

2011 年度 第 2 回暗号技術検討会 議事概要

1. 日時 平成 24 年 3 月 8 日 (木) 14:00~16:00

2. 場所 経済産業省 別館 11 階 1120 号会議室

3. 出席者 (敬称略)

構成員: 今井 秀樹 (座長)、辻井 重男 (顧問)、太田 和夫、金岡 晃 (岡本 栄司代理)、岡本 龍明、金子 敏信、国分 明男、佐々木 良一、寶木 和夫、武市 博明、近澤 武、中山 靖司、松井 充、松尾 真一郎、松本 勉、松本 泰、持麿 裕之

オブザーバ: 木本 裕司、眞弓 隆浩 (岡本 克己代理)、松宮 志麻 (栗原 利男代理)、中山 紀雄 (濱島 秀夫代理)、佐藤 真紀子 (河合 芳光代理)、佐久間 明彦 (三澤 康代理)、中島 誠 (田中 正幸代理) 浜田 和之 (川上 一郎代理)、山中 豊 (藤原 達也代理)、坂下 圭一、高橋 幸雄、渡辺 創、笹岡 賢二郎、亀田 繁、鈴木 信

暗号方式委員会事務局: 野島 良 (NICT)

暗号実装委員会事務局: 大熊 建司 (IPA)

暗号運用委員会事務局: 神田 雅透 (IPA)

暗号技術検討会 (CRYPTREC) 事務局:

総務省 佐藤 文俊、佐藤 健治、鮫島 清豪、樋口 有二

経済産業省 永塚 誠一、江口 純一、森川 淳、守山 速飛

4. 配付資料

(資料番号)

(資料名)

- | | |
|--------------|-----------------------------------|
| 資料 2 - 1 | 2011 年度第 1 回暗号技術検討会議事概要 (案) |
| 資料 2 - 2 | 次期電子政府推奨暗号リスト策定スキーム (案) について |
| 資料 2 - 3 | 次期電子政府推奨暗号リスト選定のための評価基準案の検討状況について |
| 資料 2 - 4 - 1 | 暗号技術検討会 2011 年度報告書 (案) |
| 資料 2 - 4 - 2 | 暗号方式委員会 活動計画 (案) |
| 資料 2 - 4 - 3 | 暗号実装委員会 活動計画 (案) |
| 資料 2 - 4 - 4 | 暗号運用委員会 活動計画 (案) |

参考資料 1 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

事務局から開会の宣言があり、総務省の佐藤政策統括官から開会の挨拶。

参考資料1に基づき、構成員及びオブザーバの交代等の説明（米山正夫構成員→中山靖司構成員、本間尚文構成員、（総務省）澤田氏→栗原氏、高地氏→濱島氏、山崎氏→高原氏、（法務省）江原氏→河合氏、（財務省）寺岡氏→橋本氏、（厚生労働省）松原氏→川上氏（経済産業省）山本氏→藤原氏、（独立行政法人情報処理推進機構）矢島氏→笹岡氏）。新任の中山構成員から挨拶。本間構成員は欠席。

2 議事

（1）2011年度第1回暗号技術検討会議事概要（案）の確認

資料2-1に基づき、検討会事務局から説明。質疑等なし。原案どおり了承。

（2）次期電子政府推奨暗号リスト策定スキームについて

資料2-2に基づき、次期電子政府推奨暗号リスト策定について、各委員会の関与の仕方と決定までのフローを検討会事務局から説明。概要は以下のとおり。

- ・暗号方式委員会、暗号実装委員会、暗号運用委員会の各委員会にて、担当業務の評価結果を2012年度上期でとりまとめ、総務省・経済産業省・NICT・IPAの4者からなるクリプトレック事務局に報告。（～2012年9月下旬）
- ・クリプトレック事務局で各委員会の報告をベースにリスト素案を作成し（～2012年10月上旬）、その後、合同委員会にて素案の承認（～2012年11月上旬）。合同委員会にてリスト素案を承認する旨は、各委員会の合意をもとにリスト素案を作成するため。
- ・2012年度第2回暗号技術検討会（2012年11月下旬）において素案を審議し、リスト案を決定。総務省・経済産業省にてパブリックコメントを実施（2012年12月下旬～2013年1月下旬）。
- ・パブコメ意見を受けたリスト案とパブコメ回答案について、2012年度第3回暗号技術検討会（2013年2月下旬）において承認した後、パブコメ回答公表及び次期電子政府推奨暗号リストの決定（2013年3月上旬）。

質疑等なし。原案どおり了承。

（3）次期電子政府推奨暗号リスト改訂に向けた進捗状況について

資料2-3に基づき、暗号運用委員会事務局から、次期電子政府推奨暗号選定のための評価基準案の検討状況について説明。原案どおり了承。質疑は以下のとおり。

金子構成員：スケジュールについて質問がある。先ほど検討会事務局から説明があった資料2-2によれば来年度の上期には結論が出ると理解したが、運用委員会の資料見るとやる事が多く、本当に上半期で話がまとまるのかという不安があるが、どう考えているか。

暗号運用委員会事務局：来年度早々に活動を始める予定。本日の検討会で次年度の活動計画（案）についてご了承頂くのはそのためである。その活動計画（案）については後ほど説明させて頂くが、暗号運用委員会は上期で3回の開催を予定しており、そのうちの2回で選考基準の精緻化を

図る。

金子構成員：第二次選定までを上期に終えるのか。

暗号運用委員会事務局：そうではなく、先ほどの資料2-2にあったように、評価方法、選定基準、調査のデータを提出というのが運用委員会の上期のミッションになる。これに当てはめて暗号を選定するのは、その後の事務局4者や暗号検討会等で行う。

(4) 暗号技術検討会2011年度報告書(案)及び2012年度委員会活動計画(案)について
資料2-4-1から2-4-4までに基づき、検討会事務局及び各委員会事務局から、2011年度報告書(案)及び2012年度活動計画(案)について説明。

① 報告書の全体構成及び電子政府推奨暗号リスト改訂に向けた進捗状況

資料2-4-1の全体構成、第1章、第2章及び第3章(「3.8. 第二次評価及び現リストに記載された暗号技術の再評価の進捗状況」の説明を除く)について、検討会事務局から説明。質疑等無し。

② 暗号方式委員会 活動報告及び活動計画案

資料2-4-1中3. 及び5. 並びに資料2-4-2について、暗号方式委員会事務局から説明。質疑等なし。

③ 暗号実装委員会 活動報告及び活動計画案

資料2-4-1中3. 及び6. 並びに資料2-4-3について、暗号実装委員会事務局から説明。

今井座長：SASEBOは(サイドチャネル攻撃の研究のため)国際的に利用されているのか。

暗号実装委員会事務局：サイドチャネル攻撃に関する技術を競う「DPA コンテスト」では、SASEBOがプラットフォームとして採用されている。世界中の研究者がSASEBOを使ったサイドチャネル攻撃とその対策の研究を進めている。

④ 暗号運用委員会 活動報告及び活動計画案

資料2-4-1中4. 及び7. 並びに資料2-4-4について、暗号方式委員会事務局から説明。質疑等なし。

今井座長：2-4-4の活動計画(案)にセキュリティ人材の育成とあるが、主に暗号研究の人材のことか。

暗号運用委員会事務局：次期リストが決定した後、その影響が、とりわけ暗号研究者や暗号開発にどう及ぶのかということ。セキュリティ全体を含めてということではない。

報告書(案)については、もし修正点があれば検討会事務局に連絡することとし、了承。各委員会の2012年度活動計画(案)については、原案どおり了承。

(5) その他

内閣官房木本参事官：先ほど人材育成の話があったが、情報セキュリティ政策会議でも人材育成・普及啓発の専門委員会を立ち上げており、セキュリティ全般の人材育成について議論を行っている。暗号の人材についても議論を進めていきたい。

現在、政府の暗号移行指針に基づき移行を進めるとともに、今年度末までに緊急対応計画の策定を完了するよう作業を進めている。これらの作業を進める上で、政府機関の認証局及び産業界の認証局からヒアリングを行っている。予定どおり2014年度の上期までに移行できるよう準備を進めている。

しかし、電子証明書を利用する側のユーザのアプリケーションの対応が進んでいないという問題点も浮かび上がっている。本検討会及び関係省庁の皆様から、アプリベンダ等への対応の呼びかけ、指導を行って頂きたい。

また、ヒアリングの中で、ある民間の認証局からは、暗号を移行する必要性が理解できないとの声も出てきている。本日参加しているオブザーバ省庁にも、所管の認証局にご指導頂きたい。構成員においても、様々な機会でも普及啓発に努めて頂きたい。

現在の暗号を利用した署名についても、最長で2019年までは引き続き利用される見込みであり、暗号危殆化のリスクが無視できなくなると考えている。我々としても、緊急対応計画の発動の判定のための主要な検討材料として、暗号技術検討会が発信する技術情報は大変重要かつ必須であることから、引き続き、確実な情報収集、タイムリーな情報提供を継続してお願いしたい。

辻井顧問：自民党が先月出した提言の中で、サイバー攻撃対策などの予算で約1100億円とのことだが、内閣官房としても、そこまでの数字とは言わないが、予算は付けるのか。

内閣官房木本参事官：IT予算全体の積み上げの中で、国会での議論でも、日米比較すると米国の場合はセキュリティ関連の予算はむしろ増えているのに、日本のセキュリティ予算が減っているのはけしからんとのご指摘も頂いている。こうしたご指摘を踏まえ検討していく。

3 閉会

経済産業省の永塚局長から閉会の挨拶。

検討会事務局から、来年度の第1回会合の日程、場所等については別途連絡する旨、連絡。

以上