第 3 回重点課題検討タスクフォース

日時：平成 28 年 2 月 3 日(水) 19:00～21:00
場所：経済産業省 別館 1 階　101-2 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) 暗号アルゴリズムの脆弱性に関する情報発信フローについて
(3) 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
(4) 来年度以降の検討課題について
(5) 2015 年度第２回暗号技術検討会での報告事項について
(6) その他

３．閉　会

（資料番号）	（資 料 名）
資料１	第２回議事概要（案）
資料２－１	暗号アルゴリズムの脆弱性に関する情報発信フローについて
資料２－２	暗号アルゴリズムの脆弱性に関する情報発信フロー（案）
資料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	重点課題検討タスクフォースの来年度以降の検討課題（案）
参考資料１	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）
参考資料２	暗号技術検討会 2015 年度 報告書 目次（案）

資料１

第２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（神田）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（神田）　　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（神田）　　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（神田）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　　アメリカではFIPSは当然として、SPシリーズはNISTがみずからつくっているというよりは、作りなさいという命令の下で作成しているが、日本にはそういう構造はなく、調達で使いやすい文章や強制力のある文章は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（中西）　　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（大久保）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。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ない。ほとんどの場合、プロトコル脆弱性の話しであり、本当の意味での緊急性を要しているわけではない。また、外部では緊急性を有するか否かも不明。

○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、既存の署名文書をどうするのだ、という観点がある。今のところそういう観点でCRYPTRECは物事を考えていない。使用を止めなさいというが、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（神田）　　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（神田）　　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（筒井）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

資料２－１

暗号アルゴリズムの脆弱性に関する情報発信フローについて

平成28年2月3日

重点課題検討タスクフォース事務局

暗号アルゴリズムの脆弱性に関するCRYPTRECからの情報発信の分類

情報分類	速報の必要性	過去の事例
A. 暗号アルゴリズムの**完全な危殆化**による緊急対応	高	該当なし (イメージ：世界中で使われている暗号アルゴリズムが1台PC で1時間で解読可能など)
B. 正確で信頼性の高い情報を発信することによる**過剰反応防止**	中	MISTY1へのintegral attack，SHA-1 free-start collision攻撃など
C. 長期的なシステムの安全性維持のための対策喚起	低	
D. 対応不要	無	

情報発信の手段

情報分類	速報	安全性評価	監視報告 (CRYPTREC Report, 技術報告書等)
A. 暗号アルゴリズムの**完全な危殆化**による緊急対応	実施	実施	実施
B. 正確で信頼性の高い情報を発信することによる**過剰反応防止**	実施	実施	実施
C. 長期的なシステムの安全性維持のための対策喚起	無	状況により判断	実施
D. 対応不要	無	非対象	非対象

公開資料の位置づけ

- **速報**
  外部で公開されている情報に基づき記載する
  情報源は信頼に足る機関・組織等とする
  CRYPTRECでは詳細評価していないことを明示する

- **安全性評価報告**
  CRYPTREC として安全性評価を実施する
  CRYPTREC で評価した報告内容であることを明示する
  公開までの期間は、脆弱性の内容に依る

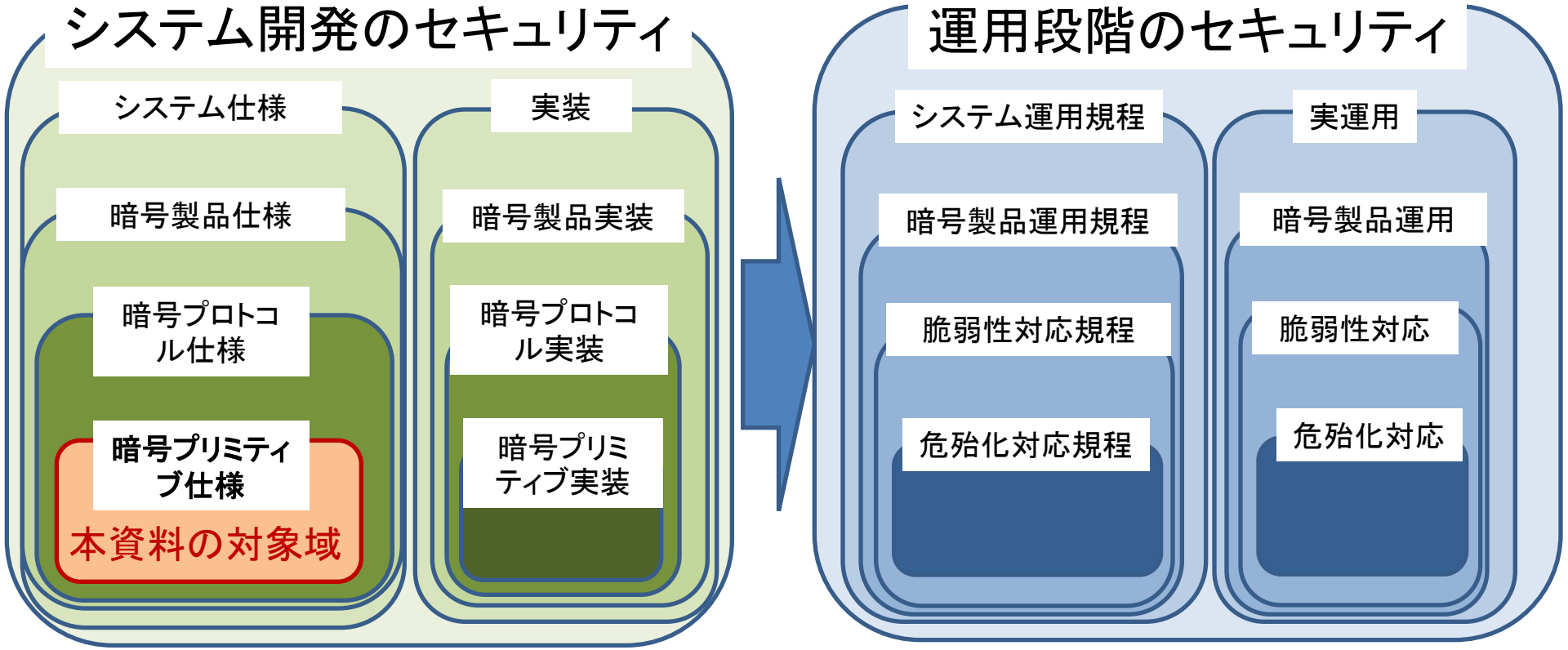
全体フロー図は資料2-2参照

以下参考

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

〇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あり
〇さらにそれぞれ仕様と実装、規程とその規程の実運用とに分けて考えた方が良い
〇その中で様々な暗号プリミティブ、プロトコル、製品からシステム全体といったレイヤ別に確認必要

システム全体のセキュリティ



第4回あり方委員会資料からの抜粋(2015年8月3日)

検討項目

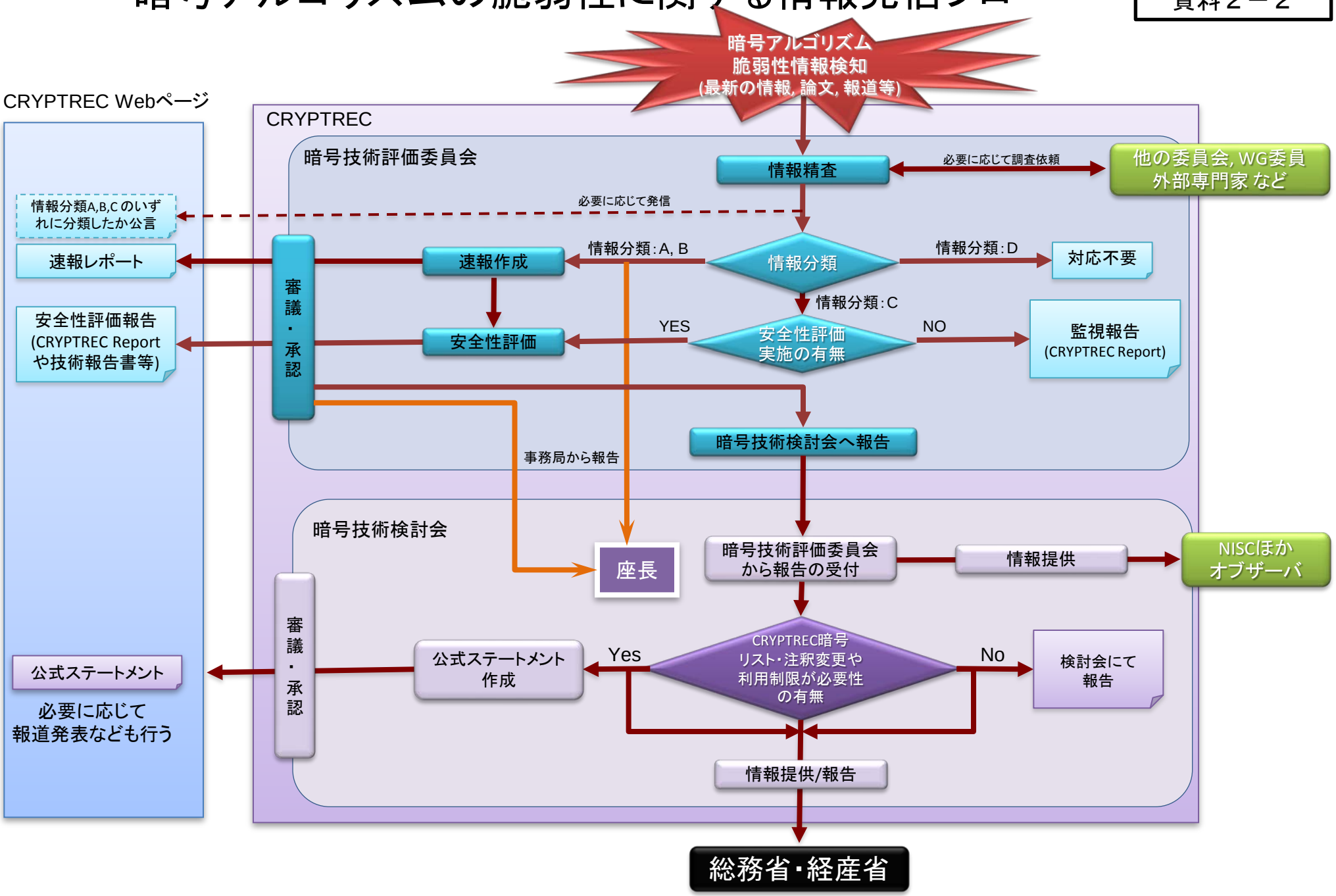
「**暗号アルゴリズム**の脆弱性」の定義	暗号アルゴリズムに対する攻撃計算量の著しい低下 - CRYPTRECにおいて参照している仕様に対する攻撃成功 - 上記までいかないが、上記攻撃の計算量低下につながりうる結果	
確認すべき暗号の範囲	◇CRYPTREC暗号リストに掲載されている暗号技術 ◇CRYPTREC暗号リストに掲載されていないが、影響度が高いと暗号技術評価委員会で認められた暗号技術	
緊急時業務の検討事項案	(1) 緊急対応を開始する契機（アラームトリガー）	緊急対応を開始する契機となる事象 （緊急対応を開始する緊急度の目安を含む）
	(2) 緊急対応時に執る行動（アクション）	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) 委員会等からのアウトプット	委員会等から外部へ伝達すべき事項 （外部との連携に要する事項を含む）
情報発信フロー	暗号アルゴリズムの脆弱性に関する情報発信の意思決定フロー	

暗号アルゴリズムの安全性低下時における緊急対応

	暗号技術評価委員会	暗号技術検討会
通常業務	◇暗号技術のセキュリティに関する監視・評価等 ◇暗号リストを中心とした暗号技術のセキュリティ評価・監視	◇暗号技術に関する調査・検討 ◇CRYPTREC活動計画の承認 ◇各種成果物の承認
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脆弱性の発生 （最新情報、論文、報道等）	◇暗号技術評価委員会からの報告・通知
緊急対応を開始する緊急度の目安	◇CRYPTREC暗号リストに掲載されている暗号技術に対する攻撃計算量の著しい低下 ◇CRYPTREC暗号リストに掲載されていないが影響度が高いと考えられる暗号技術の安全性低下	◇CRYPTREC暗号リストや注釈に影響を与える可能性があるか ◇その暗号技術の利用制限について各政府機関に周知する必要性があるか
緊急対応時に取る行動	◇暗号技術評価委員会の開催（委員長判断でメール審議も可） ◇委員長判断で他の委員会/WGの委員・外部専門家への調査依頼	◇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（影響度や緊急性など）	◇暗号技術評価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有無等の実情を踏まえ、「緊急にCRYPTREC暗号リストや注釈を変更する必要性があるか、利用制限すべき必要性があるか否か」を検討 ◇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	状況に応じて適切に設定	状況に応じて適切に設定
委員会としてのアウトプット（外部との連携）	◇重点課題検討TF及び暗号技術検討会座長への報告・通知 ◇暗号技術評価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）	◇総務省・経産省への報告 ◇公式ステートメントの発表 ◇NISCほかオブザーバメンバーへの情報提供

暗号アルゴリズムの脆弱性に関する情報発信フロー

資料２－２



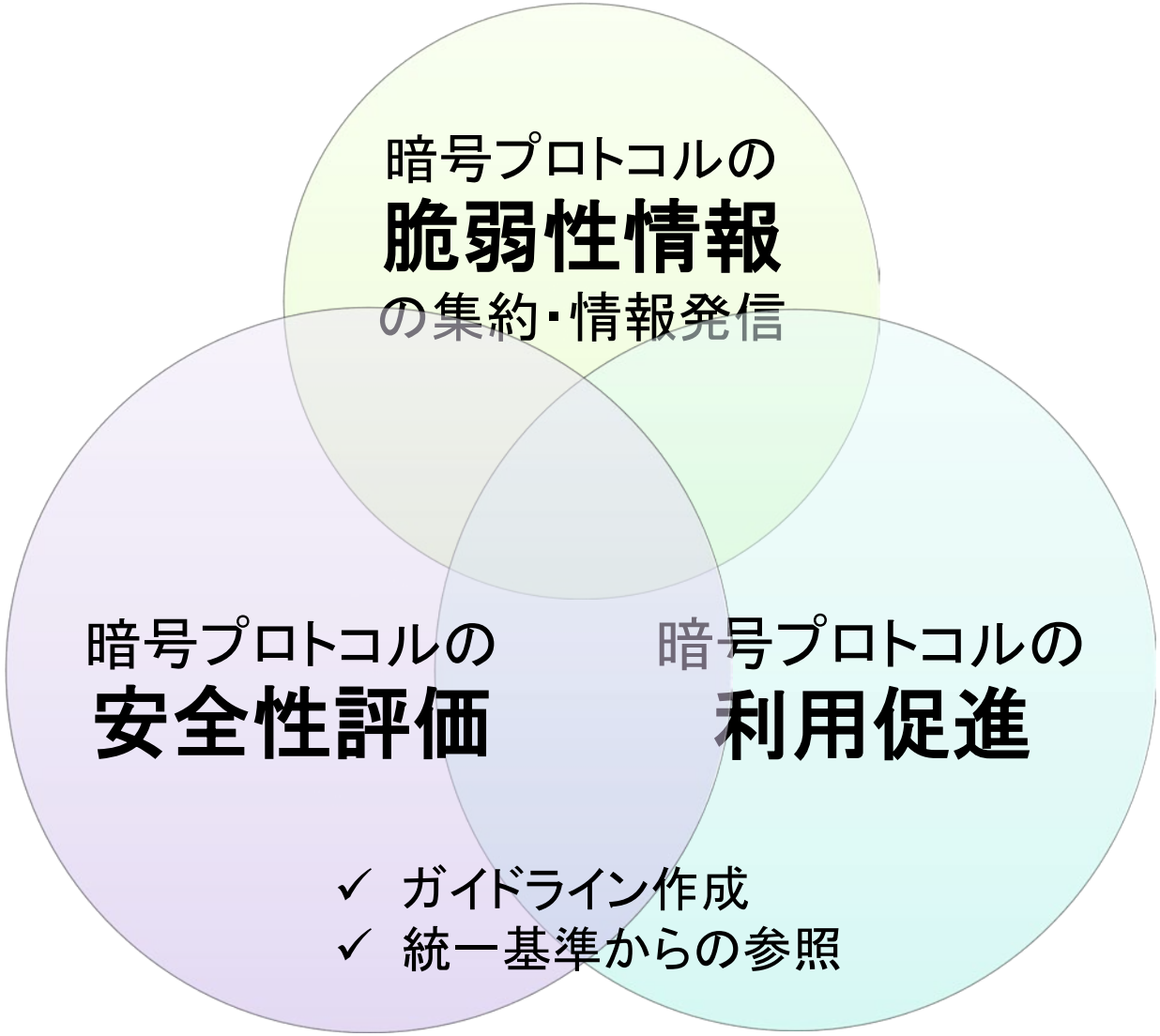
資料３

暗号プロトコルのセキュリティ確保に向けた活動案

平成28年２月３日

重点課題検討タスクフォース事務局

［再掲］CRYPTRECに求められる暗号プロトコル関連のアウトプット



[再掲]課題整理
①暗号プロトコルの脆弱性情報の集約・情報発信

- 「暗号プロトコルに関する脆弱性情報」としてどのレベルまで情報収集・発信を行うか
  - プロトコル仕様レベル, プロトコル実装レベル, システムレベル…
- どのような情報発信を行うか
  - 外部情報へのリンクのみか、CRYPTREC自身でも評価するか
- どのような体制で実施するか
  - CRYPTREC窓口は？　他機関との連携は？

暗号プロトコルの脆弱性情報の集約・発信の整理

団体	ポリシー	監視	評価	発信
（例）CELLOS	速報性重視	有識者がボランティアベースで社会的影響力のある脆弱性情報に対して日々監視を行う	有識者がボランティアベースで迅速に議論	速報として発信
CRYPTREC活動案（A）	CRYPTRECのチャネルを活かしてタイムリーに発信	他組織より情報を受ける	他組織より情報を受ける	外部情報へのリンクが中心のポータル機能を提供
CRYPTREC活動案（B）	正確性を重視技術的な安全性評価	学会, Web, 他組織等から情報を得る	専任のリソースによる詳細評価	詳細な評価情報を提供

CRYPTRECに求められることは

速報　＜　詳細な評価

暗号プロトコルの「詳細評価」のポイント整理

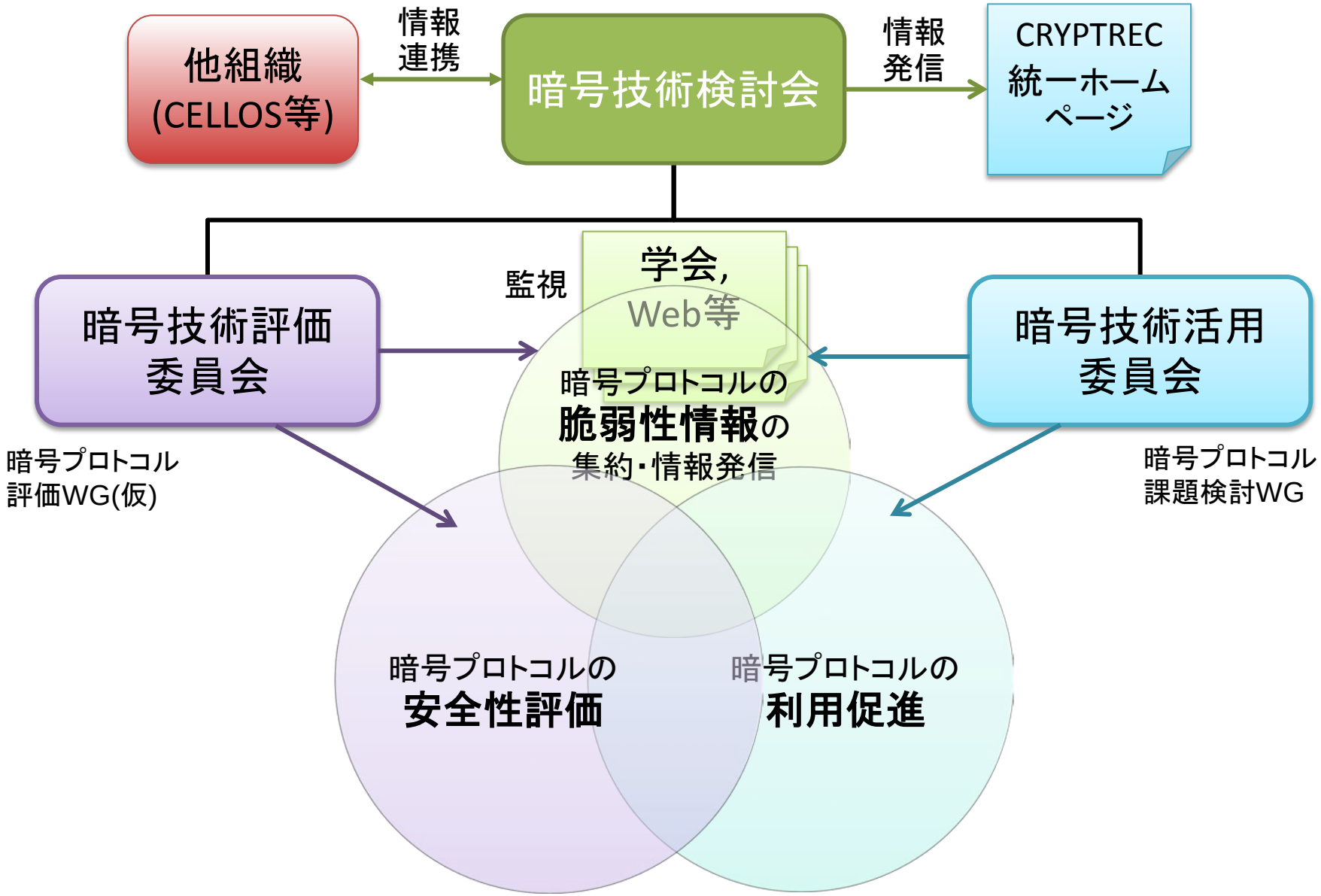
	Who ア)監視/イ）評価/ウ）発信	What 対象		How 情報の入手法
Protocol	暗号技術活用委員会， 暗号技術評価委員会 が連携して実施	電子政府？ ※議論が必要		学会やWebから一次情報を探す／取りに行く、に加え 評価結果を他有識者団体 より受け取る
		仕様	実装	
Primitive	暗号技術評価委員会	CRYPTREC 暗号リスト		学会やWebから一次情報を探す／取りに行く
		仕様	実装	

②暗号プロトコルの安全性評価
③利用促進に向けて何を対象とするか
に関する課題整理

現在の電子政府システムやその他のシステムで活用されている暗号プロトコルの利用状況の調査が必要
（手塚構成員御意見（第2回TF））

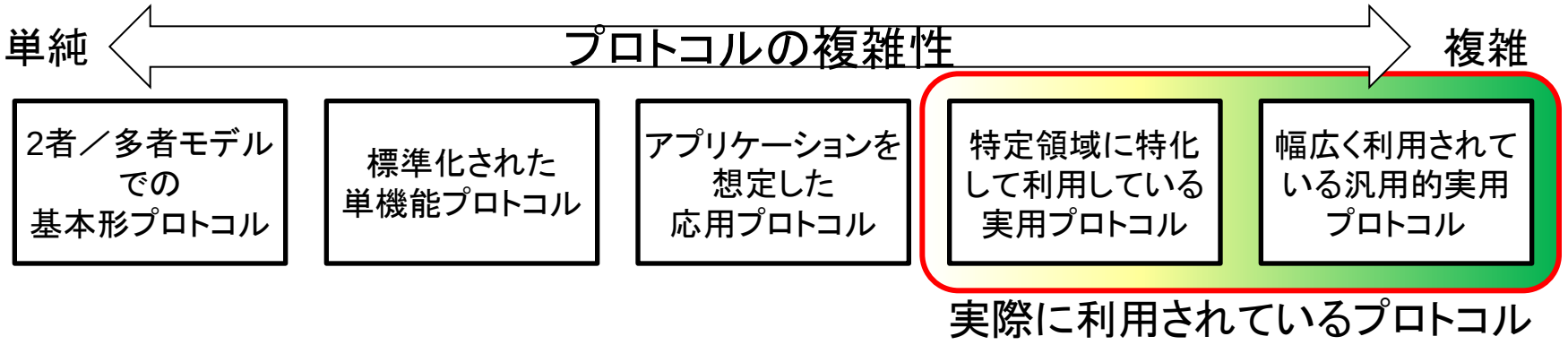
暗号プロトコルの安全性評価について対象及び出口について方向性を決める必要がある

暗号プロトコルに関するCRYPTREC体制案



暗号技術活用委員会の活動概要（案）

- 暗号プロトコル課題検討WG（2016年度 3回開催予定）
  - CRYPTRECとして扱うべき暗号プロトコルの対象範囲の集中検討



  - 運用ガイドラインの作成を前提とした安全性情報や脆弱性情報の取扱方法、他組織との連携方法等の課題整理
    - 運用ガイドラインごとにばらつきが大きく出ないような安全性情報や脆弱性情報の取り扱いルールの明確化
    - 運用ガイドラインに含める脆弱性情報の範囲
    - 安全性情報や脆弱性情報を提供してもらう組織、同種ガイドラインを作成している組織、ガイドラインの主要な利用ユーザと想定される組織等との連携方法

  - 2017年度以降の暗号プロトコルに関する活動方針案の整理・検討
    - 運用ガイドライン（〇〇プロトコル）WGに衣替えを想定

暗号プロトコルの安全性評価について

- 2016年度
  - 暗号プロトコルの安全性評価について他組織と連携について意見交換を行いつつ具体的な方針を事務局で検討開始
- 2017年度
  - 上記方針により安全性評価を開始
  - 実施方法はWG立ち上げまたは有識者等への外部評価依頼を想定
  - アウトプットイメージ:
    - Webからの情報発信，ガイドライン作成など

資料４

重点課題検討タスクフォースの来年度以降の検討課題（案）

平成２８年２月３日
重点課題検討タスクフォース事務局

1. 本年度の主な議題の検討状況

（第1回重点課題検討タスクフォース資料2「重点課題検討タスクフォースの設置について」を元に作成）

⓪ 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～

→具体的な活動にあたっての前提となる方針を議論する。特に活用委員会の活動の評価軸議論が必要。これまでCRYPTRECの活動はリスト作成に代表されるようにあらかじめコンセンサスが得られた基準をもとにした“中立性・公平性”を基本の評価軸としてきたが、活用委員会の活動ポリシーの見直しが必要か議論する。

→文書体系の在り方について議論する。

その他（ SHA-2,SHA-3の取扱い　等）

→SHA-2,SHA3の取扱い方針、タスクフォース設置の目的確認等。

第1・2回 整理済

文書体系については、来年度も引き続き議論

① 定常的な普及・広報活動に加え、脆弱性対応など緊急時の対応を踏まえた情報発信フローの整備　（暗号アルゴリズムのみ）

→脆弱性に関する情報発信の意思決定フローを整備する。このため、脆弱性の定義、トリガーとすべき事象、情報発信時期、確認方法、情報発信手段、確認すべき暗号の範囲等を議論。

② 暗号プロトコルレベルのセキュリティ確保に向けた活動

→どのようなタスク（脆弱性対応、リスト作成、ガイドライン作成等）を想定しているか議論した上で、実施する体制を決め、他関連組織(CELLOSなど) との連携方法を検討。

③ 来年度以降の議論方針　等

第2・3回 整理予定

④ 政府統一基準に向けた新たなCRYPTREC成果物

→過去の成果物の検証及び、NISCの改定方針も踏まえた詳細な計画化が必要。

⑤ 新たな社会ニーズを見据えた新規活動

→方向性をある程度事務局で整理した上で議論すべき。

⑥ 情報システム全体のセキュリティ確保を意識した他団体との連携

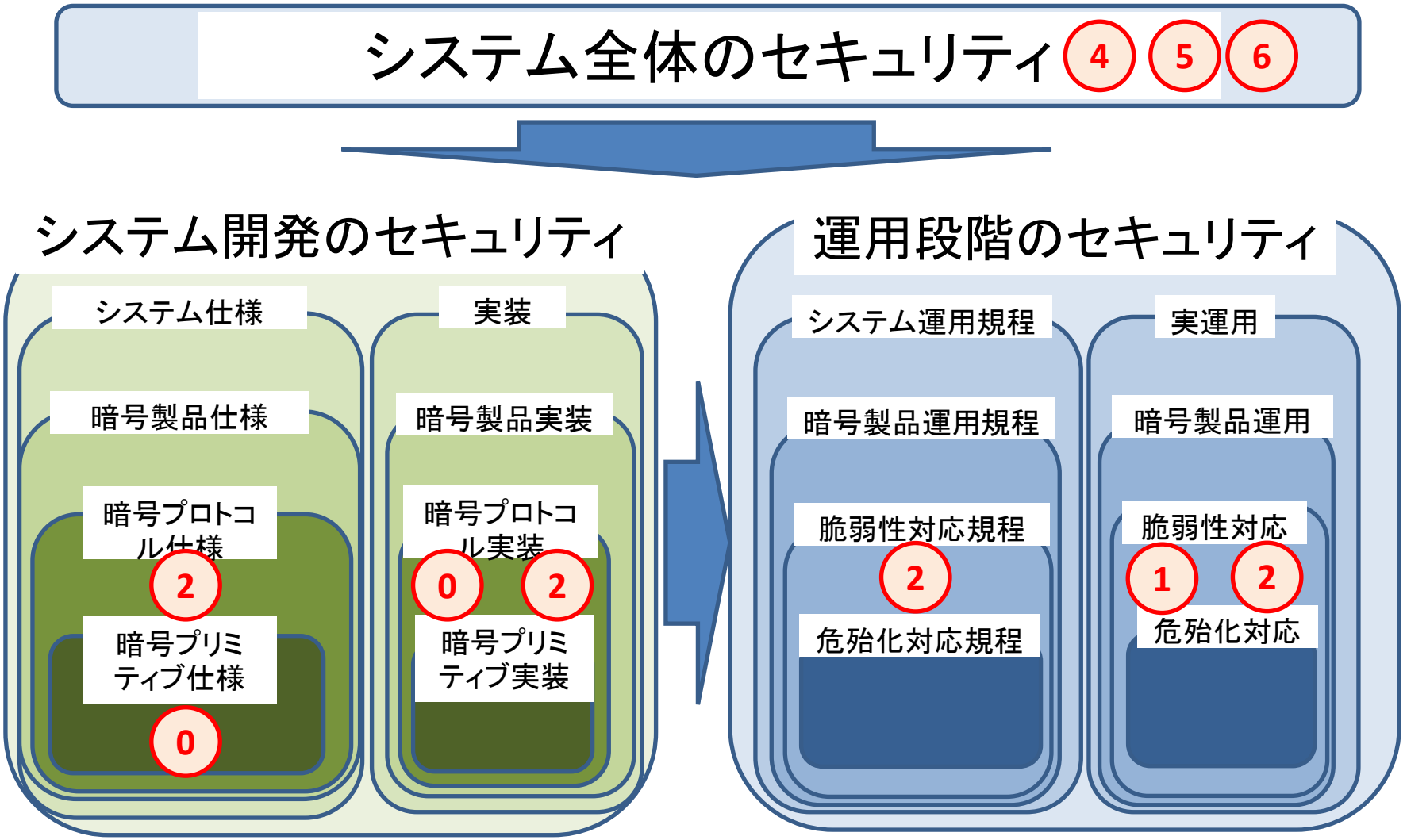
→JCMVP等との連携。今後対象のタスクがある程度具体化してからの議論。

来年度検討

時間の制約上今年度は検討方針のみ議論想定

2. 主な検討課題の全体俯瞰図におけるマッピング

（第4回CRYPTRECの在り方に関する検討グループ資料2「CRYPTRECの在り方に関する検討グループまとめ案」を元に作成）



3. 来年度の主な議題(案)

(1) 文書体系の在り方について

→CRYPTREC成果物の区分の仕方・構成、読者、CRYPTRECが扱うべき範囲等を議論。

(2) 政府統一基準に向けた新たなCRYPTREC成果物

→過去の成果物の検証及び、NISCの改定方針も踏まえた詳細な計画化が必要。

(3) 新たな社会ニーズを見据えた新規活動

→方向性をある程度事務局で整理した上で議論すべき。

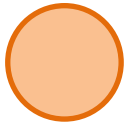
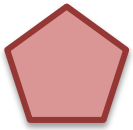
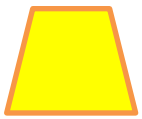
(4) 情報システム全体のセキュリティ確保を意識した他団体との連携

→JCMVP等との連携。今後対象のタスクがある程度具体化してからの議論。

(5) その他

→ChaChaの安全性評価の必要性の判断など、CRYPTRECとしてどう取り組むか議論が必要なテーマ。

4. 本年度のスケジュール

	2015年度 2月	3月	2016年度 4月以降
○暗号技術検討会		 第2回(3/29)	 2回程度 開催予定
○重点課題検討 タスクフォース	 第3回(2/3)		 数次 開催予定
○暗号技術 評価委員会		 第2回(3/8)	 数次 開催予定
○暗号技術 活用委員会		 第1回(3/2)	 数次 開催予定
○CRYPTREC シンポジウム			 調整中 6月開催 予定

参考資料1

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。

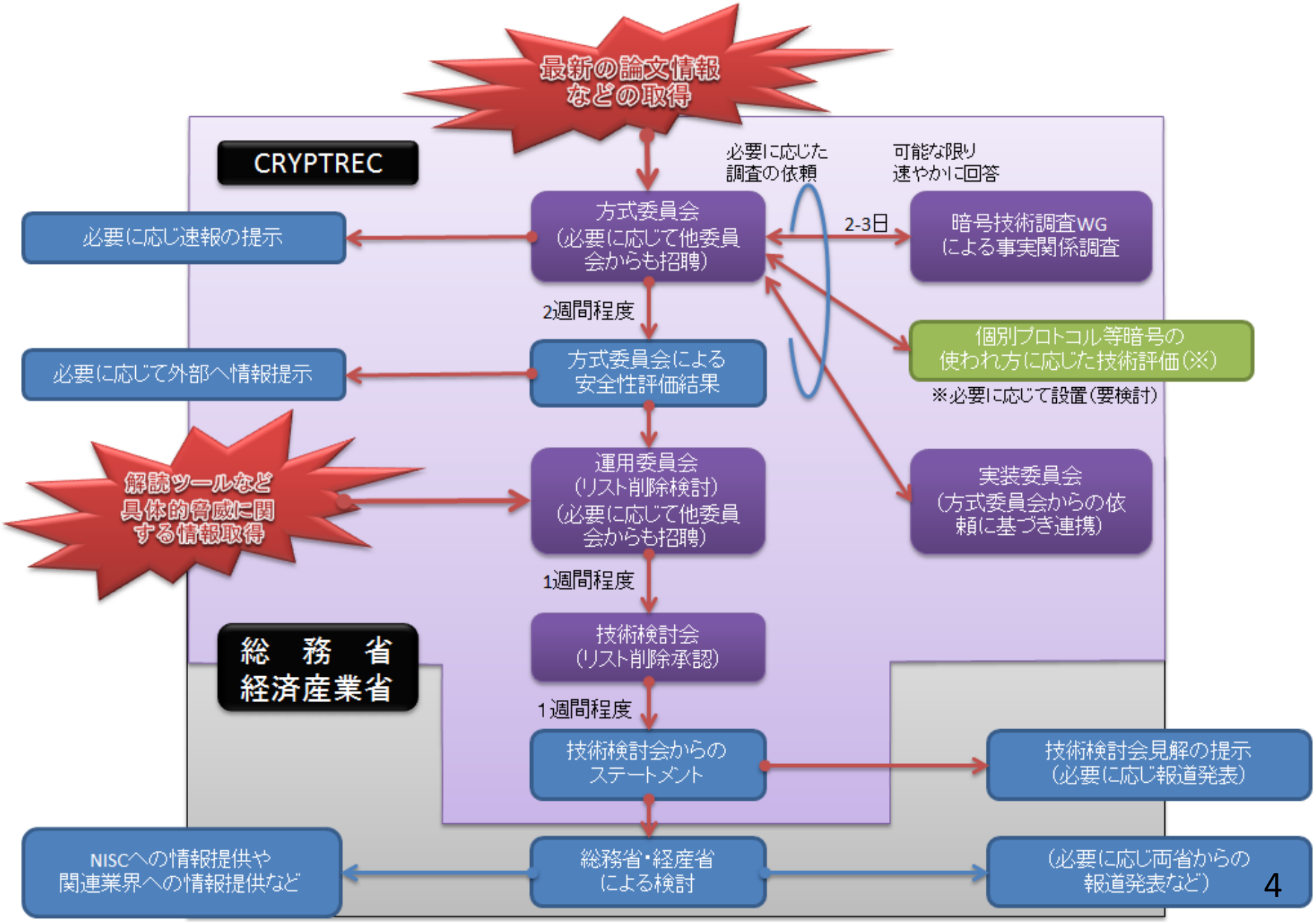
検討会及び各委員会の暗号危殆時対応（各委員会検討結果取りまとめ版）

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。

参考資料２

暗号技術検討会　2015 年度　報告書　目次（案）

目　　次