第２回　CRYPTREC の在り方に関する検討グループ　議事概要

１．日時　平成２７年６月２４日（水）　１８：３５～２０：４０

２．場所　経済産業省別館１階　１０１－２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、盛合志帆

事務局：総務省（赤阪晋介、筒井邦弘、中村一成）

経済産業省（上村昌博、上坪健治、中野辰実、中村博美）

４．配布資料

（資料番号）	（資　料　名）
資料１－１	第１回議事概要（案）
資料２	「CRYPTREC に関する問題意識」（上原構成員）
資料３	「暗号プロトコル評価技術コンソーシアム(CELLOS)の概要」（手塚構成員）
資料４	「サービス視点からの暗号技術(の重要性)」（松本泰構成員）
参考資料１	CRYPTREC に関する現状について（第２回会合版）

５．議事概要

１　開会

事務局から開会の宣言があった。参考資料１に関して、前回会合での構成員意見を追記した旨説明があった。

２　議事

（１）前回議事確認と本日の議論の進め方について

前回議事概要については、文書の体裁についてコメントがあり、事務局が修正のうえ後日再度構成員にメールにて展開することとなった。

（２）CRYPTREC に関する問題意識

資料２に基づき、上原構成員より説明が行われた。

（３）暗号プロトコル評価技術コンソーシアム(CELLOS)の概要

資料３に基づき、手塚構成員より説明が行われた。

（４）サービス視点からの暗号技術（の重要性）

資料４に基づき、松本泰構成員より説明が行われた。

（５）全体を通しての意見交換

議事（２）～（４）までの発表に対して行った意見交換の内容は以下のとおり。

〇意見交換

①上原構成員プレゼンに対する質疑

松本座長：ガイドラインに附版したり小さい単位に分割したりといった利便性向上のための工夫を行うべきという提案には、全く同感である。これらの工夫はガイドラインの改定に当たっても便利である。CELLOS に一部機能を委譲するという資料の記載中、CRYPTREC が情報の正確性を追認するとあるが、具体的にどのようなイメージか。

上原構成員：CELLOS 等が速報性を重視して情報発信を行うが、調達の仕様等に使うためには正確性の担保がない。議論が固まった段階で、CRYPTREC として情報の正確性を追認するイメージである。

手塚構成員：調達要件として標準が採用されることも多い。欧州では ETSI で盛んに標準化が行われているのに対し、日本でも JIS などの標準規格で暗号を上手くひも付けできないか。

松本座長：例えば米国の調達では FIPS が仕様を定め、CMVP が製品を指定している。日本の調達では、調達のための参照規格や基準という意味で、暗号に関わる部分は後発であり、あまり整備されていない。

上原構成員：日本は標準化にかけているリソースが欧州と比較して少ないと感じている。国際標準化と調達の関係では、デジュール標準以外の規格を仕様に入れると非関税障壁扱いとなってしまうという問題もある。

近澤構成員：情報セキュリティは安全保障に関係してくるため、特に国際標準を使う必要はないという考えもある。

松本座長：いずれの場合であっても、調達の部分毎に標準やリストといった参照すべき文書が用意されているが、網羅的でないという問題があるのだと思う。

太田構成員：資料２の最後から２頁目の「設計上の安全性の確保」はどういう意味だったか。

上原構成員：実装物の安全性確保は JCMVP 等に頼るとして、アルゴリズムやプロトコルといった仕様の部分はこれまで CRYPTREC が担当してきており、その部分でもまだ「認証プロトコル」等の取り組むべき課題がある、ということ。暗号を基礎とする部品の安全性について、現在足りない部分に注力するべきではないかと考える。暗号の安全性についても当然従来どおり注力するべき。

盛合構成員：CRYPTREC では、仕様だけでなく実装の安全性確保も重要であるという議論があり、暗号モジュール委員会や JCMVP の立ち上げに繋がった。CMVP の製品数が大きく増えているのに対し、JCMVP の製品数があまり伸びていないと感じる。JCMVP の認

定を調達の必須条件にすれば利用が進むと思うが、今後の展望についてどう考えるか。

上原構成員：プロトコルや認証方式（パスワード認証の要件等）にも広げられるのではないか。本当はもっと JCMVP の製品が参照されるようになればいいが、今は不十分と感じる。

手塚構成員：仕様の部分は仕様のリストで規定し、実装の部分は製品リストから製品を選ぶ形が望ましい。複数社が同じ仕様に基づいて作成しても、ある社の製品は安全性に疑問があるといったことがあり得るので、調達の要件としては仕様のリストで規定する一方で、実際に選択する製品群は製品のリストの中から選び、それ以外のところから選ばないようにすることが必要。

松本座長：JCMVP では、使用して良い暗号アルゴリズムは JCMVP Approved のものとなっており、電子政府推奨暗号リストに掲載されている暗号技術は当然対象であるが、他のものも入れることができる。CRYPTREC よりスコープが広いので、CRYPTREC で評価していない暗号については、独自で評価を行う必要が出てくるが、我が国における暗号専門家の人材リソースが限られていることを考えると、色々と改善の余地がある。

松本泰構成員：資料４の参考の部 60 頁に CMVP と JCMVP の比較を書いている。日本のベンダ数が米国に比べ少ないということもあるが、情報セキュリティ製品の競争力の縮図とも言えるかもしれない。

松本座長：調達における強制力の有無がやはり大きいのではないか。

②手塚構成員プレゼンに対する質疑

近澤構成員：CELLOS は、脆弱性情報が発表されてから１，２日後にはレポートが掲載されており CRYPTREC でも見習いたいところだと感じているが、何人ぐらいで作業し、どのような承認プロセスを取っているのか。

手塚構成員：中心的な数人がドラフトを作成し、メーリングリストでの審議を経て、最終的に私や、WG リーダーの松尾氏が判断する形となっている。

松本座長：CELLOS の活動対象としている「プロトコル」はどういったものをいっているのか。

手塚構成員：CELLOS で活動の対象としているプロトコルとは、主に標準化団体が規定しているプロトコルで、具体的なコードも含むが、主に仕様レベルである。実装レベルまで確認することはリソース的に難しい。例えば、形式的手法による評価の実績は、３種類のツールを使って 33 個のプロトコルを評価した。活動を通じて見えてきたものとしては、標準化団体における認定のスキームが必ずしも十分ではないということ。標準化に際してしっかりと評価手法を導入していくことを推進していきたいと考えている。プロトコルの評価と脆弱性情報に対する対応が活動の大きな２本柱といえる。

松本座長：CELLOS は、大変有能な方々が集まっていることは理解したが、現時点ではまだ、組織として作業を発注できるような体制はとれていないと理解してよいか。

手塚構成員：現時点ではそのとおり。

松本座長：CELLOS の活動を引き続き継続していくにあたって、人的資源確保のためにうまく連携していけないかと思う。若い人材も巻き込んでいった方がよい。継続的な活動としていくために、CRYPTREC との協力範囲を明確にして役割分担を行えば、より一層活動が広がっていくのでは。

手塚構成員：プロトコルの部分は CELLOS で評価し、純粋に暗号アルゴリズムに関する部分は CRYPTREC で評価するという役割分担の構造ができると CELLOS にとってもありがたいところ。CELLOS 内では、脆弱性の速報を作成する人やプロトコル評価をする人など、それぞれの得意な分野を活かして役割分担はできている。ただ、ボランタリーな活動に基づいているので、仕事として活動に参加できるようになるとよい。また、CRYPTREC との連携としては、CELLOS の速報情報のページへのリンクを CRYPTREC のウェブページに貼るようなことでも十分に意義がある。プロトコル評価結果知識データベースを拡充し、海外にも発信していきたい。また、海外の人材もどんどん巻き込んでいきたいと考えている。

<u>③松本泰構成員プレゼンに対する質疑</u>

手塚構成員：資料８頁の「標準化」はどのような意味か。

松本泰構成員：例えば ETSI の標準化は、欧州の競争力を念頭においた活動であると認識しているが、技術標準の仕様だけでなく、相互運用性の確保や法制度との調整なども行っている。そのような広い意味での「標準化」活動だと考えているが、これは欧州における電子政府の活動にも深い関係がある。

盛合構成員：これまでの CRYPTREC は、過去の取組や電子政府という枠組に囚われすぎる傾向があったと思う。今後、CRYPTREC の活動範囲を広げていくのであれば、こういう風に変わります、ということをもっと打ち出して行く必要があると感じた。

松本座長：そのとおり。

松本泰構成員：HIPAA は、米国の医療分野の個人情報保護法にあたるものであり、保護医療情報（PHI）等の守る対象について規定しているが、暗号技術等によりの「どうやって守るか」に関しては、個別に記述している訳ではなく NIST が発行している技術ガイドラインを参照している。米国においては、包括的な個人情報保護法は存在しないが、技術ガイドラインについては、このように共通のものが参照されている。日本では、包括的な個人情報保護法が存在するが、それぞれの主管省庁ごとに業界にあったガイドラインを作成している。技術ガイドラインについては、米国において NIST のガイドラインを参照しているように、統一的な技術ガイドラインが参照するべきではないか。現在の主管省庁ごとの個別のガイドラインが技術的に必ずしも全て練られているとは思えない。

松本座長：その意味では、鍵管理なども同様の例。IoT において鍵管理は重要であるが、

CRYPTREC において鍵管理に関する文書はない。従っておくべき事項を規定する文書があり、かつ、その文書に沿って、実装されているかまでチェックできることが理想的だがまだまだ困難である。NIST が膨大な資料を作成してはいるが、それはあくまで米国モデルのものであるが、日本でも NIST の翻訳版で良いかは疑問があり、しっかり吟味する必要がある。

手塚構成員：CRYPTREC の活動範囲を実装などの方向に広げるのであれば、それらのレイヤーに知悉したベンダのシステムエンジニアなどの人をもっと巻き込むべき。CRYPTREC は今後、社会において暗号技術がどう活用されていくか議論し、活動範囲を自律的に決定していくべきであり、暗号よりもっと広い視野に立つ上位のレイヤーからインプットを受けて活動する構造になった方がよりよい。

松本座長：暗号技術を部品単位で評価する体制は整っているが、鍵管理、トラスト構築といったより上位のレイヤーについても CRYPTREC の活動範囲としていくべき。

手塚構成員：そのとおり。そのレイヤーの議論が不十分であり、部品レベルの議論のあと、いきなりアプリケーションや調達のレイヤーに議論が飛んでしまう。

事務局（経済産業省）：松本泰構成員の発表にもあるように、クラウドサービスやプライバシー保護等における暗号技術の応用についての検討は社会的な関心も高い。

松本泰構成員：Data at Rest において、日本では、暗号鍵を消去することでデータを消去するという手法が制度上明確でないことが、技術開発を促していない面がある。今後有望な技術だと考えられる Data in use のプライバシー保護データマイニングについても法制度との調整が考慮されないと技術開発の発展を阻害する可能性があるかもしれない。

事務局（総務省）：NIST のガイドラインのうち Data at Rest の分類にあるものは、内容によっては日本でも取組やすいものがあるのではないか。

松本泰構成員：CCRA に用いる PP と同様の記載であるので、日本にも文書としては存在する。ただ、基準を満たす製品の導入が進んでいない。

３　閉会

松本座長より、第３回会合について、近澤構成員と盛合構成員によるプレゼンを依頼した。また、議論の進め方として第３回で CRYPTREC の今後の活動の方向性について検討し、第４回でとりまとめを行う旨説明があった。

事務局から、第３回及び第４回の日程について連絡があった。