２０１５年度　第２回暗号技術検討会　議事概要

１．日時　平成 28 年 3 月 29 日（火）　16:30～18:30

２．場所　経済産業省別館 1 階　104 各省共用会議室

３．出席者（敬称略）

構成員：松本勉（座長）、今井正道、宇根正志、上原哲太郎、太田和夫、岡本栄司、金子敏信、近澤武、手塚悟、本間尚文、松井充、松本泰、向山友也、渡邊創

オブザーバ：太田裕介（坂本三郎　代理）、加藤誠司（橋本道雄　代理）、後藤怜（松永一義　代理）、下地邦寿（溝口浩和　代理）、平和昌、寶木和夫、竹内英二、中村武英（村田利見　代理）、西村敏信、野口広明（橋本敬史　代理）、頓宮裕貴、渡邉実（中山　隆介　代理）

CRYPTREC 事務局：盛合志帆（国立研究開発法人情報通信研究機構（NICT））、大久保美也子（NICT）、神田雅透（独立行政法人情報処理推進機構（IPA））

暗号技術検討会事務局：総務省　池永敏康、筒井邦弘、丸橋弘人、今野孝紀
経済産業省　竹内芳明、上坪健治、中野辰実、中村博美

４．配付資料

（資料番号）	（資料名）
資料１	2015 年度 暗号技術検討会報告書（案）
資料２	2015 年度 暗号技術評価委員会活動報告
資料２別添１	64 ビットブロック暗号 MISTY1 の安全性について（続報）
資料２別添２	SHA-1 の安全性について
資料２別添３	2015 年度 暗号技術調査 WG（暗号解析評価）活動報告
資料２別添４	2015 年度 暗号技術調査 WG（軽量暗号）報告
資料２別添５	暗号技術ガイドライン（軽量暗号）作成方針
資料３	2015 年度 暗号技術活用委員会活動報告
資料４	CRYPTREC 暗号リスト（推奨候補暗号リスト）への新規追加について（案）
資料４別添１	CRYPTREC 暗号リスト変更案
資料５	2016 年度 暗号技術評価委員会活動計画（案）
資料６	2016 年度 暗号技術活用委員会活動計画（案）
参考資料１	2015 年度 第 1 回暗号技術検討会議事概要
参考資料２	2015 年度　暗号技術検討会　構成員・オブザーバ名簿
参考資料３	「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

参考資料４－１　　CRYPTREC 暗号技術活用委員会の今後の活動に向けて
参考資料４－２－１　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
参考資料４－２－２　暗号アルゴリズムの脆弱性に関する情報発信フロー
参考資料４－３　　暗号プロトコルのセキュリティ確保に向けた活動案

５．議事概要

１　開会

暗号技術検討会事務局から開会の宣言があり、総務省の池永敏康審議官から開会の挨拶が行われた。参考資料２に基づき、暗号技術検討会事務局より構成員の欠席（佐々木構成員、松浦構成員）について連絡があった。

２　議事

（１）2015 年度　暗号技術検討会報告書（案）について

資料１に基づき、「2015 年度 暗号技術検討会報告書（案）」の構成について暗号技術検討会事務局より説明が行われた。質疑はなし。構成については、原案のとおり承認された。

（２）重点課題検討タスクフォース活動報告について

資料１の「３．２．重点課題検討タスクフォース」及び「４．今後の CRYPTREC の活動について」について暗号技術検討会事務局及び CRYPTREC 事務局より説明が行われた。質疑はなし。

（３）2015 年度　暗号技術評価委員会　活動報告について

資料２に基づき、CRYPTREC 事務局より説明が行われた。質疑応答は以下のとおり。原案のとおり承認された。なお、資料は誤植等の修正を行った上で公開する。

○質疑応答

宇根構成員：資料２別添１及び別添２について、レポート発行後に何か問合せはあったのか。

CRYPTREC 事務局：これまでのところ問合せはなし。

宇根構成員：資料２別添３の 4.5 Post-Quantum Cryptography への対応方針について、今後、CRYPTREC Report 等のドキュメントに記載される予定はあるのか。

CRYPTREC 事務局：第 2 回暗号技術解析評価 WG が開催されたのは、PQCrypto2016 開催直後であったため、今回は意見交換にとどまった。これから CRYPTREC 事務局にて検討する必要があるため、今年度の CRYPTREC Report に記載する予定はない。

（４）2015 年度　暗号技術活用委員会　活動報告について

資料３に基づき、CRYPTREC 事務局より説明が行われた質疑応答は以下のとおり。原案のとおり承認された。なお、資料は誤植等の修正を行った上で公開する。

○質疑応答

宇根構成員：CRYPTREC の在り方に関する検討グループ及び重点課題検討タスクフォースで整理したのは、暗号技術活用委員会の活動方針か、それとも活動目的か。

CRYPTREC 事務局：活動目的である。資料は「活動目的」に統一する。

（５）CRYPTREC 暗号リスト（推奨候補暗号リスト）への新規追加について

資料４に基づき、暗号技術評価委員会事務局より説明が行われた。質疑応答は以下のとおり。原案のとおり承認された。なお、作成日付の記載方法及び改定後の CRYPTREC 暗号リストの公開手続きについては暗号技術検討会事務局に一任することも併せて承認された。

○質疑応答

松本座長：SHA-3 は比較的早く推奨候補暗号リストに載せるための調整を進めることができた。しかるべき調査・評価が終了すれば、電子政府推奨暗号リストへの追加もありえる。

上原構成員：作成日は平成 25 年 3 月 1 日のままでよいのか。

暗号技術検討会事務局:今回は部分的に CRYPTREC 暗号リストに追加するものであり、暗号リストそのものの改定ではないため、作成日は平成 25 年 3 月 1 日から変更せず、変更履歴情報にて変更日付が分かるようにしたいと考えている。作成日と公開までの手続きについては、総務省、経産省における手続きに沿って対応したい。

松本座長：総務省、経産省に一任することとしたい。

（６）2016 年度　暗号技術評価委員会　活動計画について

資料５に基づき、CRYPTREC 事務局より説明が行われた。質疑応答は以下のとおり。原案のとおり承認された。

○質疑応答

實木構成員：SHA-1 の衝突事例が１つ発見された場合の影響はどう考えているのか。

CRYPTREC 事務局：具体的なケース次第。また、影響は SHA-1 の利用用途（署名生成、署名検証、HMAC など）によっても異なるだろうと考えている。

實木構成員：現状を理解せず SHA-1 を使用すると、被害を受けるアプリケーション

もあるという理解か。

CRYPTREC 事務局：発見された衝突のレベルによって対応は検討するが、「CRYPTREC 暗号技術ガイドライン（SHA-1）」のアップデートは必須であると考えている。

松本泰構成員：フリースタート衝突が発表された論文では、SHA-1 の証明書の発行はただちにやめるように、という記載だったが、それを追認すると、JPKI における 2015 年 12 月までの SHA-1 を使った電子証明書の新規発行を否定することになった。SHA-1 を使った JPKI の電子証明書の有効期間は最長 2018 年までであることも注意する必要がある。今後、2018 年までに SHA-1 の衝突発見の可能性もあるが、速報の発表等は、現在使用されている SHA-1 を使った電子証明書が、衝突発見に関するセンセーショナルな報道により、単純に否定されることのないように、実態を把握した上で行ってほしい。

松本座長：資料４－２－２のフロー図において、暗号アルゴリズムの脆弱性を検知した場合、技術的な問題としての対応は整理されているが、発表内容が利用者にどのような印象・影響を与えるかまでは考慮されていないため、今後検討が必要である。

太田構成員：暗号技術評価委員会としては、当該アルゴリズムの利用者へのメッセージは、利用方法をある程度予測してからでないと対応できない。

松本座長：自らのシステムで SHA-1 がどのように利用されているのか把握する必要がある。

金子構成員：本件は暗号の活用の議論でもあるため、暗号技術活用委員会での検討も必要なのではないか。

松本座長：CRYPTREC では、政府に CRYPTREC が発表する情報を受け取ってもらえるような発信方法を検討している。情報の受信側が「自分は関係ない」とならないように、情報の発信側と受信側との連携が必要。

松本座長：すぐに結論を出すことはむずかしいが、暗号アルゴリズムがどのように使われていて、どのようなリスクがあるかを発信していくことも必要である。

宇根構成員：重要インフラの脆弱性対応としては、暗号アルゴリズムの脆弱性等が発生した場合は、情報を入手した NISC から所管官庁及び当該重要インフラ分野のセプターを経由して各企業等に連絡される。そして、各企業等が社内システムでどのような暗号を使っているか調べ、内部調査を行った後に所管官庁や NISC に対して報告する義務がある。暗号アルゴリズムや暗号プロトコルの脆弱性に関する情報を発信する場合は、NISC 及び重要インフラ分野のセプターカウンシルと連携することが必要である。まずは、こうした脆弱性に関する情報の取扱いや対応の流れについて、NISC と調整・連携してから暗号技術評価委員会での検討に入ることが必要であると考えるので、そのようにお願いしたい。脆弱性への対応状況の報告等を早急に実施する必要がある事業者としては、NISC からの情報に、CRYPTREC

での検討状況が含まれているとありがたい。また、資料４－２－２のフロー図において、それぞれの対応にかかる時間の目安についても検討しておくことが有用である。

松本座長：CRYPTREC 関連会議には、NISC もオブザーバ参加しているので、連携して議論していきたい。また、フロー図の運用方法は内々で議論している。

暗号技術検討会事務局：NISC はインシデント対応で手一杯となっているのが現状である。SHA-1 の事例をきっかけとして、NISC から各府省庁、自治体等への情報発信に関する議論を行いたい。また、NISC とも連携し、政府としての情報発信について検討していきたい。

宇根構成員：量子コンピュータによる暗号危殆化の見通しについて、CRYPTREC としてどのような心構えでいるのか確認したい。

CRYPTREC 事務局：2016 年 6 月に開催予定の CRYPTREC シンポジウムにて量子コンピュータに関する招待講演を予定しているので、これを契機に議論を開始したいと考えている。

宇根構成員：多重線形写像と双線型写像についても検討をお願いしたい。金融業界では、クラウドを活用する動きが広がってきているが、クラウドで扱うデータが増加するほど、それらの不適切な取扱いによるデータ流出等の情報セキュリティ・リスクも増加する筋合いにある。そうしたリスク対策として、ペアリング暗号等、データを暗号化したまま各種処理を実現する、いわゆる「高機能暗号」が重要となってくると思う。クラウドをさらに活用していくという流れは政府機関においても同様であると考えられるので、こうした暗号技術のクラウドでの利活用についても暗号技術評価委員会にて検討してほしい。

CRYPTREC 事務局：多重線形写像及び難読化に関する最新動向については、次年度も有識者に外部評価を依頼予定であるため、その評価レポートをもとに検討していきたい。また、ペアリング暗号についても必要に応じて検討したい。

（７）2016 年度　暗号技術活用委員会　活動計画について

資料６に基づき、CRYPTREC 事務局より説明が行われた。質疑応答は以下のとおり。原案のとおり承認された。

○質疑応答

宇根構成員：資料６の①について。認証に暗号技術を使う時のガイドラインとして、2010 年に NISC から「オンライン手続きにおけるリスク評価及び電子署名・認証ガイドライン」が発行されたが、発行以降アップデートがなされていない状況である。このような既存ガイドラインのアップデートも暗号技術活用委員会の活動とすることを検討してほしい。

暗号技術検討会事務局：NISC のガイドラインは暗号技術だけでなく、認証方法やセキュリティ要件なども広く記載されているので、暗号技術活用委員会の活動範囲を超えていると思われるが、NISC とは連携していく。

松本座長：NISC のガイドラインについては、NISC から暗号技術に関連する知恵を出してほしいと要望があれば CRYPTREC として対応することになると思うが、重要なご指摘なので事務局から NISC に伝えてほしい。

宇根構成員：資料６の【参考】にある運用ガイドラインの作成を前提とした脆弱性情報の取扱いについては、暗号技術評価委員会にて整理された資料４－２－２のフロー図とも併せて議論してほしい。

CRYPTREC 事務局：ここでの脆弱性情報の取扱いの議論というのは、例えば、「Heartbleed のような個別製品に関わる脆弱性は取り上げないが、圧縮機能のような製品に共通した脆弱性は取り上げる」といった線引きの議論を指している。

暗号技術検討会事務局：今回はまず、暗号アルゴリズムの脆弱性の情報発信フローについて整理した。暗号プロトコルの脆弱性対応にまで範囲を広げた整理はこれから行っていきたい。

３　閉会

経済産業省の竹内審議官から閉会の挨拶が行われた。

暗号技術検討会事務局から、CRYPTREC シンポジウムの日程（平成 28 年 6 月 27 日 13:00-17:00）、CRYPTREC Report 2015 の発行予定日（平成 28 年 6 月を予定）、CRYPTREC 暗号リスト改定公表日（平成 28 年 6 月を予定）について連絡があった。また、2016 年度第１回暗号技術検討会は平成 28 年夏頃の開催を予定しており、詳細な日程、場所等については、別途連絡する旨の説明が行われた。

以上