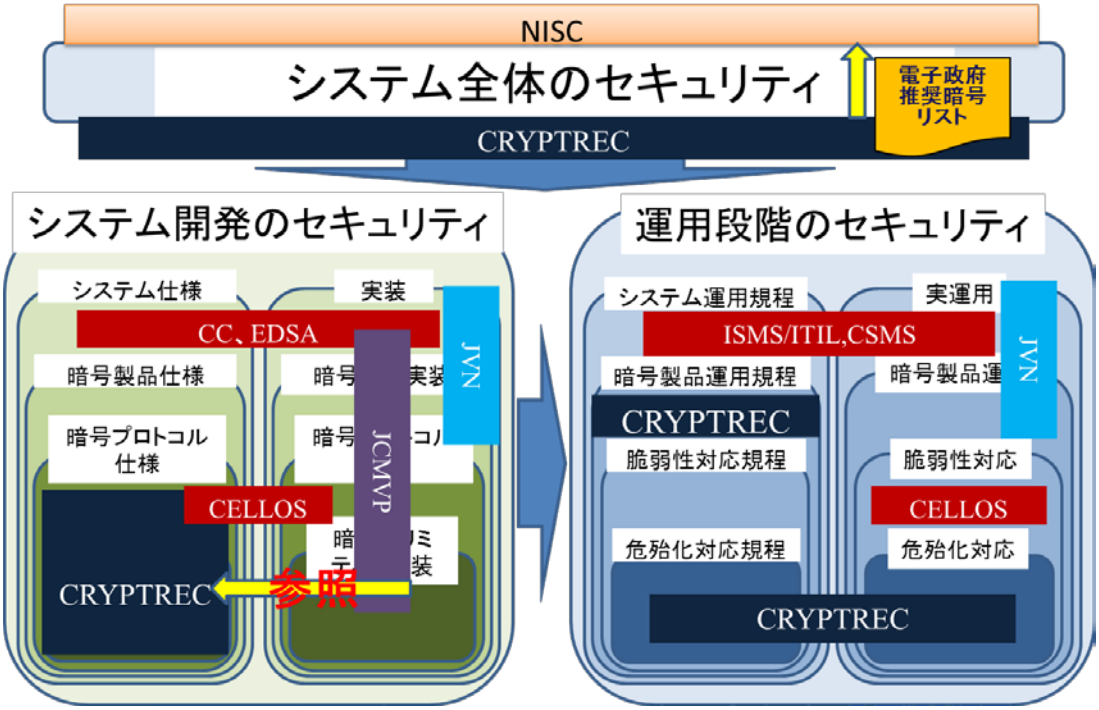
- 情報システムにおける暗号技術のセキュリティは開発及び運用段階で分けて考える必要がある
- さらにそれぞれを「仕様と実装」、「規程とその規程の実運用」とに分けて考えた方が良い
- その上で様々な暗号プリミティブ、プロトコル、製品から情報システム全体といったレイヤ別に確認が必要

上記を踏まえて以下の全体俯瞰図を作成した。

資料２



さらにこの俯瞰図を踏まえた上で、現状の「政府」情報システムにおける暗号技術のセキュリティ確保する既存の各活動と各役割の整理を以下のように行った。



※CC(Common Criteria):IT 製品のセキュリティ認証制度　CELLOS(Cryptographic protocol Evaluation toward Long-Lived Outstanding Security(CELLOS) Consortium) : 暗号プロトコル評価技術コンソーシアム　CSMS(Cyber Security Management System):制御システムに関するセキュリティマネジメントシステム　EDSA(Embedded Device Security Assurance):制御機器（組込み機器）のセキュリティ保証に関する認証制度　ITIL(Information Technology Infrastructure Library):IT サービスマネジメントのベストプラクティスをまとめたフレームワーク　JCMVP(Japan Cryptographic Module Validation Program):暗号モジュール試験及び認証制度
JVN(Japan Vulnerability Notes):ソフトウェアなどの脆弱性対策情報ポータルサイト

その結果、以下のようなCRYPTRECの現状の位置付けと、関連する活動の状況が整理された。

- CRYPTREC は主に、情報システム開発の暗号プリミティブへの対応を主眼におき、暗号プロトコルの仕様まで対象に含めて対応してきた。
- 運用に関しても、CRYPTREC は危殆化監視活動の他、一部製品レベルに踏み込んだ運用規程（SSL/TLS暗号設定ガイドライン等）を提供している。
- CRYPTREC が主に対象としている以外の領域にも、基本的にはセキュリティの担保をするための認証制度や情報提供機能等の仕組みがある。

上記の全体俯瞰状況を踏まえた上で、各項目について議論を行った。

3.2 CRYPTRECのミッション（目的）に関する議論結果概要

CRYPTRECミッションに関わる事項についても多くの議論がなされた。

現行のミッションは「CRYPTREC暗号の安全性及び信頼性確保のための調査・検討、CRYPTREC暗号リストの改定に関する調査・検討に加え、暗号技術の普及による情報セキュリティ対策の推進検討」となっているが、それらに対して各種意見が出され、以下の課題が整理された。

- 暗号アルゴリズムより上のレベルであるプロトコルや製品、また実装・実運用に関する活動に関して、CRYPTRECとしてどのようなミッションを持つか
- CRYPTRECで行う「暗号技術の普及による情報セキュリティ対策の推進検討」を今後どうするか
- プライバシー保護やIoT社会など社会ニーズを見据えた暗号技術への取組や提言機能をミッションとして加えるか

上記の課題に対して、以下のような検討の指針が示された。

- 活動領域の詳細議論にて、情報システム全体のセキュリティ確保に最適なCRYPTREC活動の在り方について検討
- 今後、CRYPTRECで行うべき「普及促進」の明確化が必要
- 新たな社会ニーズの把握と、必要な提言機能のミッション追加を検討する

これらを踏まえて、新たなミッションに関する案が示された。

「CRYPTREC 暗号(※１)のセキュリティ及び信頼性確保のための調査(※２)・検討、CRYPTREC 暗号リストの改定に関する調査・検討に加え、関係機関と連携した暗号技術の普及による情報セキュリティ対策の推進検討（※３）や提言」

（※１）暗号プロトコルを含む。

（※２）監視活動を含む。

（※３）一般利用者からのニーズの検討も含む。

ただしミッションについては、その他の各種議論を踏まえた上で最終的には見直すものであり、継続的な議論が必要との結論となっている。

3.3 CRYPTREC が対象とする活動領域に関する議論結果概要

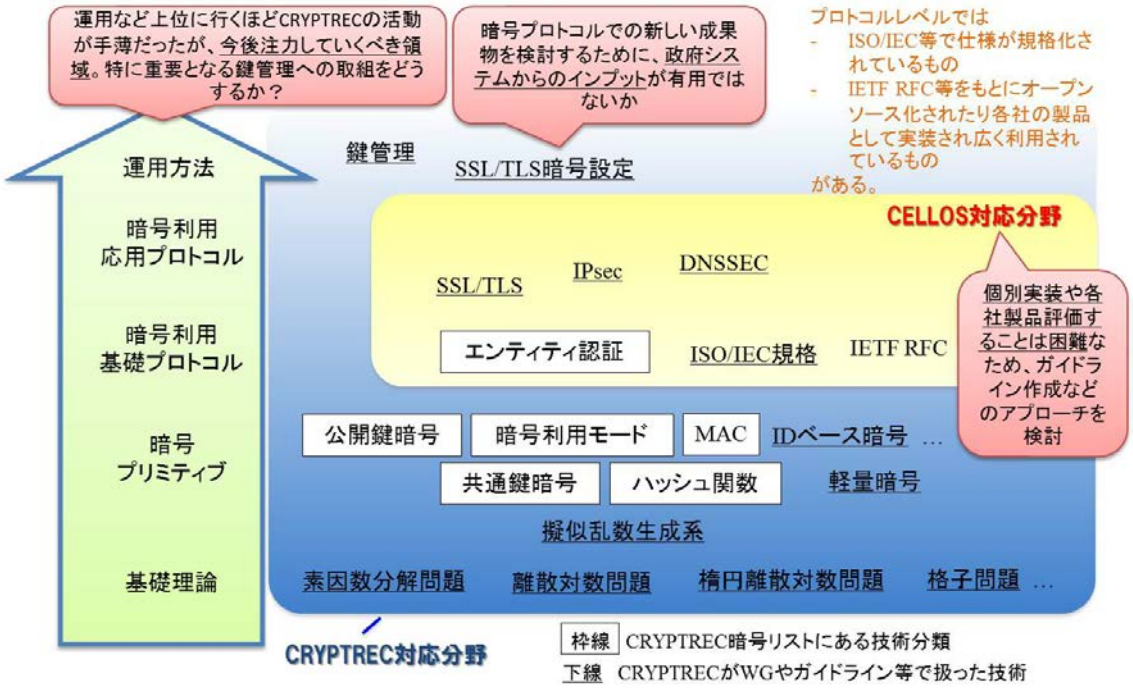
対象とする活動領域の検討について、既存の他団体の活動（プロトコルのセキュリティ評価（CELLOS)、製品（ソフトウェア）の脆弱性（JVN）等）との関係を考慮した上で各種議論がなされ、以下のような課題が整理された。

- CRYPTREC の網羅性
- 暗号プロトコル評価に関する CELLOS との役割分担
- その他既存の他団体と連携

上記の課題に対して、それぞれ以下のような議論がなされた。

- CRYPTREC の網羅性に関しては、既に CRYPTREC で活動している領域でも、活動の網羅性（政府調達から参照されるべき成果物を揃えることができるか、という観点）から再検討されるべき、という観点で多くの議論がなされた。例えば暗号プロトコル及び運用面（鍵管理等）での活動を再検討することが必要といった意見がみられた。
- 暗号プロトコルでの評価活動を検討するにあたっては、活動目標に応じて、CELLOS との詳細な情報交換を行い、具体的連携方法の議論が必要との認識が示された。
- CRYPTREC の限られたリソースも考慮すると、実装や製品評価といった個別評価の分野や脆弱性対応など迅速性が要求される分野は積極的に他団体との連携を検討することが必要との認識が示された。

資料２



（参考）暗号技術マップのイメージ

これらを踏まえて、活動領域に関する以下の案が示された。

・既存の CRYPTREC 活動領域について、以下の観点で見直す
-暗号プロトコル仕様のセキュリティ確保対策について、CELLOS との連携を考慮しつつ、引き続き検討する
-運用のセキュリティ確保に関連して必要な活動について、引き続き検討する

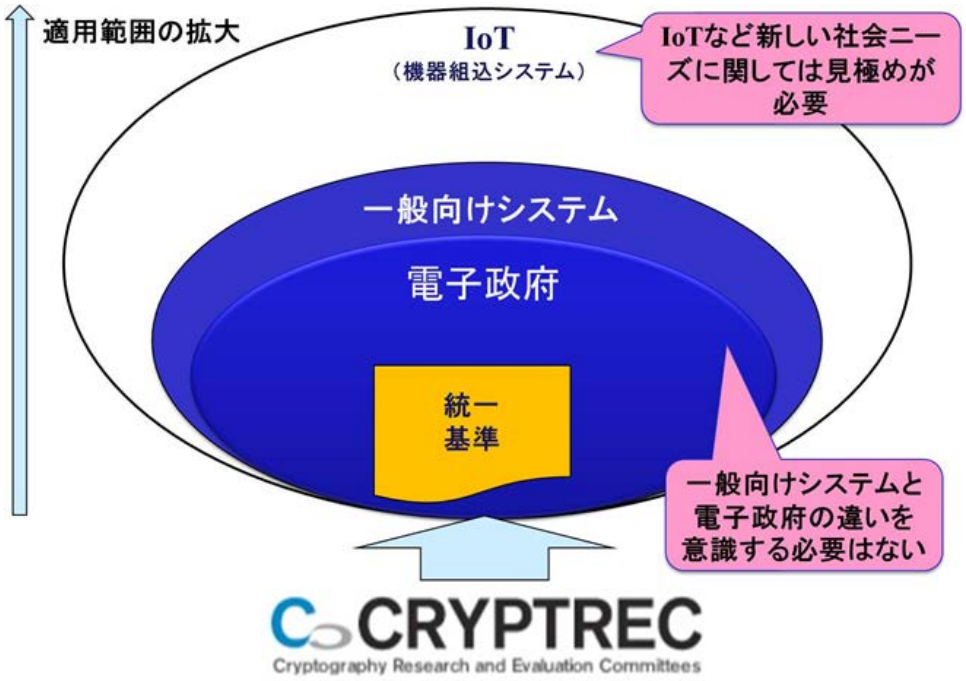
・実装や製品評価といった個別評価の分野や脆弱性対応など迅速性が要求される分野について、他団体との具体的連携を引き続き検討する
-CELLOS との脆弱性対応での連携における具体的フロー検討
-その他の団体との連携に関する必要性やその具体的フロー検討

3.4　CRYPTREC の成果物の主な適用範囲に関する議論結果概要

主な適用範囲については、ビジネスの現状や今後の IoT 社会の到来などの変化も踏まえて、技術的な安全性は前提としながらも、厳密性と運用上の制約とのバランスを考慮しながら、CRYPTREC 活動が主に対象とする領域をどう考えるべきか議論が行われた。

資料２

まず電子政府情報システムから一般情報システムへと領域拡大を検討すべきかが議論されたが、その差異をあまり意識する必要はないとの結論となった。（電子政府情報システム向けの成果物でも利用しやすいものであれば一般情報システムでも利用可能）



（参考）CRYPTREC 成果の適用範囲のイメージ

ただし、IoT やプライバシーなど新しい社会ニーズに関しては見極めが必要との意見が多く出され、以下の課題が整理された。

- IoT 社会を見据えた暗号技術への取組
- 社会ニーズを見据えた調査・検討と提言機能

これらに対して、以下の様な解決に向けた方針が示された。

- IoT 社会で重要になる軽量暗号等について、CRYPTREC として更なるアプローチが可能か、検討が必要
- 暗号技術が社会において活用されるために必要な制度・ガイドラインについて検討し、各種制度や法律も視野に入れた議論が出来る体制が必要

これらを踏まえて、成果物の主な適用範囲に関する以下の案が示された。

- 軽量暗号に関する更なる活動強化を引き続き議論
- 新たな社会ニーズを調査・検討する体制を検討

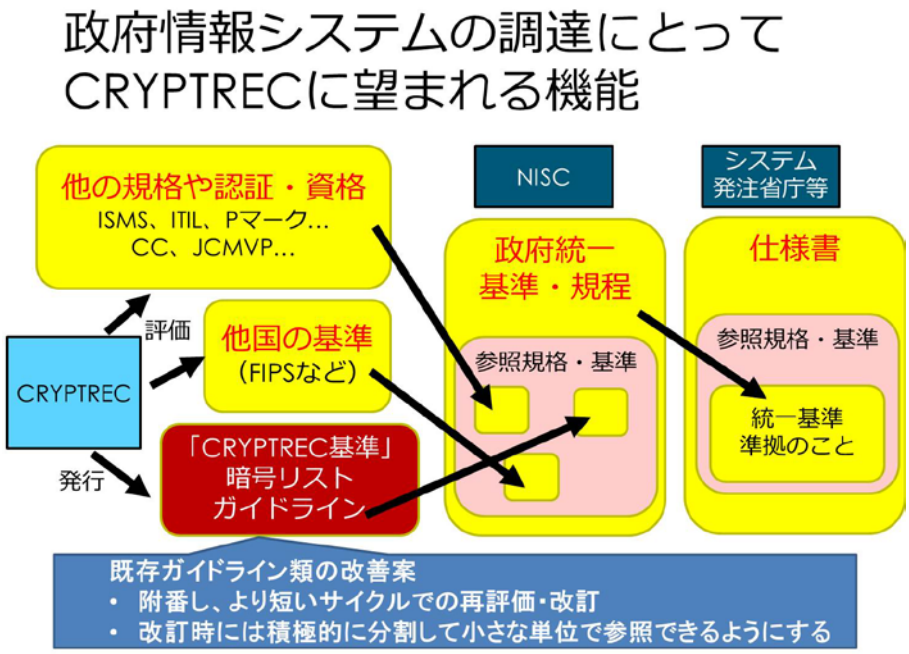
3.5　CRYPTREC の成果物に関する議論結果概要

成果物として、まずは電子政府向けでも現状の暗号リスト以外に柱となるべきものの検討が必要との観点から、以下の課題を挙げた。

- 「情報システム全体における暗号技術のセキュリティ確保」の為に必要なコンテンツ（成果物）の整理

特に CRYPTREC の本来の活動領域である政府調達情報システムにおいて上記課題を解決するために、CRYPTREC がどのような活動を行うべきかが議論された。その結果、既存ガイドライン類を改善し、より政府統一基準等から参照しやすいものとすべき、との意見が提出された。具体的には、成果物ごとの目的の明確化とそれに合わせた内容作成・更新とその情報発信が必要との認識であり、例えば以下のような改善案が示された。

・附番し、より短いサイクルでの再評価・改訂
・改訂時には積極的に分割して小さな単位で参照できるようにする



（参考）政府調達と CRYPTREC 成果物のあるべき関係性イメージ

資料２

これらを踏まえて、成果物に関する検討に対して、以下の案が示された。

- 政府調達に向け統一基準から参照可能な成果物体系の議論を引き続き継続
  -NIST との比較分析を含む
- 適切な情報発信の在り方について引き続き検討
  -他団体との連携方法

以上

参考資料2

2011年度　第１回暗号技術検討会
資料２　別紙１

（2010年度第2回暗号技術検討会
資料「資料2－2」の改訂版）

急激な安全性の低下時における CRYPTRECの対応について

暗号技術検討会事務局

検討の経緯等

- 平成22年度第1回暗号技術検討会において、事務局から検討の背景及び趣旨並びに検討事項案等を提案。

1. 緊急時業務の検討事項案	(1) 緊急対応を開始する契機（アラームトリガー）	緊急対応を開始する契機となる事象 （緊急対応を開始する緊急度の目安を含む。）
	(2) 緊急対応時に執る行動（アクション）	アラームトリガーを受けての行動
	(3) 緊急対応時に検討するべき事項（役割）	アクションにおける所要の作業内容
	(4) 想定検討期間	役割の遂行に要する期間の目安
	(5) 委員会としてのアウトプット	委員会外部へ伝達すべき事項 （委員会外部との連携に要する事項を含む。）
	(6) 検討課題	(1)から(6)までを実現するために整理を要する事項
2. 情報伝達フロー	関係者間の相関に係る概念	

- 平成22年度第2回暗号技術検討会（メール審議）までの期間に、各委員会において、通常業務に比し緊急業務として特に作業や整理を要する事項を調査。
- 加えて、他の委員会との連携の在り方や、情報伝達フローの案を策定。
- 当該メール審議において別添1、2のとおり了承。

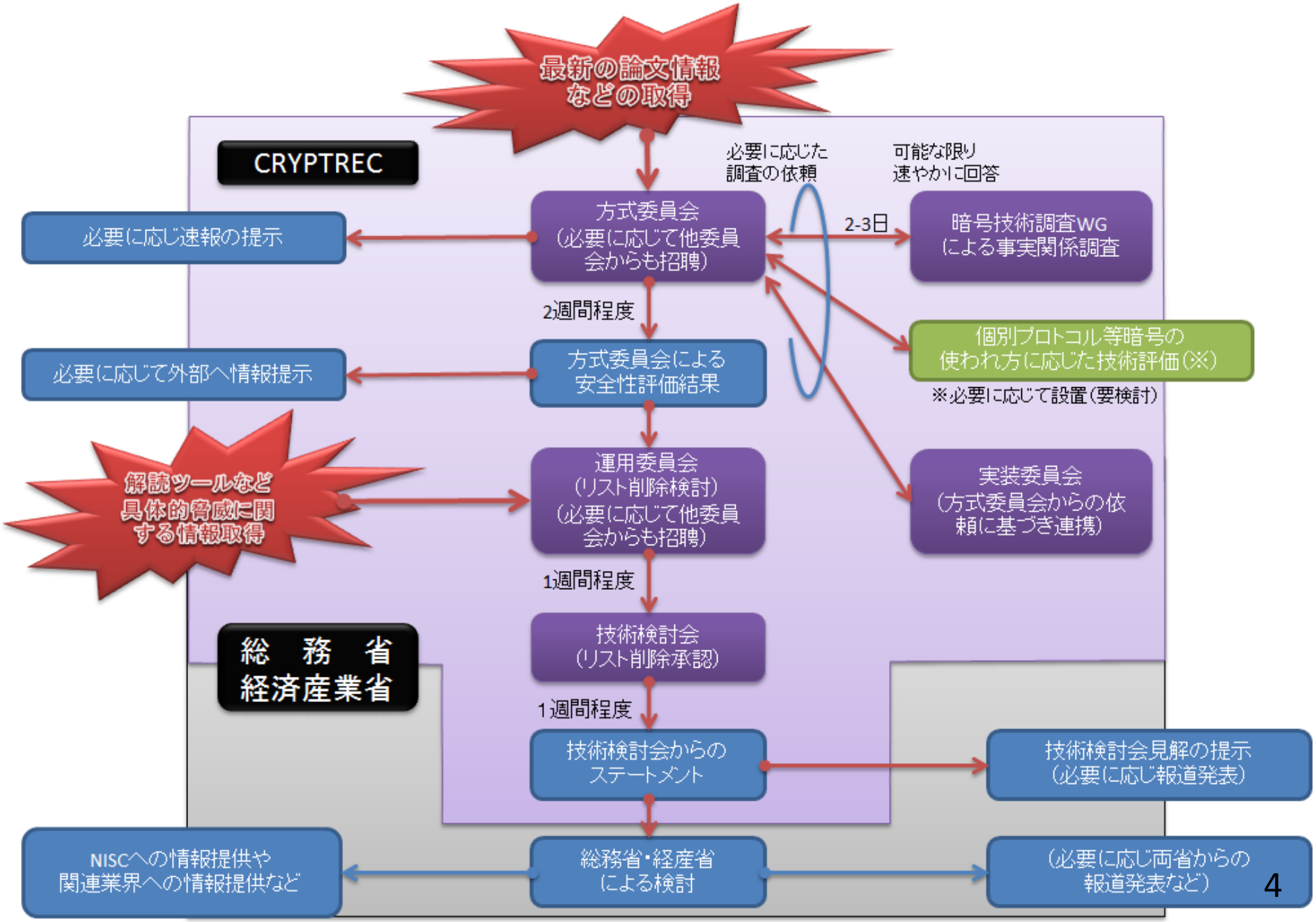
検討会及び各委員会の暗号危殆時対応（各委員会検討結果取りまとめ版）

別添1

		暗号方式委員会	暗号実装委員会	暗号運用委員会	暗号技術検討会
通常業務		◇学会や論文の調査による情報収集 ◇暗号方式の評価、検証 ◇リストガイド作成など	◇電子政府推奨暗号リスト暗号プリミティブの実装性評価	◇電子政府推奨暗号リストの運用に関する検討 ◇利用実績調査など	◇暗号技術検討会の定期開催（事務局） ◇各委員会及び事務局からの議題検討
緊急業務	緊急対応を開始する契機（アラームトリガー）	◇緊急性が高いと思われる事項の発生（論文等の発表、報道等）	◇暗号方式委員会もしくは関連組織・機関からの連絡・通知	◇暗号方式委員会からの報告・通知 ◇SHA-1及びRSA-1024相当[*1]に対する具体的な解読ツールもしくはサービス提供上明らかな具体的脅威となる事例が公表された場合 ◇暗号方式委員会からの報告で、多数の製品で同一理由による脆弱性が発見された場合（例としてBleichenbacher攻撃が該当）	◇暗号運用委員会からの報告・提案の受理（事務局）
	緊急対応を開始する緊急度の目安	◇暗号アルゴリズムごとの攻撃に要する計算量の著しい低下（プロトコルごとの実装暗号の安全性の著しい低下、等）	◇暗号方式委員会もしくは関連組織・機関からの連絡・通知により検討を開始。攻撃が論文化されていなくても検討対象とする。	◇具体的な解読ツールもしくはサービス提供上明らかな具体的脅威となる事例が公表された場合 ◇多数の製品で同一理由による脆弱性が発見された場合	◇運用委員会からの報告内容対する座長判断（事務局から座長へ相談）
	緊急対応時に取る行動	◇暗号方式委員会の開催（委員長判断でメール審議も可） ◇委員長判断で他の委員会の委員やプロトコル技術の専門家を招聘 ◇委員長判断でWGや実装委員会へ調査依頼	◇委員長の判断により、次の選択肢から適切な対応を選択 （1）暗号実装委員会の開催 （2）メール審議 （3）他の委員会への委員派遣（要請された場合）	◇暗号運用委員会の開催（緊急度が高い場合には委員長判断でメール審議も可能） ◇委員長判断で他の委員会の委員を招聘	◇暗号技術検討会の開催（座長判断でメール審議も可） ◇必要に応じ各委員会の委員や専門家を招聘
	緊急対応時に検討するべき事項	◇事項の事実関係の確認 ◇内容の精査（信ぴょう性など） ◇論文等の情報源の詳細精査 ◇技術的確認、検証、追認 ◇技術的安全性の評価、判定（等価安全性への影響や緊急性など）	◇暗号方式委員会が提示する安全性の低下度合いや緊急度に基づき、明らかとなった危殆化により現実的攻撃が短期間のうちに攻撃可能となる対象製品分野、危殆化を発現させるための攻撃のコスト・難易度等	◇暗号方式委員会が提示する安全性の低下度合いや緊急度に基づき、一般的な実利用状況や代替暗号の利用可能性等の実情を踏まえ、「緊急に推奨リストや監視リストからの削除や利用制限すべき必要性があるか否か」の視点のみから検討	◇暗号運用委員会からの報告確認 ◇暗号運用委員会提案の電子政府推奨暗号リスト改定案に対する検討 ◇暗号技術委員会としてのステートメント検討・作成
	想定検討期間	事実関係確認：2-3日程度 安全性評価判定：2週間程度	可能な限り速やか	概ね1週間程度	1週間程度
	委員会としてのアウトプット（外部との連携）	◇運用委員会（事務局及び委員長）への報告・通知 ◇方式委員会としての技術情報の外部発表（危険度や緊急性に応じて）	◇暗号方式委員会に対して「攻撃成立条件の対象製品分野、攻撃の実装可能性・難易度」の判断結果（及び回避策）を報告	◇暗号技術検討会（事務局）に対して「緊急に推奨リストや監視リストからの削除や利用制限すべき必要性があるか否か」の判断結果（及び回避策）を報告 ◇緊急対応不要と判断した場合、推奨リストや監視リストにどのように反映するかは運用委員会の通常業務として改めて審議を行うものとし、その結果を年次報告の形で報告	◇総務省・経産省への報告 ◇公式ステートメントの発表 ◇オブザーバメンバーへの情報提供

暗号危殆化時における暗号技術検討会及び各委員会の間の主な情報伝達フロー

別添2



検討結果1

現在の暗号技術検討会で対応可能な暗号危殆化事案

- 対応が可能な危殆化事案
  - 暗号方式に関する論文の発表や報道など
    - 方式委員会で対応
  - 具体的な解読ツールもしくはサービス提供上明らかな具体的脅威となる事例が公表された場合
    - 運用委員会で対応
  - 多数の製品で同一の理由による脆弱性が発見された場合（例としてBleichenbacher攻撃が該当）
    - 方式委員会で情報取得し、運用委員会で対応

- 対応外の危殆化事案
  - 個別製品・システムにおける脆弱性
  - 電子政府推奨暗号リストに掲載されていない暗号の危殆化

- 現状では対応外だが今後検討が求められる事案
  - 暗号を利用したプロトコルの観点からの安全性の低下
    - 対応方法について方式委員会にて今後検討予定

検討結果2

主な課題と今後の検討

今後検討が必要と考えられる課題	現状の体制では対応困難と思われる課題
① 暗号アルゴリズムとシステムとの間（プロトコル）の脆弱性監視体制（※）【方式委員会】 ② 重要度（安全性の低下度合い）・緊急度による検討の深度、深度による評価期間の目安の変動、即座の判定の実現性の見積もり【実装委員会】 ③ 暗号に対する攻撃の実装コストや実現性の評価【実装委員会】 ④ 暗号実装委員会が緊急対応開始の起点となる事案の有無、及びその対応可能性【実装委員会】 ⑤ 委員会内での情報伝達フロー、検討体制の在り方【全体】 ⑥ 全体の情報伝達フローの検証【全体】 ⑦ 委員会間の情報交換のオーバーヘッドの削減（初動段階で役割分担する体制の是非等）【全体】 括弧【】内は、検討の必要性の意見提出元（委員会）を意味する。 当該課題の継続検討の必要性については、各委員会で判断。	① 暗号アルゴリズムとシステムとの間（製品）の脆弱性監視体制（※） ② 多数の製品で同一理由による脆弱性が発見された場合の周知体制や対応状況の把握体制 ③ 電子政府推奨暗号リストに未掲載の暗号アルゴリズムであって、実社会において無視できない程度の利用実態があるものの扱い（特に具体的脅威となる事例が発生した場合の扱いやその必要性）

※ 脆弱性情報の収集／取扱／注意喚起の方法、緊急事態のケースごとの議論の順序、地位／立場の在り方、通常時／緊急時の区別の必要性を含む。