2011 年度第 1 回暗号技術検討会　議事概要

１．日時　平成 23 年 6 月 30 日（木）　16：00～18：00

２．場所　経済産業省別館 9 階　944 会議室

３．出席者（敬称略）

構成員：今井 秀樹（座長）、岡本 龍明、金子 敏信、国分 明男、佐々木 良一、寶木 和夫、近澤 武、
辻井 重男（顧問）、酒井 康行（松井 充代理）、松尾、真一郎、松本 勉、松本 泰、
米山 正夫

オブザーバ：木本 裕司、柳原 忠明（岡本 克己代理）、松宮 志麻（澤田 稔一代理）、
中山 紀雄（高地 圭輔代理）、舘野 圭悟（山崎 重孝代理）、
佐藤 真紀子（江原 健志代理）、荒木 美敬（中前 隆博代理）、
石井 貴光（寺岡 光博代理）、浜田 和之（松原 徳和代理）、
山中 豊（山本 雅亮代理）、坂下 圭一、近藤 玲子（高橋 幸雄代理）、
渡辺 創、矢島 秀浩、松宮 信行（鈴田 信代理）

暗号方式委員会事務局：田中 秀磨

暗号実装委員会事務局：大熊 建司

暗号運用委員会事務局：神田 雅透

暗号技術検討会（CRYPTREC）事務局：

総務省　武井 俊幸、中野 正康、水野 伸太郎、佐々木 伸行、谷岡 大祐

経済産業省　石黒 憲彦、山田 安秀、森川 淳、守山 速飛

４．配付資料

（資料番号）	（資　料　名）
資料１－１	2011 年度暗号技術検討会開催要綱（案）
資料１－２	暗号技術検討会の公開について（案）
資料２	2010 年度第２回暗号技術検討会メール審議の結果について
資料３－１	電子政府推奨暗号リストに関する考え方について
資料３－２	電子政府推奨暗号リストの考え方の明確化に向けた論点整理
資料４－１	暗号技術検討会活動計画（案）
資料４－２	暗号方式委員会活動計画（案）
資料４－３	暗号実装委員会活動計画（案）
資料４－４	暗号運用委員会活動計画（案）
参考資料１	暗号技術検討会構成員・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、経済産業省の石黒局長から開会の挨拶。

参考資料１に基づき、構成員及びオブザーバの交代の説明（苗村構成員→近澤構成員、櫻井構成員→松尾構成員、加藤構成員→持麾構成員、（警察庁）高橋氏→岡本氏）。新任の近澤構成員及び松尾構成員から挨拶。持麾構成員は欠席。

２）議事

（１）暗号技術検討会開催要綱等について

資料１－１及び１－２に基づき、検討会事務局から説明。質疑等なし。原案どおり了承。

座長として今井構成員を選出。顧問として辻井構成員を選出。

（２）２０１０年度第２回暗号技術検討会メール審議の結果について

資料２に基づき、検討会事務局から説明。質疑等なし。原案どおり了承。

（３）次期電子政府推奨暗号リストに関する考え方について

※石黒局長退席

資料３－１、３－２及び附属資料（構成員限り）に基づき運用委事務局から説明。

今井座長：運用委員会委員長から補足することはあるか。

佐々木構成員：特にない。

今井座長：質問をどうぞ。

金子構成員：多面的な検討が必要だろう。暗号アルゴリズムは送信側と受信側で同じものを搭載する必要がある。シナリオ１・２では「絞る」ということだが、シナリオ２とは「二つ（以上）の暗号を搭載しなければならない」ということなのか。だとすれば、調達者である政府のコスト増になる。多くのシステムに導入されていけば、そのうちコストも安くなるという見込みがあるのか。

運用委事務局：シナリオ選択後に運用についてはつめていく必要があると考えている。

金子構成員：シナリオ選択において、その後どのような運用がなされるのか、予め考えておくべき。

運用委事務局：その意味では、シナリオ１は米国標準暗号しか用いられていない現状を追認することになり、調達市場に対する影響はない。シナリオ２で複数の暗号搭載製品を調達すればコストアップになるが、国全体で使っていけば中長期的なコストダウンにはなっていくだろう。本検討会では「いたずらに多くない」を規範としてきて今に至るが、その解釈は立場によって異なることがアンケート結果で明らかになった。政府や提案ベンダーではその解釈は「たくさんある方が良い」であり、供給ベンダーの解釈は「１つ」が望ましい、である。供給ベンダーは１つに絞れば実装バグも少なく安全になり、多数の搭載製品を選択できるため、ベンダロックインになることもない、という立場である。

金子構成員：政府のコスト増は、税金を投入している以上、ひいては国民のコスト増になる。国民が高い製品を買わされる、ということは考えなければならない。電子政府の構築には、コストという観点も必要ではないか。

検討会事務局：誤解もあるように思う。シナリオ１・２の選択後には、実際にどのような選択基準で絞り込みをかけるかが重要で、調達コスト含め安全性以外の尺度も考慮すべきこととなる。シナリオ２では選択された暗号の推奨施策を検討していくことになるが、これには確かにコスト面の影響の検討が必要である。

佐々木構成員:前提として､電子政府推奨暗号リストは掲載暗号を全て搭載した製品しか認めない、というものではなく、どれかを搭載している製品であれば調達して良い、というものだと認識している。一方で、国として国産暗号をどのように普及・推奨していくかや、国民のコストについても考えていかなければならないと考える。

今井座長：確かに、コストも一つの観点として考えていかなければならないだろう。他に御意見はないか。

国分構成員：当方は IC カードが専門なので、仮に IC カードに適用するのであればどのような影響があるかを考えていた。例えば電子パスポートでは世界的に電波のインタフェースがＡタイプとＢタイプが併存しており、結果としてリーダはＡ、Ｂどちらのタイプも読めなければならない。社会保障カードをこれから全国民に配付することも報じられているが、現実に即したアルゴリズムの選択の議論があっても良いのではないか。

今井座長：そのとおりだと思う。どのシナリオが良いのか、率直に意見をもらえないか。順番にお願いしたい。

米山構成員：４つのシナリオのうちなら、シナリオ２となる。ユーザーの視点からは、調達容易性が重要で、数の議論はあるだろうが、選択と集中が必要だろう。セキュリティの強化という観点からはコメントできない。

松本（泰）構成員：シナリオ２が現実的だと考える。電子政府推奨暗号リストは、策定から 10 年を経て、状況が変わっていることを認識しなければならない。

松本（勉）構成員：自分自身は 10 年前から絞るべきと主張してきたので、シナリオ２を強く主張したい。国内の研究体制の問題で言っても、シナリオ４を選択したからといって、生き残れるというものでもない。国内の技術開発、知見の蓄積という観点からも、シナリオ２が矛盾するものではないだろう。

酒井構成員代理：シナリオ２を推したい。日本政府の調達において、米国標準暗号だけというシナリオ１を国として推すことは考えにくい話ではないのか。ただ、２でも危殆化したときにリストから取り除くルールと同様、新しい暗号が入る余地を確保し、そのルールづくりが必要だろう。

松尾構成員：安全性の観点からも、シナリオ２を推したい。国産暗号を推奨していくためには、電子政府推奨暗号リストをベースにして、ISO や IETF といった土俵で勝負していく必要があるが、どのアルゴリズムをナショナルボディとして推奨するのか絞らなければ、相手にされないだろう。

寶木構成員：ISO の場でも絞る、という同様の議論がなされており、CRYPTREC の活動も注目されている。ISO では日本も絞るという意見を提示し、シナリオ２が一番整合性があるものと思う。

なお、ISO ではリストはユビキタスな暗号、マルチ・パーパスな暗号、歴史的価値の暗号に３分類している。ただ、アルゴリズムを幾つに絞るかは同様の議論が必要で、暗号の技術的摩耗が通常 5～10 年だと考えると、１＋Ｎの Ｎを具体的に考えていかなければならない。

辻井顧問：寶木さんの意見にはなるほどと思う。どれかと言われれば、シナリオ２だろう。趣旨としてはシナリオ３も良い。国民のコストという観点は確かに必要で、公的個人認証にしてもコストの議論抜きにはできない。広い視野をもって取り組まないと、韓国に対しても遅れているこの現状を打破することはできないだろう。認証の分野に関して言えば、法律を改正していき日本も電子政府の推進に行政が一体となって取り組んでいかなければならない。災害への不安に対して総合設計して取り組めば、長期的なコストも下がっていくだろう。

佐々木構成員：シナリオ２だと考える。どのような選択基準で絞り込むかは十分な議論が必要で、利用実績だけか、それとも何かしらの技術評価を含めることも考え得る。技術評価を実施することには、一度「安全」という評価をした掲載暗号に対して、再度評価を行うことの是非の議論もある。そして、国産暗号を推奨といっても、どの対象に実装していくのかで強さや性能が決まってくる話で、選択基準づくりは、多角的に検討していかなければならない。

近澤構成員：SC27/WG2 コンビーナの立場からは、寶木さん同様にシナリオ２を推したい。補足すると、日本の技術力は高いが韓国・ロシアでは自国の暗号を一本に絞り込んで強力に暗号アルゴリズムを推奨してきて、日本は国内標準ではない暗号をバラバラと推奨して技術力とは関係ない部分で存在感を示せていない。１＋Ｎの話があったが、国際の土俵では、国産暗号Ｎを一つに絞ってアピールすることが一番強い。

国分構成員：シナリオ２が良いだろう。システムインテグレータ（SIer）の立場で考えると、調達時にリスト内に順序がなく、フラットにどの暗号でもかまわない、となれば米国標準暗号を採用するだろう。国産暗号を推奨するのであれば、調達時の点数を高くするなど、何かしらのインセンティブが必要だと思える。また、新しい暗号を採用するとなれば不安もあるので、信頼性に関するサポート体制も検討されるのではないか。実際の運用においては、様々な工夫が必要になると思う。

金子委員：絞る方向には基本賛成したい。ただ、リストの扱いについては注意が必要と考えている。あくまでも、この中から一つを使えば良い、というリストであるべき。また、強制力をもって国産暗号を搭載させることは避けるべきではないか。その意味では、シナリオ２か３を推したい。

岡本構成員：リストの考え方については、この中から搭載する暗号を選ぶもの、というように考えていた。それを前提とすれば、シナリオ２を推したい。絞り込む数については議論が必要。アプリケーションによっては複数のアルゴリズムを搭載していて良いのではないか。また、選択基準については、統計的に一番利用実績があるというだけでなく、CRYPTREC としては技術的な観点からの絞り込みをするべきなのではないか。

今井座長：皆さんの意見はシナリオ２でまとまったものと思う。一方で、運用方法、リストの分類等については議論していくことになるだろう。今日は大きな意思の決定となった。一方で、シナリオ２でも研究体制は重要な課題であり、国内技術力が低下すれば暗号アルゴリズム

の技術評価もできない。基礎研究については、国としても努力してほしいと思っている。国としての見解はいかがか。

山田室長：研究・評価だけではなく、経済産業省と総務省が今までどのような観点で検討してきたのか説明したい。2003 年に今のリストを策定してから、実際どのような暗号アルゴリズム搭載製品が電子政府で調達されてきたのか、リストに多数の暗号アルゴリズムが掲載されることが、セキュアな調達の推進になっていたのか、多数の暗号が掲載されたリストが諸外国にどのように見られていたのか、また外国暗号だけで国の安全保障を確保できるのか。まずは基本方針を置き、細かいところを埋めていく段取りが必要だと考え、シナリオ２が良いと思ってきた。一方で、実際の適用領域や、研究体制の確保についてはきちんと議論していきたいと考えている。ただ、そのような推進策や保全策なしにシナリオを選択できない、というのは言わないでほしいと考えている。

今井座長：シナリオ２で決定する。運用方法等については、これから CRYPTREC できちんと考えていくことにする。

（４）2011 年度の活動計画（案）について

資料 4-1 に基づき、検討会事務局から説明。

①暗号方式委員会活動計画

資料 4-2 に基づき、方式委員会事務局から説明。

辻井顧問：CRYPTREC の範囲外の課題だと思うが、想定外をどう想定するかが一つのキーワードになっていると思う。暗号アルゴリズムの危殆化の際に、産業に対してどのようなダメージがあるのか、政府全体で考えてほしい。

今井座長：政府全体とともに、CRYPTREC としてもある程度考えていきたい。リスクに対する考え方は、日本は甘かったものと考える。

②暗号実装委員会活動計画

資料 4-3 に基づき、方式委員会事務局から説明。質疑等なし。

③暗号運用委員会活動計画

資料 4-4 に基づき、方式委員会事務局から今回の検討会でのシナリオ２決定を踏まえて取り組んでいく旨、説明。質疑等なし。

（５）その他

木本参事官：方式委活動計画で辻井顧問からも言及があった件にも関連して、２点説明・報告したい。１番目は緊急時対応計画（コンティンジェンシープラン）であり、各省庁でつくるように昨年の本検討会で議論し、実施することとなった。CISO 等連絡会議でアラートの発報

を検討し、緊急時には、電子政府の手続きを止めて紙ベースでの申請届出に戻すことなどを検討することが、その骨子である。ただ、国民への影響を最小限にとどめるため電子政府を止めないよう、代替暗号を搭載した製品をもって電子政府を構築してほしい、とは考えている。２番目は、平成 22 年度からの情報漏えいへの関心の高まりである。米国では 2010 年に暗号移行を行うことに関して、我が国の国会で質問主意書の提出が 11 月、12 月にあり、電子政府推奨暗号リストに基づいて粛々と移行する旨を回答した。移行時期については、2013 年で良いのか、トップ 100 の計算機の性能は、以前に CRYPTREC でご評価いただいた見通しが正しいことを裏付けているが、CRYPTREC の高い知見を引き続き頂き、助言を請いたい。

辻井顧問:しっかりやっていただいていることは分かった。危殆化時にどのような被害が出るのか、想定・シミュレーションしていく必要がある。

３．閉会

総務省の武井審議官から閉会の挨拶。

事務局から、次回会合の日程、場所等については別途連絡する旨、連絡。

以上