2009年度第1回暗号技術検討会　議事概要

１．日時　平成21年7月10日（金）　10：00～11：20

２．場所　経済産業省本館17階　西2国際会議室

３．出席者（敬称略）

構成員：今井 秀樹（座長）、辻井 重男（顧問）、宇根 正志、岡本 栄司、岡本 龍明、
加藤 義文、国分 明男、武市 博明、宝木 和夫、松井 充、松本 勉、松本 泰

オブザーバ：伊藤 毅志、齋藤 文信（高橋 浩二代理）、松本 和人（橋本 敏代理）、藤井 信英（井上 知義代理）、平野 友貴（新井 孝雄代理）、馬場 啓晴（江原 健志代理）、荒木 美敬（菊田 豊代理）、郡司 久（田中 正幸代理）、井上 幹邦、坂下 圭一、根本 健治、米子 房伸（篠田 陽一代理）、山田 安秀、亀田 繁、岸本 博之

暗号方式委員会事務局：松尾 真一郎

暗号実装委員会事務局：大熊 建司

暗号運用委員会事務局：田中 秀磨

暗号技術検討会（CRYPTREC）事務局：

総務省　河内 正孝、田中 宏、荻原 直彦、梶原 亮、齊藤 修啓

経済産業省　三角 育生、黒田 俊久、池西 淳

４．配付資料

資料１－１	２００９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１－３	第３回暗号技術検討会議事概要（案）
資料１－４	新しい電子政府推奨暗号リストに対応したCRYPTREC体制見直し（案）
資料１－５－１	２００９年度暗号技術検討会（CRYPTREC）活動計画（案）
資料１－５－２	２００９年度暗号技術安全性評価委員会活動計画（案）
資料１－５－３	２００９年度暗号技術安全性評価委員会運用方針（案）
資料１－５－４	２００９年度暗号技術実装性評価委員会活動計画（案）
資料１－５－５	２００９年度暗号技術実装性評価委員会運用方針（案）
資料１－５－６	２００９年度暗号技術運用性評価委員会活動計画（案）
資料１－５－７	２００９年度暗号技術運用性評価委員会運用方針（案）
資料１－６	新しい電子政府推奨暗号リストの名称（案）

参考資料１	暗号技術検討会　構成員・オブザーバ名簿
参考資料２	暗号技術検討会　２００８年度報告書
参考資料３	CRYPTREC REPORT　２００８
参考資料４	２００８年度版リストガイド
参考資料５	ＩＤベース暗号に関する調査報告書

５．議事概要

１．開会

事務局から開会の宣言があり、総務省の河内総括審議官から開会の挨拶があった。

構成員の交代及びご所属の変更とオブザーバの交代について報告があった。

２．議事

（１）2009 年度暗号技術検討会開催要綱（案）について

資料 1-1 に基づき、暗号技術検討会の開催要綱について、暗号技術検討会事務局から説明があり、了承された。

（２）暗号技術検討会の公開（案）について

資料 1-2 に基づき、暗号技術検討会の公開について、暗号技術検討会事務局から説明があり、了承された。

（３）座長、顧問の選任について

座長の選任、顧問の指名があり、今井座長、辻井顧問が選任された。

（４）2008 年度第 3 回暗号技術検討会議事概要（案）の確認

資料 1-3 に基づき、暗号技術検討会事務局から 2008 年度第 3 回暗号技術検討会議事概要（案）の確認が行われた。

（５）新しい電子政府推奨暗号リストに対応した体制見直しについて

資料 1-4 に基づき、暗号技術検討会事務局から新しい電子政府推奨暗号リストに対応した体制見直しについて説明があった。その後の質疑応答で以下の発言があった。

今井座長：委員会の体制・名称等について、ご意見はあるか。名称については、長い印象がある。

松本勉構成員：検討会の下に 3 委員会を設置することについては、了承する。各委員会の名称については、対称性は良いが、長いので、差分の「安全性委員会」、「実装性委員会」、「運用性委員会」と呼ばれると思う。短い名称にするべきである。昨年度までの暗号モジュール委員会では、サイドチャネル攻撃への対応として安全性についても扱っていたが、今回の名称では、暗号技術安全性評価委員会が安全性をすべて扱うように見えてしまう。CRYPTREC の委員会はすべて安全性を扱っているはず。また、技術も評価もすべての委員会に該当する。案としては、①「暗号方式委員会」、「暗号実装委員会」、「暗号管理委員会」というのはいかがか。あるいは、②「暗号アルゴリズム委員会」、「暗号モジュール委員会」、「暗号マネジメント委員会」、③前の 2 案にそれぞれ頭に CRYPTREC と付ける案も考えられる。いかがか。

暗号技術検討会事務局：事務局案と松本勉構成員案について皆様でご議論いただきたい。

今井座長：松本勉構成員案について、暗号方式の方が、暗号アルゴリズムより良い。暗号方式との並びで、暗号実装の方が、暗号モジュールより良い。暗号技術運用性評価委員会の名称

については、どうか。

辻井顧問：科学技術振興機構では社会的実装と良く言っている。社会との接点を持つことは大事である。暗号方式については、範囲が広いのではないか。暗号運用については、特に問題ないと思う。

松本勉構成員：先ほどの理由で、「暗号技術安全性評価委員会」については、是非とも名称を変えていただきたい。

今井座長：本日は、新委員会の委員長となる予定の佐々木構成員が不在である。

暗号技術検討会事務局：事務局案について、暗号技術検討会という冠を付けなくても、各委員会の内容が分かるような案を提示した。そのため、共通部分があり、長い名称となっている。

今井座長：委員会の名称は、「暗号方式委員会」、「暗号実装委員会」、「暗号運用委員会」とすることで、承認でよいか。

（異議なし）

今井座長：資料の委員会の名称については、新しい名称にて読み替えていただきたい。

（６）2009 年度の活動計画（案）について

資料 1-5-1、1-5-2、1-5-3、1-5-4、1-5-5、1-5-6 及び 1-5-7 に基づいて、暗号技術検討会事務局、暗号方式委員会事務局、暗号実装委員会事務局及び暗号運用委員会事務局から説明が行われた。

暗号運用委員会の体制については、委員長は、佐々木構成員で本人の内諾済みであり、委員については検討中である旨、事務局から連絡があった。決まり次第構成員に連絡することとなった。

引き続いて、各委員会について質問、意見が交わされた。質疑の概要は以下のとおり。

ア　暗号技術検討会

今井座長：今年度は、検討会の下に 3 委員会を設置する。体制の横に NISC があるところが若干気になるが、例年このような体制図である。

構成員から特段の意見、コメントはなく、了承された。

イ　暗号方式委員会

今井座長：各委員会の英語の名称はどうするのか。事務局で決めていただけるか。

暗号技術検討会事務局：事務局にて案を作成して、構成員にご確認いただく。

今井座長：今年度は、7 月に開始して、4 回行うとのことだが、昨年度と同じか。

暗号方式委員会事務局：昨年度と同じ 4 回である。

松本勉構成員：昨年度は WG を設置して、様々な検討を行っていたが、今年度の WG は昨年度と同じような活動を行うのか。

暗号方式委員会事務局：昨年度は、次期の電子政府推奨暗号リストの公募概要の検討のみを事務局で行っていたが、今年度は、電子政府推奨暗号リストの改訂に関する検討が中心のため、事務局が中心となって検討を行う。WG ではリストガイドの部分のみを検討する。

松本勉構成員：リストガイド WG 以外に WG はあるのか。

暗号方式委員会事務局：WG は１つのみであり、それ以外の検討事項は基本的に事務局において検討を行う。

今井座長：他にご意見が無いようであれば、暗号方式委員会の活動計画は委員会の名称を修正したもので承認として良いか。

（異議なし）

ウ　暗号実装委員会

松本勉構成員：資料 1-5-4 の 2.2 について、「ソフトウェア／ハードウェア実装要件の検討を行う。この活動の一環として、～国際標準化に協力する。」とあるが、2.2 は、「サイドチャネル攻撃耐性の評価」とあり、2.3 では、「サイドチャネル攻撃検証 WG」とある。2.3 の WG の活動は何をするのか。WG を設置するということが明記されていない。

暗号技術検討会事務局：2.3 を「サイドチャネル攻撃に関するデータ収集」として、その中で WG を設けてデータ収集を行うことを書く。

松本勉構成員：2.2 と 2.3 では、合わせて 3 種類の業務を行うと思われるが、2.3 では、WG を組織して行うということか。

暗号技術検討会事務局：その通りである。

松本勉構成員：WG の名称「サイドチャネル攻撃検証 WG」について、「攻撃」という表現は少し刺激的に思う。「サイドチャネルセキュリティ WG」としてはどうか。

今井座長：昨年度の WG の名称は、「電力解析実験 WG」であった。今年度の WG の名称について、松本勉構成員の案「サイドチャネルセキュリティ WG」はいかがか。

（異議なし）

今井座長：2.3 の表現として、原案から「サイドチャネル等の攻撃等の実験データの収集」と変更し、WG を設置する旨を内容に記載することとする。

今井座長：スケジュール等についてご意見はあるか。（意見無し）特になければ、指摘を踏まえた活動計画で承認ということとしたい。

エ　暗号運用委員会

松本泰構成員：資料 1-5-6 の 2.2 について、タイムスタンプ等の別のセキュリティ技術の併用とあるが、タイムスタンプ技術自体も暗号技術であり、違和感がある。この資料は、署名済み文書に対する対応を指しているようにも読め、危殆化について狭くとらえすぎているのではないか。矮小化しているのではないか。

暗号運用委員会事務局：検討対象とする技術、システムについて、まだ決まっているわけではないので、事務局にて整理していきたい。

辻井顧問：先般、電子私書箱に関する話も出たが、署名と認証は似ているが、法的には異なる。各会議について、オブザーバが求められることもあるが、こちらから積極的に出席することも必要ではないか。また、危殆化については、マルチメディア振興センターによる調査で、ヨーロッパの有料放送において、数十億円を用いて危殆化対策をしている旨の報告があった。ヨーロッパ等で危殆化が起きたときの状況等について海外調査を行ってもよいのではないか。

今井座長：運用委員会については、初めてできる委員会で、まだ活動についても、これから事務局で練っていかなければいけないと思うが、活動の方向性についてご審議いただきたい。

活動計画の文章は分かりにくい部分がある。2.3 の WG について、事務局から量子暗号などと説明があり、若干分かったが、この文章は直してもらいたい。私の立場としては、暗号はなるべく広くとらえたい。

松本勉構成員：タイムスタンプについてのコメントとして、ほとんどすべてのタイムスタンプはデジタル署名ベースであるが、一部アーカイブのもので暗号技術を使っていないものもあり、暗号技術に含まれないものもある。

今井座長：一連の計画に皆様からいただいた意見を反映した形で修正するということで、ご了承いただきたい。

（異議なし）

（７）新しい電子政府推奨暗号リストの名称（案）について

資料 1-6 に基づき、暗号技術検討会事務局から新しい電子政府推奨暗号リストの名称（案）について説明があった。その後の質疑応答で以下の発言があった。

今井座長：「互換性維持暗号リスト」より「運用監視暗号リスト」の方が良くなったと思われる。異論はあるか。

（異議なし）

松本勉構成員：「電子政府推奨暗号リスト」の「推奨」はとれないのか。「電子政府暗号リスト」としてはだめなのか。「電子政府暗号リストに掲載されている暗号を推奨する」というようにはできないのか。

暗号技術検討会事務局：資料 1-1 にあるとおり、CRYPTREC 自体が「電子政府推奨暗号リスト」の検討を行う場という位置づけである。CRYPTREC が推奨した暗号技術を行政管理局から各省庁に利用していってもらう中で、推奨が取れていくようなイメージである。

今井座長：最終的なリストにも推奨とあるが、かなり強制力（実質的な影響力）があるものなので、推奨ではなく、「電子政府暗号リスト」とできるのではないか。最後の「互換性維持暗号リスト（仮称）」については、「運用監視暗号リスト」とすることでよろしいか。「推奨停止暗号リスト」などの案もあったが、使用者に不安を与えるおそれもあるとのことだった。

岡本栄構成員：「電子政府暗号リスト」という名称は、政府全体でオーソライズしたもののように思われるので、大げさではないか。

暗号技術検討会事務局：「電子政府暗号リスト」というと電子政府運用側の立場でのリストとなる。我々は、技術を評価し、提供しているのであり、電子政府の暗号として用いるかは使う側が判断するべきことである。したがって、「電子政府推奨暗号リスト」との名称が適当かと思われる。

今井座長：「電子政府推奨暗号リスト」ということでよろしいか。

松本勉構成員：私は「電子政府暗号リスト」の方が良いと思うが、大勢がそうなら仕方がない。

今井座長：実質的には、このリストにあるものが標準的な暗号となると思うが、名称については、事務局案のとおり「電子政府推奨暗号リスト」、「推奨候補暗号リスト」、「運用監視暗号リスト」で確定することとしたい。

辻井顧問：「推奨」に関連するコメントだが、法的にどこが責任をとるのか。危殆化したときに、提供したことの責任はどこが負うのかということにならないか。使用者の責任もあるかもしれないが、利用を強制する形になると、提供した側の責任を問われる可能性がある。名称に「推奨」を付けるのは責任を回避する意味でも適当かもしれない。

今井座長：名称は、事務局案を採用することとする。

３．閉会

経済産業省の木村審議官の代理で、三角室長から閉会の挨拶があった。

事務局より、本日の議論を反映して、「電子政府推奨暗号リスト改訂のための公募要項」と、本日の資料について、委員会名、暗号リスト名を修正したものを作成し、構成員の皆様に送付する旨、また、次回会合については今秋の開催を予定しており、詳細については別途連絡する旨、連絡があった。

以上