２０１３年度　第２回暗号技術検討会　議事概要

１．日時　平成２６年３月２７日（木）　１４：００～１５：３５

２．場所　経済産業省別館１階　１０４各省庁共用会議室

３．出席者（敬称略）

構成員：今井秀樹（座長）、上原哲太郎、太田和夫、岡本栄司、岡本龍明、国分明男、佐々木良一、武市博明、中山靖司、本間尚文、高島克幸（松井充構成員代理）、松尾真一郎、松本勉、松本泰、向山友也、渡辺創

オブザーバ：奥山剛、根本農史（佐藤正明 代理）、堤紀代子（稲垣浩 代理）、江森久子（野口宣大 代理）、楢木野由善（大村周一郎 代理）、郷敦、岩下守男（三富則江 代理）、岩永敏明（辻本崇紀 代理）、木村和仙、平和昌、寶木和夫、伊藤毅志、山岸篤弘（亀田繁 代理）、西村敏信

暗号技術評価委員会事務局：盛合志帆（独立行政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（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　吉田靖、赤阪晋介、飯田恭弘、河合直樹、中村一成

経済産業省　大橋秀行、上村昌博、中谷順一、室井佳子

４．配布資料

（資料番号）

資料１	2013 年度　暗号技術評価委員会活動報告
資料２	2013 年度　暗号技術活用委員会活動報告
資料３	2013 年度　暗号技術検討会報告書（案）
資料４	2014 年度　暗号技術検討会活動計画（案）
資料５	2014 年度　暗号技術評価委員会活動計画（案）
資料６	2014 年度　暗号技術活用委員会活動計画（案）
参考資料１	2013 年度　第１回暗号技術検討会議事概要
参考資料２	CRYPTREC 暗号技術ガイドライン（SSL/TLS における近年の攻撃への対応）
参考資料３	CRYPTREC 暗号技術ガイドライン（SHA-1）
参考資料４	電子政府における調達のために参照すべき暗号のリスト
参考資料５	2013 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

経済産業省の大橋審議官から開会の挨拶が行われた。参考資料５に基づき、暗号技術検討会事務局よりオブザーバの交代（(警察庁）羽室氏→佐藤氏、(法務省）佐藤氏→野口氏、(外務省）中村氏→大村氏）及び構成員の欠席等（松井充構成員の代理として高島克幸氏が出席、金子敏信構成員、近澤武構成員は欠席）について説明が行われた。

２　議事

（１）2013 年度 暗号技術評価委員会活動報告

資料１に基づき、2013 年度暗号技術評価委員会の活動報告について、暗号技術評価委員会事務局から説明が行われた。質疑応答は以下のとおり。

〇質疑応答

佐々木構成員：暗号技術ガイドライン（SSL/TLS における近年の攻撃への対応）はいつ公開されるのか。本ガイドラインを通じて RC4 の脆弱性について周知することは重要である。ブロック暗号の CBC モードに脆弱性があるために RC4 の使用を推奨している場合があるようで、相談を受けたことがある。その時は RC4 の使用はやめた方がよいのではないかと助言したが、このように暗号の専門家でも RC4 を使用しようとすることがあるため、必ずしも正しい理解が広まっていないのではないと危惧している。

暗号技術評価委員会事務局：今回作成したガイドラインは、TLS1.0、1.1、1.2 でそれぞれどのパッチが当たっているのか、どのバージョンなら RC4 の使用が許容されるのか、TLS1.2 なら GCM のような認証暗号が利用できるオプションがきちんとついている、といったことをバージョン別に記載しており、有用なもの。可能な限り早い時期の公開を予定している。

今井座長:乱数については､CRYPTREC暗号リストの技術項目には含まれていないものの、使い方を間違えると大変なことになる。どのような事例があるか簡単に説明してほしい。

暗号技術評価委員会事務局：乱数については、楕円曲線に関連してクローズアップされていたが、それ以外にも、乱数の生成方法について生成が上手くいかなかった時にどのようなことが起こるかという話題で出てきている。暗号技術ガイドラインの来年度の重要なテーマとして検討していきたい。

今井座長：軽量暗号はいろいろと検討していただいているが、デバイスの進歩を十分考慮に入れなければならない。

本間構成員：ご指摘のとおり。小型デバイスに通信機能を持たせる場合、最先端のプロセスを使うことはできず、いわゆる枯れたプロセスを使うことになる。そこに軽量暗号を使う場合、実装面積が非常に小さくて済むため、大きなアドバンテージがあると認識している。

（２）2013 年度 暗号技術活用委員会

資料２に基づき、2013 年度暗号技術活用委員会の活動報告について、暗号技術活用委員会事務局から説明が行われた。質疑応答は以下のとおり。

〇質疑応答

今井座長：作成中の運用ガイドラインについて、暗号技術評価委員会の結論と相違があるとのことだが、具体的にどういうことか。

暗号技術活用委員会事務局：暗号技術評価委員会というよりは、CRYPTREC 暗号リストとの相違である。現在の CRYPTREC 暗号リストはアルゴリズム名で記載されており、鍵長での判断がない。しかし本ガイドラインでは鍵長を考慮して判断した。具体的には、RSA は 2048 ビットがスタンダードであり、また鍵長を電子証明書でコントロールできる一方で、DH は鍵長をサーバ側がコントロールできず、知らないうちに 1024 ビットの鍵を使用して通信を行う可能性を排除できないため、電子政府推奨暗号である DH よりも運用監視暗号である RSA の優先順位を高くしている。そこが CRYPTREC 暗号リストとの相違である。

松本（勉）構成員：暗号は解読に強くなければならないが、強いだけでもだめで、実際に使えなければ意味がない。今回、暗号技術活用委員会の運用ガイドライン WG で精力的に検討いただき、いろいろと考えなければならない事が明らかになってきた。電子政府推奨暗号リストの活用方法を考えるに当たって、従来から実用面を考慮してきたが、最近はさらに細かい所まで詳細に議論できる環境が整ってきた。これを踏まえて、今後 CRYPTREC の活動をどのように進めていくかということを検討していかなければならない。

今井座長：Forward Secrecy については、十分に意識されていないため、こういったものがあり非常に重要であることが分かるように広報していただきたい。

暗号技術活用委員会事務局：本ガイドライン中に、Forward Secrecy が備わっている方がよいということは記載する。

松本（勉）委員：言葉の問題だが、「特高」セキュリティという名称はいかがなものか。

暗号技術活用委員会事務局：名称は仮称であるため、何か良い名称があればご教示いただきたい。

寶木オブザーバ：NIST が楕円曲線や RSA の鍵長の安全性について調べており、使用の是非についてアナウンスを行っている。そちらとのバランスはどうか。

暗号技術活用委員会事務局：基本的に合わせようと思っている。NIST の場合は政府機関向けとして 1024 ビットを使用不可としてしまうということが簡単だと思う。しかし、本ガイドラインでは、特高セキュリティ型について鍵長を 2048 ビットのみ使用可能と記載してもよいと思うが、ベースラインセキュリティ型について 2048 ビットとしてしまうと、携帯電話からアクセスできない可能性があり、相互接続性を維持する観点から確認が必要と考えている。よって、冒頭説明したバッドプラクティスを書くか

どうかの議論と併せて検討中である。具体的には、ベースラインセキュリティ型としては 2048 ビットとするが、バッドプラクティスとしての 1024 ビットへの言及は行わない等が考えられる。

寳木オブザーバ：概ね NIST の考え方と合致していると認識した。ただ、ビジネスの分野で支障が生じないか懸念している。

暗号技術活用委員会事務局：SSL-VPN のベンダや携帯電話のキャリアに、ドラフトの段階で一度このガイドラインを確認していただく予定である。

今井座長：モバイル決済の観点からはどうか。

中山構成員：モバイル決済は「使える」ということが一番重要。実装を考慮した上でどの暗号を採用するのかということだと思う。

（３）2013 年度 暗号技術検討会報告書（案）

資料３に基づき、2013 年度暗号技術検討会報告書（案）について、暗号技術検討会事務局から説明が行われた。質疑はなし。本日の議事内容を反映させた上で、本日の議事概要とともにメールで最終的な確認を行うこととして承認された。

（４）2014 年度 暗号技術検討会活動計画（案）

資料４に基づき、2014 年度暗号技術検討会活動計画について、暗号技術検討会事務局から説明が行われた。質疑応答は以下のとおり。原案どおり承認された。

〇質疑応答

佐々木構成員：基本的にはこの計画で良いと思うが、サイドチャネル攻撃に関する検討は委員会で行っているのか。

暗号技術評価委員会事務局：サイドチャネル攻撃に関する検討は現在暗号技術評価委委員会の活動に含まれており、監視活動として学会発表の内容等を検討している。本活動は CRYPTREC レポートにも掲載予定である。

佐々木構成員：最近、サイドチャネル攻撃に関して問題になっていることはないのか。

本間構成員：攻撃は進化しているが、緊急に対策が必要なものはない。

今井座長：来年度の暗号技術検討会の開催回数は 2 回を予定しているとのことだが、１回目の開催が 10 月と遅くなるのは何か理由があるのか。

暗号技術検討会事務局：2013 年度については、2012 年度の最後の暗号技術検討会で 2013 年度の活動計画を審議いただくことができなかったため、年度の早い時期に 1 回目の会合を開催する必要があった。2014 年度については、今回の暗号技術検討会で活動計画の承認をいただきたいと考えており、この場合 2014 年度の早い時期に会合を開催する必要はなくなるため、年度中間の 10 月頃の開催を予定している。ただし、緊急で開催する必要が生じた場合は、柔軟に対応したいと考えている。

（５）2014 年度 暗号技術評価委員会活動計画（案）

資料５に基づき、2014 年度暗号技術評価委員会活動計画（案）について、暗号技術評価委員会事務局から説明が行われた。質疑応答は以下のとおり。原案どおり承認された。

〇質疑応答

今井座長：乱数の取扱に関しては、活動計画の「（３）暗号技術の安全な利用方法に関する調査（技術ガイドラインの整備、学術的な安全性の調査・公表等）」に含まれているのか。

暗号技術評価委員会事務局：そのとおり。

今井座長：SHA-3 については安全性評価を行うということか。

暗号技術評価委員会事務局：安全性評価を実施し、その上でまずは推奨候補暗号リストへの追加を検討したいと考えている。

（６）2014 年度 暗号技術活用委員会活動計画（案）

資料６に基づき、2014 年度暗号技術活用委員会活動計画（案）について、暗号技術活用委員会事務局から説明が行われた。質疑応答は以下のとおり。一部修正を行うこととして承認された。

〇質疑応答

上原構成員：SSL/TLS サーバ構築ガイドラインは、非常に有用で影響が大きいと考えている。というのも、現在、共通番号法に関係して政府のシステムの大規模な改修が行われている。そのような時期にこのガイドラインができるということは非常によいことだと思っている。ただ、例えば認証プロトコルのように、運用方法についてガイドラインが必要なものがあるのではないかと考えている。来年度の後半には、次にどのようなガイドラインが必要か検討してほしい。

松尾構成員：暗号プロトコルの評価については既に NICT で実施しているが、運用や製品の部分に関して CRYPTREC のガイドラインで補完していただくという方法も考えられる。適宜情報共有しながら、連携して進めていきたい。

今井座長：暗号プロトコルの評価については、現在、暗号プロトコル評価技術コンソーシアム（CELLOS）という組織が立ち上がっているため、そちらとの連携も今後検討していただければと思う。暗号技術活用委員会の活動計画については、SSL/TLS サーバ構築ガイドライン完成後に、次にどのようなガイドラインが必要かを検討することを盛り込むよう修正していただきたい。修正内容については、座長一任とさせていただく。

３　閉会

総務省の吉田政策統括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、2014 年度第 1 回目の暗号技術検討会は 10 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