２０１６年度　暗号技術検討会　議事概要

１．日時　平成 29 年３月 30 日（木）　15:00～17:00

２．場所　経済産業省別館　１１４各省庁共用会議室

３．出席者（敬称略）

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

オブザーバ：山本雅亮、岡野孝子（二宮清和代理）、國信綾希（阿部知明代理）、藤原茂樹（坂本三郎代理）、田中雅大（小川英俊代理）、下地邦寿（溝口浩和代理）、松本裕悟（二宮勉代理）、林良樹（坂本成範代理）、宮崎哲弥、寶木和夫、江口純一、大澤昭彦、西村敏信

暗号技術評価委員会事務局：盛合志帆（国立研究開発法人情報通信研究機構（NICT））

暗号技術活用委員会事務局：神田雅透、時田俊雄（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　今林顯一、大森一顕、酒井雅之、上東孝旭、丸橋弘人、今野孝紀

経済産業省　伊東寛、師田晃彦、市ノ渡佳明、森川淳

４．配付資料

（資料番号）	（資料名）
資料１	CRYPTREC の今後の体制（案）について
資料２	文書番号体系について
資料３	2016 年度　暗号技術評価委員会活動報告
資料３別添１	2016 年度　暗号技術調査 WG（暗号解析評価）活動報告
資料３別添２	2016 年度　暗号技術調査 WG（軽量暗号）活動報告
資料４	2016 年度　暗号技術活用委員会活動報告
資料５	SHAKE128 の推奨候補暗号リストへの追加について
資料６	ChaCha20-Poly1305 の CRYPTREC 暗号リストへの追加を視野に入れた評価について
資料６参考資料１	ChaCha20-Poly1305 の安全性評価について
資料７	KCipher-2 の仕様書について
資料７参考資料１	KCipher-2 の仕様書の変更について
資料７参考資料２	KCipher-2 の暗号技術仕様書（日本語版・英語版）の誤記について
資料８	SHA-1 に関する速報掲載について（報告）
資料９	共通鍵暗号の安全性調査と MISTY１について
資料１０	2016 年度　暗号技術検討会報告書（案）
参考資料１	2016 年度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

暗号技術検討会事務局から開会の宣言があり、総務省の今林政策統括官から開会の挨拶が行われた。その後、暗号技術検討会事務局より、岡本構成員、佐々木構成員、および手塚構成員が欠席である旨の連絡がなされた。

２　議事

（１）CRYPTREC の今後の体制（案）について

資料１に基づき、事務局より説明が行われた。質疑はなし。原案のとおり承認された。

（２）文書番号体系について

資料２に基づき、事務局より説明が行われた。質疑は以下のとおり。原案のとおり承認された。

○質疑応答

近澤構成員： 2016 年度の報告書を 2017 年３月に発行したとすると、文書番号末尾の数字はどちらになるのか。報告書のタイトルと違う年になるのであれば読者が混乱する可能性はないのか。

暗号技術活用委員会事務局：管理情報の番号については、従来年度で管理しているため、年度の数字を末尾に付けることを想定している。

松本座長：発行された日の年で良いのではないか。

近澤構成員：そうするとどちらかが間違っているのではないか、という誤解を招くおそれがある。

松本座長：この文書体系の説明文を一行付ければよいのではないか。

暗号技術活用委員会事務局：年度か発行年のどちらにするにしろ、統一すれば誤解を招くことはない。発行された日の年に統一する。

寶木オブザーバ：他組織と共同して文書を作成するとあるが、ここでいう他組織とは公的機関、民間企業等どういったところを想定しているのか。

暗号技術活用委員会事務局：公的機関だけでなく、民間企業やコンソーシアムも含めて想定しているが、具体的にどこか、というのがあるわけではない。例えば、車に関するガイドラインを作成する場合、その業界、コミュニティと連携しないとうまくいかないと考えている。

太田構成員：これは過去に発行した文書も対象となるのか。

松本座長：対象として付番されることになる。

（３）2016 年度　暗号技術評価委員会活動報告について

資料３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。

○質疑応答

宇根構成員：暗号解析評価 WG の報告資料５．３．に「今後の課題について」とあるが、今後評価委員会でどのように進めていくのか。

暗号技術評価委員会事務局：まず１つ目について。解析評価 WG は２年を単位として委員委嘱を行っており、今年度で２年の委員任期が終了した。来年度は PQC に特化して委員を配置し、検討を行っていく。２つ目について。確約はできないが、前向きに検討を進めていく。３つ目について。５．１．（１）に記載があるが、CRYPTREC 暗号リストに掲載されている DSA や DH の安全性については、素体 GF(p)から構成されており、素数 p のサイズが 2048 ビット以上であれば直ちに影響はない、ということからすぐには公表を行わなかったが、今後、注意喚起ではないが、お知らせという形で公表を行いたいと考えている。最後に４つ目について。10 年以上の長期の評価をどのようにしたらよいか、というのは問題を認識したので、今後の課題としたい。

金子構成員：安全性評価は 10 年の有効期間では足りず、20 年必要であるというのはそのとおりだと考えるが、一方で軽量暗号のようなニーズの異なる暗号もある。今後 CRYPTREC としてどちらを扱うのか、両方をめざすのかという方針を決めたらいかがか。

太田構成員：金子構成員の提案については、マンパワーにもよるため、今後検討したいと思う。

松本（泰）構成員：SHA-1 や RSA2048bit の移行は PQC（Post Quantum Crypto）の件にも関係する。PQC のアルゴリズムの議論が活発化してきているのは量子コンピュータ研究の影響であり、既存の暗号アルゴリズムがいつまで使えるかの判断がシビアになってきている。また、近年、IT 機器から産業機器へと暗号の組み込み先が移行してきている。産業機器だと 10 年では足りず、より長期に安全性が担保されることがクローズアップされてくると考える。例えば自動車など、リコール問題等も発生する可能性もあり、耐量子コンピュータ対策も含めて考える必要がある。

松本座長：今後の課題の対処方針については、メール審議で行う予定の来年度作業計画の審議のなかで明確化していきたい。

（４）2016 年度　暗号技術活用委員会活動報告について

資料４に基づき、暗号技術活用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。

○質疑応答

宇根構成員：表４－１で網掛けと網掛けではない部分の違いはなにか。

暗号技術活用委員会事務局：暗号プロトコル課題検討 WG にて、まずどういったものが必要かについて表４－１のとおりまとめ、その中でも重要なものとして網掛けされたものが表４－２にまとめられている。

太田構成員：表４－２にて、「安全性評価（暗号技術評価委員会への参考意見）」とあるが、評価委員会としてどのようなアクションを期待されているのか。

暗号技術活用委員会事務局：評価委員会にて評価をすべきである、といった強い意見ではない。

宇根構成員：表４－２を作成するに当たり、３月９日に公開されたＩＴ総合戦略本部・規制制度改革ワーキングチームの規制制度改革との連携による行政手続・民間取引 IT 化に向けたアクションプラン（「デジタルファースト・アクションプラン（仮称）」）中間整理は参考としたのか。

暗号技術活用委員会事務局：その公開日には課題検討 WG の最終回が終了していたため、参考としていない。

宇根構成員：このアクションプランでは、オンライン行政サービスの推進を説いており、ＡＰＩの整理を行い、民間のサービスと連携していくこと等が書いてある。具体的な検討課題として、主要手続のＡＰＩ公開の義務付けや、民間サービスにおけるマイナンバーカード、法人番号による認証などが挙げられている。最終的にどのようにとりまとめられるかは分からないが、政府としての方針が出されているため、こうしたものも参考にしながら、安全なＡＰＩを実現するためにベストプラクティスをまとめるのがよい。電子政府をより推進するために、ガイドライン（ベストプラクティス）を作成するときには是非連携してほしい。そのほか、金融分野では、ＡＰＩのオープン化について金融庁等を中心に検討が進められており、本年２月には、銀行がＡＰＩを開示しノンバンク企業等と接続する際のチェックリストの検討を行うＷＧをＦＩＳＣが立ち上げた。チェックリストは今年の夏頃を目途に作成していくこととなっており、こういったアウトプットも参考とするのがよいのではないか。

（５）SHAKE128 の推奨候補暗号リストへの追加について

資料５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。質疑応答はなし。原案のとおり承認された。

（６）ChaCha20-Poly1305 の CRYPTREC 暗号リストへの追加を視野に入れた評価について

資料６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。御意見は以下のとおり。原案のとおり承認された。

○質疑応答

上原構成員：元々私の意見で始まったことだが、評価委員会でしっかり安全性評価を行ってもらった。TLS1.3 の標準化が思ったよりゆっくりではあるが、今後も使用される状況は変わらないと考えられ、引き続き評価を行っていくのがよいと考える。

（７）KCipher-2 の仕様書の変更について

資料７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。質疑応答はなし。原案のとおり承認された。

（８）SHA-1 に関する速報掲載について

資料８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。

○質疑応答

上原構成員：SHA-1 の安全性低下については前から言われていたが、今回の件で電子証明書などの置き換えが進むというのはよいことだと思う。ただし、MAC の一部で SHA-1 がまだ使われており、特段インパクトはないと考えるが、SHA-1 がまだ使われている、ということを以て何か問題が起きないか若干懸念がある。CRYPTREC では、現在監視対象として移行の対象としているが、どういう条件であれば使ってもよいのか、あるいはこれ以上危殆化が進んだときにはどうするのか、といったところを考えなくてはならない。

松本座長：監視対象リストから外すということもありうる。

太田構成員：（上原構成員から指摘された SHA-1 の安全性低下に伴う利用方法への影響について、「CRYPTREC 暗号技術ガイドライン（SHA-1）」への反映方法についての検討を）承りました。

暗号技術評価委員会事務局：CRYPTREC で以前、利用目的に合わせてどれならまだ使えるかを示す SHA-1 のガイドラインを作成したが、今回の衝突発見の発表を受けて、改定に着手しようと考えている。具体的にどうしていこうという方針は言

えないが、引き続き検討していきたい。

（９）共通鍵暗号の安全性調査とMISTY1について

資料９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。

○質疑応答

宇根構成員：Ｐ８に、「審議の結果、１と４はない」とあるが、４はないとした理由はなにか。また、３と４の違いが分からない。３を選択した場合にリストを移行しないことの意味は何か。

暗号技術評価委員会事務局：これは委員からの意見であり、具体的な理由は伺っていない。事務局の見解としては、MISTY1 の全ての利用法について危険であるわけではなく、２の３２乗回の暗号化ごとに暗号鍵を変更すれば安全な利用が可能である。そうした意味で、その利用方法、利用時の注意点を提示するのが現実解だと思う。

宇根構成員：３は移行を推奨し新たな利用を推奨しないとするのであれば、電子政府での利用を推奨する「電子政府推奨暗号リスト」から監視リストに移すのが適切であると思う。

松本座長：あくまで評価委員会の審議のために４つの案が挙げられているのであり、今回選択肢を確定させ、このようにしたい、ということではなく、検討会に意見を求めている。MISTY1 については、ほとんど安全である、という見方と全数探索より僅かでも計算量が少なくなっているということをもって危険だ、とする見方もある。今後も同様の事態は起きると考えており、しっかりと議論されるべきである。

松井構成員：今日はあくまで意見を出す場として理解してよいか。

松本座長：そのとおり。今回いただいた意見をもとに、評価委員会でまたどのようなアクションを取るべきか審議をしていただく。

松井構成員：６４ビット暗号をどうするかについて、今後軽量暗号など、様々なところで同様の話がでてくると思う。Ｐ６の結論にあるが、それぞれの判断ということとなり、短い言葉で表すのは難しい。こうだから、こうというのは言えない。

松本座長：軽量暗号については、今般ガイドラインを作った。CRYPTREC 暗号リストに掲載するのではなく、ガイドラインを作成することにより、軽量暗号の利用ニーズに対応したが、６４ビット暗号自体がどうなのかという話と、CRYPTREC 暗号リストとしてどう扱うか、という話があると思う。

暗号技術評価委員会事務局：先ほどの３と４の違いは何かという質問に関連するが、

６４ビット暗号を全てリストから落とすことにも繋がる可能性があるため、一概に全て同じ、とはとらえないでほしい。

松本座長：それではいただいた意見をもとに、引き続き評価委員会で検討を進めていくこととする。

（10）2016 年度暗号技術検討会報告書（案）について

資料 10 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。質疑応答はなし。原案のとおり承認された。

３　閉会

経済産業省の前田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次回暗号技術検討会は来年３月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