CRYPTREC Report 2013

平成 26 年 3 月

独立行政法人情報処理推進機構
独立行政法人情報通信研究機構

「暗号技術活用委員会報告」

目次

はじめに

本報告書は、総務省及び経済産業省が主催している暗号技術検討会の下に設置され、独立行政法人情報処理推進機構及び独立行政法人情報通信研究機構によって共同で運営されている暗号技術活用委員会の 2013 年度活動報告である。

暗号技術活用委員会は、2012 年度に CRYPTREC 暗号リストが策定されたことに鑑み、電子政府の安全性及び信頼性を確保し国民が安心して電子政府を利用できる環境を整備すること、並びに我が国の暗号政策に係る中長期の視野に立った課題に引き続き取り組む観点から、セキュリティ対策の推進、暗号技術の利用促進及び産業化を中心とした暗号利用に関する検討課題を主に担当する委員会として新たに設置された委員会である。

本委員会では、暗号の普及促進・セキュリティ産業の競争力強化に係る検討、暗号技術の利用状況に係る調査及び必要な対策の検討、暗号政策の中長期的視点からの取組の検討（暗号人材育成等）など、従来から重要な検討課題として度々挙げられていたものの、日本において本格的な検討が行われたことのない項目について、2 年間の審議期間をかけて審議を行う。具体的には、「暗号政策上の課題の構造」や「暗号と産業競争力の関連性」などの課題に対する分析を行い、暗号アルゴリズムの普及促進やセキュリティ産業の競争力強化に向けた障壁が何かを明らかにするとともに、その解決策を取りまとめる予定である。

また、日本からの暗号アルゴリズムの国際標準化を効率よく進める準備として様々な標準化活動の取り組みを横断的に支援・意見交換するワーキンググループを設置したり、暗号に関する一定水準以上の知識・リテラシーがあることを前提とせずに暗号システムとして安全に利用できるようにするための運用ガイドラインを作成するワーキンググループを設置したりするなど、暗号技術評価を中心とした従来の CRYPTREC 活動の枠組みから、実際の暗号技術の活用を視野に入れた新たな活動領域へ踏み出そうとしていることも特筆すべき視点である。

このような新しい活動成果が、今まで以上に、暗号の普及促進・セキュリティ産業の競争力強化や、より安全な情報化社会の実現に役立つことを期待している。

末筆ではあるが、本活動に様々な形でご協力下さった委員の皆様、関係者の皆様に対して深く謝意を表する次第である。

暗号技術活用委員会 委員長　松本 勉

本報告書の利用にあたって

本報告書の想定読者は、一般的な情報セキュリティの基礎知識を有している方である。例えば、電子署名や GPKI[1] システム等、暗号関連の電子政府関連システムに関係する業務に従事している方などを想定している。しかしながら、個別テーマの調査報告等については、ある程度の暗号技術の知識を備えていることが望まれる。

本報告書は、第 1 章には CRYPTREC 新体制の概要、第 2 章には 2013 年度の暗号技術活用委員会の活動内容と成果概要を記述した。

2012 年度以前の CRYPTREC Report は、CRYPTREC 事務局（総務省、経済産業省、独立行政法人情報通信研究機構、及び独立行政法人情報処理推進機構）が共同で運営する下記の Web サイトから参照できる。

http://www.cryptrec.go.jp/report.html

本報告書ならびに上記 Web サイトから入手した CRYPTREC 活動に関する情報の利用に起因して生じた不利益や問題について、本委員会及び事務局は一切責任をもっていない。

本報告書に対するご意見、お問い合わせは、CRYPTREC 事務局までご連絡いただけると幸いである。

【問合せ先】 info@cryptrec.go.jp

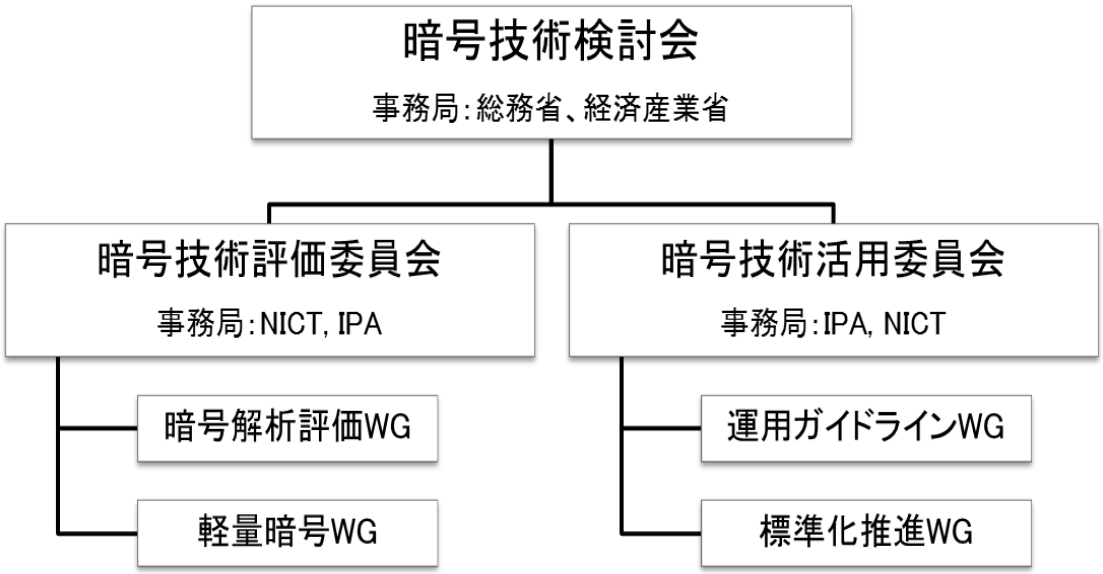
[1] GPKI：Government Public Key Infrastructure（政府認証基盤）

委員会構成

暗号技術活用委員会（以下「活用委員会」）は、図 1 に示すように、総務省と経済産業省が共同で共催する暗号技術検討会の下に設置され、独立行政法人情報処理推進機構（IPA）と独立行政法人情報通信研究機構（NICT）が共同運営している。

活用委員会は、電子政府の安全性及び信頼性を確保し国民が安心して電子政府を利用できる環境を整備するため、セキュリティ対策の推進、暗号技術の利用促進及び産業化を中心とした暗号利用に関する検討課題を主に担当する委員会として、2013 年度に新たに設置された。具体的には、2012 年度にあった暗号運用委員会の担当業務の大半を引き継ぐ形で、暗号の普及促進・セキュリティ産業の競争力強化に係る検討、暗号技術の利用状況に係る調査及び必要な対策の検討、暗号政策の中長期的視点からの取組の検討（暗号人材育成等）などを実施する。

活用委員会と連携して活動する「暗号技術評価委員会」も、活用委員会と同様、暗号技術検討会の下に設置され、NICT と IPA が共同で運営している。



英語名称

- 暗号技術検討会：CRYPTREC Advisory Board for Cryptographic Technology
- 暗号技術評価委員会：Cryptographic Technology Evaluation Committee
- 暗号技術活用委員会：Cryptographic Technology Promotion Committee

図 1　2013 年度の CRYPTREC の体制

委員名簿

暗号技術活用委員会 （2014 年 3 月現在）

委員長	松本 勉	国立大学法人横浜国立大学 教授
委員	上原 哲太郎	立命館大学 教授
委員	遠藤 直樹	東芝ソリューション株式会社 技監
委員	川村 亨	日本電信電話株式会社 担当部長（チーフプロデューサ）
委員	菊池 浩明	明治大学 教授
委員	鈴木 雅貴	日本銀行 主査
委員	高木 繁	株式会社三菱東京 UFJ 銀行 次長
委員	角尾 幸保	日本電気株式会社 主席技術主幹
委員	手塚 悟	東京工科大学 教授
委員	前田 司	EMC ジャパン株式会社 部長
委員	松井 充	三菱電機株式会社 技師長
委員	満塩 尚史	内閣官房 政府 CIO 補佐官
委員	山口 利恵	国立大学法人東京大学 特任准教授
委員	山田 勉	株式会社日立製作所 ユニットリーダ（主任研究員）
委員	山本 隆一	国立大学法人東京大学 特任准教授

オブザーバ

福永 利徳	内閣官房情報セキュリティセンター[2013 年 6 月まで]
今福 健太郎	内閣官房情報セキュリティセンター[2013 年 6 月まで]
中山 慎一	内閣官房情報セキュリティセンター[2013 年 8 月まで]
大川 伸也	内閣官房情報セキュリティセンター[2013 年 8 月から]
石原 潤二	内閣官房情報セキュリティセンター[2013 年 6 月から]
森安 隆	内閣官房情報セキュリティセンター[2013 年 10 月から]
岡野 孝子	警察大学校
稲垣 浩	総務省 行政管理局
佐藤 健太	総務省 行政管理局[2013 年 7 月から]
飯田 恭弘	総務省 情報流通行政局
河合 直樹	総務省 情報流通行政局
中村 一成	総務省 情報流通行政局
岩永 敏明	経済産業省 産業技術環境局
中谷 順一	経済産業省 商務情報政策局
室井 佳子	経済産業省 商務情報政策局
谷口 晋一	防衛省 運用企画局

事務局

独立行政法人 情報処理推進機構（笹岡賢二郎[2013 年 6 月まで]、伊藤毅志[2013 年 7 月から]、近澤武、小暮淳、大熊建司、神田雅透、菅野哲[2013 年 10 月から]、稲垣詔喬、吉川法子）

独立行政法人 情報通信研究機構（平和昌、沼田文彦、盛合志帆、野島良、大久保美也子、黒川貴司、金森祥子、側高幸治）

第１章　CRYPTREC 新体制について

2012 年度は、「電子政府推奨暗号リスト」（平成 15 年 2 月 20 日公表；以下「旧電子政府推奨暗号リスト」）を改定した「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（CRYPTREC 暗号リスト)」を策定するなど、CRYPTREC として節目の１年となった。この CRYPTREC 暗号リストは「安全性」及び「実装性」の観点に加え、「製品化、利用実績等」といった様々な視点で検討され、「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」の 3 つのリストから構成される。今後は、政府機関における情報システムの調達及び利用において、この新しいリストが大いに活用されることが期待される。

2013 年度は、2012 年度に CRYPTREC 暗号リストが策定されたことに鑑み、電子政府の安全性及び信頼性を確保し国民が安心して電子政府を利用できる環境を整備すること、並びに我が国の暗号政策に係る中長期の視野に立った課題に引き続き取り組む観点から、2012 年度までの暗号方式委員会・暗号実装委員会・暗号運用委員会の 3 委員会体制から、暗号技術評価委員会・暗号技術活用委員会の 2 委員会体制に改組した（図 1 参照)。

各々の検討会・委員会での活動内容は以下のとおりである。

(1)　CRYPTREC 暗号リストの小改定に関する意思決定（暗号技術検討会が実施）
- (a) 推奨候補暗号リストに掲載されている暗号技術の昇格方針を検討する。
- (b) 新規暗号（事務局選出）及び新技術分類の追加（新規暗号公募含む）に関する方針を検討する。
- (c) 内閣官房情報セキュリティセンター等政府関係機関との連絡・調整を実施する。

(2)　暗号技術の安全性評価を中心とした技術的な検討（暗号技術評価委員会が実施）
- (a) 新世代暗号に係る調査（軽量暗号、セキュリティパラメータ、ペアリング、耐量子計算機暗号等）を実施する。
- (b) 暗号技術の安全性に係る監視及び評価（SHA-3 の評価を含む）を実施する。
- (c) 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）を実施する。

(3)　セキュリティ対策の推進、暗号技術の利用促進及び産業化を中心とした暗号利用に関する検討（暗号技術活用委員会が実施）
- (a) 暗号の普及促進・セキュリティ産業の競争力強化に係る検討（運用ガイドラインの整備、教育啓発資料の作成等）を実施する。
- (b) 暗号技術の利用状況に係る調査及び必要な対策の検討等を実施する。
- (c) 暗号政策の中長期的視点からの取組の検討（暗号人材育成等）を実施する。

第 2 章　2013 年度の活動内容と成果概要

2.1　活動内容

暗号技術活用委員会では、2012 年度暗号運用委員会の全部及び暗号実装委員会の一部からの課題を主に引き継ぎ、暗号技術における国際競争力の向上及び運用面での安全性向上に関する検討を実施する。主な検討課題は以下のとおり。

① 暗号の普及促進・セキュリティ産業の競争力強化に係る検討（運用ガイドラインの整備、教育啓発資料の作成等）
② 暗号技術の利用状況に係る調査及び必要な対策の検討等
③ 暗号政策の中長期的視点からの取組の検討（暗号人材育成等）

このうち、2013 年度は、暗号技術の利用状況に係る調査を実施する予定がないことから、①暗号の普及促進・セキュリティ産業の競争力強化に係る検討、及び③暗号政策の中長期的視点からの取組の検討（暗号人材育成等）についてのみ実施する。

具体的には、以下の検討項目について取り組むこととした。

(A) 暗号の普及促進・セキュリティ産業の競争力強化に係る検討

CRYPTREC 暗号リストの策定により、同リストに掲載されている暗号アルゴリズムの普及が促進し、ひいては日本のセキュリティ産業の競争力強化につながることが期待されている。しかし、現実には「優れた暗号アルゴリズムがセキュリティ産業の競争力強化に直接的に繋がる」という関連性については、2012 年度運用委員会の委員ならびに CRYPTREC シンポジウム 2013 でのパネリストから極めて懐疑的な意見が多数出された。また、2012 年度の暗号技術の利用状況に係る調査結果からは、旧電子政府推奨暗号リスト策定から 10 年経過していたにもかかわらず、同リストに掲載されていた国産の暗号アルゴリズムの普及がほとんど進んでいない実態も明らかとなった。

そのため、本委員会では、「暗号政策上の課題の構造」や「暗号と産業競争力の関連性」などの課題に対する分析について約 2 年間の集中審議期間を設けることにより、暗号アルゴリズムの普及促進やセキュリティ産業の競争力強化に向けた障壁が何かを明らかにするとともに、その解決策を取りまとめる。

2013 年度は、上記課題分析を行うにあたって幅広く現況を俯瞰する必要があることから、議論を行ううえで有用な基礎データを収集し、取りまとめる。すぐに対応可能な課題には本年度中に取り掛かるが、本格的な課題分析や具体的な解決策の検討についてはタイムスケジュールを作成する。

- 各種団体（政府機関を含む）等へのヒアリング
- セキュリティ産業競争力の源泉の俯瞰（市場動向など）
- 政策動向（共通番号制度、医療ガイドラインなど）
- 工程表の作成

(B) 暗号政策の中長期的視点からの取組の検討

人材育成の観点に関しては、様々なシステムを安全に動かしていく人材にとって、暗号についての必要な知識やスキルがどういうものかを検討することにより、CRYPTREC として取り組むべき課題を明らかにする。

- 各種団体（政府機関を含む）等へのヒアリング
- 工程表の作成

(C) 標準化推進

様々な標準化機関に対して日本から提案する暗号アルゴリズムが受け入れられるようにするため、標準化活動の取り組みを横断的に支援・意見交換するワーキンググループ（標準化推進 WG）を設置し、日本からの暗号アルゴリズム提案の効率的な横展開を図る。

(D) 運用ガイドライン作成

暗号に関する一定水準以上の知識・リテラシーがあることを前提とせずに、暗号システムとして安全に利用できるようにするための運用ガイドラインを、運用ガイドライン WG を設置して作成する。

2013 年度は、利用者が非常に多く、また暗号に関するリテラシーのレベルにも大きな差がある「SSL/TLS」について作成する。

2.2 今年度の委員会の開催状況

2013 年度暗号技術活用委員会は 3 回開催された。各回会合の概要は表 1 のとおり。

表 1 2013 年度暗号技術活用委員会概要

回	開催日	議案
第 1 回	2013 年 9 月 11 日	● 活用委員会活動計画の確認 ● ワーキンググループ活動計画案の審議・承認 ● 2013 年度調査方向性の審議 ● ヒアリング内容（ヒアリング先を含む）の審議

第 2 回	2013 年 12 月 13 日	● SSL/TLS サーバ構築ガイドライン（骨子）についてのとりまとめ中間報告及び審議 ● ヒアリング及び標準化推進 WG の中間報告
第 3 回	2014 年 3 月 19 日	● 2013 年度ヒアリング調査の報告 ● 各ワーキンググループからの活動報告 ● SSL/TLS サーバ構築ガイドライン技術的取りまとめ（WG 案）報告及び審議

2.3 成果概要

2.3.1 ヒアリング調査結果について

「暗号政策上の課題の構造」や「暗号と産業競争力の関連性」などの課題に対する分析を行うにあたって幅広く現況を俯瞰すること、並びに様々なシステムを安全に動かしていく人材にとって暗号についての必要な知識やスキルがどういうものかを検討することを目的として、各種団体（政府機関を含む）等へのヒアリング（アンケート形式を含む）を実施した。

主なヒアリング対象は以下のとおりである。

- 政府 CIO
- 政府機関・公的機関
- 業界団体
- サプライヤ（SIer、ベンダ等）
- ユーザ（オンラインショッピング、等）

また、ヒアリングを行う上で、以下のような仮説を立て、それらの視点を考慮してヒアリング項目を審議・作成した。

【設定した仮説】

- **暗号政策としてあるべき姿とは何か**

  仮説１：電子政府推奨暗号リストを具体的な暗号政策に結び付ける施策が必要ではないか

  仮説２：国家安全保障や情報資産保護等の観点を考慮すべきではないか

- **高度な暗号技術を産業競争力に反映させる要素は何か**

  仮説３：実際には暗号アルゴリズムの選択についての自由度が高くないのではないか

  仮説４：技術的な要素よりもそれ以外の要素のほうが暗号アルゴリズムの選択への影響が大きいのではないか

- **国産暗号の利用を促進させるために必要な要素は何か**

  仮説５：国産暗号を使いたいと思っても実際に使おうとすると高い障壁があるのではないか

  仮説６：利用実績や今後の利用可能性なども考慮した今回のリスト改定により、国産暗号の選択が容易になったのではないか

- **暗号に関してのどのような人材が不足しているか**

  仮説７：暗号アルゴリズムの選択等に対する目利き人材が不足しているのではないか

【設定したヒアリング項目一覧】

下線部は、ヒアリング項目における主な候補対象者を示している。例えば、“政府担当者”との記載は、政府機関での調達実務者や仕様策定に権限がある担当者が当該項目におけるヒアリング候補先ということを示す。

- **暗号を利用する機会がありますか？**

  政府担当者・業界団体・サプライヤ・ユーザ

  (a-1) 担当業務において、過去にセキュリティ向上策の一環として何らかの形で、暗号を利用したり、利用するように指示・取りまとめをしたりする場面がありましたか。

  - その際のセキュリティ向上策として、暗号以外の対策と比較して、暗号による対策はどの程度重要視されましたか。

  政府担当者・業界団体

  (a-2) 現在または近いうちに、暗号アルゴリズムの指定を伴うような調達仕様や規格等を作成・検討している、もしくは予定がありますか。

  - あるとすれば、どのような形で作成・検討が行われますか。

- **どのような観点で暗号の選択や利用方法を決めていますか？**

  政府 CIO・政府担当者・業界団体・サプライヤ・ユーザ

  (b-1) 利用する暗号アルゴリズムはどういった経緯で決まりましたか。自ら（自らが開催する委員会等での審議を含む）の暗号アルゴリズム選択自体の検討結果による

ものですか、それとも何らかの別の要因で決まったものですか。

- 前者の場合、利用する暗号アルゴリズムを具体的に決める際に考慮した要件は何でしたか。また、そのうち、もっとも影響する要因は何でしたか。
  例えば、
  - 知名度・信頼感
  - 安全性
  - 処理性能
  - コスト（製品開発コスト、購入コスト、運用コスト、移行コストなど）
  - 製品選択の容易性（製品種類の多さ、など）
  - 開発期間（サービス導入・開始までの時間）
  - 特許・ライセンス
  - 輸出管理などの法規制
  - その他
- 後者の場合、誰が利用する暗号アルゴリズムを具体的に決めることになりましたか。
  例えば、
  - トップダウン的に決まっていた
  - 大きな議論なく、なんとなく決まった（初めから一つしか候補がなかった）
  - 暗号研究者などの専門家に選択を委ねた
  - 利用する暗号アルゴリズムは細かく指定せずに（もしくは選択肢を示すだけで）、ベンダやサプライヤ、運用者、利用者などの実質的な担当部門に選択を委ねた
  - その他

政府担当者・業界団体・サプライヤ・ユーザ

(b-2) 期限を切って利用する暗号アルゴリズムを交換するような対策を実施したことがありますか。

- その対策は支障なく実施できましたか。

サプライヤ

(b-3) 利用する暗号アルゴリズムによって製品開発コストや利益に違いが生じますか。また、その違いはビジネス的に許容できるレベルを超えていますか。

- 違いが生じるとすれば、どのような要因によるものですか。

- **電子政府推奨暗号リストを活用していますか？**

  政府 CIO・政府担当者・業界団体・サプライヤ・ユーザ

  (c-1) 電子政府推奨暗号リスト、CRYPTREC 暗号リスト、CRYPTREC 等の活動成果を知っていましたか。

  - 暗号アルゴリズムの選択や利用方法を具体的に決める際に参考にしましたか。参考にしたとすれば、どの程度参考にしましたか。

    例えば、

    - 具体的な暗号アルゴリズムを選択するにあたっての技術比較として利用
    - 特定の暗号アルゴリズムについての技術的な裏付けとして利用
    - 安全な暗号アルゴリズムの選択肢の提示としての利用
    - その他

  サプライヤ

  (c-2) 電子政府推奨暗号リストに掲載されている暗号アルゴリズムにもかかわらず、何らかの理由で、当初利用することを予定（提案を含む）していたものとは異なるものに途中で変更したこと、または変更させられたことがありますか。

  - 変更したこと、または変更させられたことがあるならば、どのような要因によるものですか。

- **国産暗号アルゴリズムについてどのように考えていますか？**

  政府 CIO

  (d-1) 国産暗号アルゴリズムの利用が進まない原因はどのようなものだと思いますか。

  例えば、

  - 国産暗号アルゴリズムを利用しようとは思わない。利用するメリットがない。
  - 利用しようとは思っても何らかの障壁がある。
  - ベンダやサプライヤ、運用者、利用者などの実質的な担当部門に選択を委ねている。

  政府担当者・業界団体・サプライヤ・ユーザ

  (d-2) 国産暗号アルゴリズムを利用しようと考えたことがありますか。

  - 考えたことの有無にかかわらず、その理由はなんですか。

  サプライヤ

  (d-3) 官公庁向けのシステム・製品において、国産暗号アルゴリズムを利用しましたか。

  - 利用しなかった場合、その理由はなんですか。

政府担当者・業界団体・サプライヤ・ユーザ

(d-4) 国産暗号アルゴリズムを利用しようと考えたとき、実際に大きな支障なく利用できましたか。

- 利用しようとは考えたが実際には利用できなかった場合、何が障壁になって国産暗号アルゴリズムを利用することを断念しましたか。

政府 CIO・政府担当者・業界団体・サプライヤ・ユーザ

(d-5) 今後、もし国産暗号アルゴリズムを利用しようと考える場合に、利用実績や今後の利用可能性なども考慮した今回のリスト改定で電子政府推奨暗号の国産暗号アルゴリズムの個数が絞り込まれたことにより、国産暗号アルゴリズムを選択することが容易になると思いますか。

- 容易になっていないとすれば、その理由はなんですか。

政府 CIO・政府担当者・業界団体

(d-6) 「国家安全保障」や「情報資産保護」、「日本の暗号研究開発力の維持」等の視点から、政府や業界団体などがトップダウン的に国産暗号アルゴリズムの利用を優先させるという考え方をどのように思いますか。

- そのように思う理由はなんですか。
- 実際に行うとした場合に何が障壁になりそうですか。

サプライヤ・ユーザ

(d-7) 「国家安全保障」や「情報資産保護」、「日本の暗号研究開発力の維持」等の視点から、仮にトップダウン的に国産暗号アルゴリズムの利用促進を図ろうとした場合に、何か困ることが起きそうですか。

- 起きるとすれば、どういったことが予想されますか。

政府 CIO・サプライヤ

(d-8) 日本の企業や大学、独立行政法人が国産暗号アルゴリズムを作ることの意義はなんだと考えますか。例えば、

- 日本の国益に直接的にかかわるもの
- 日本の産業力強化に関わるもの
- いざという時のための暗号研究開発力の保持
- 自己のビジネスのため
- 自己満足のため

サプライヤ・ユーザ

(d-9)「米国政府標準暗号」と「電子政府推奨暗号である国産暗号」のどちらが知名度／信用度／アピール効果を持っていますか。

- どのような点でそのような違いを感じますか。

- **暗号アルゴリズムの選択等に対する目利き人材が必要ですか？**

政府 CIO・政府担当者・業界団体・サプライヤ・ユーザ

(e-1) 利用する暗号アルゴリズムの選択や安全性動向の把握、暗号アルゴリズムの切り替えなどの技術的課題に対して、現在、どの程度の暗号についての知識やスキルを持っている人が担当していますか。

- 暗号研究者との間で適切な議論が行える状況にありますか。
- 実務を行ううえで支障になっていることがありますか。

政府 CIO・政府担当者・業界団体・サプライヤ・ユーザ

(e-2) 利用する暗号アルゴリズムの選択や安全性動向の把握、暗号アルゴリズムの切り替えなどの技術的課題に対応できる人材を、自らの組織内に持つ必要があると考えますか。それとも、そういった課題について対応してくれる人材が集約された組織が外部にあれば十分と考えますか。

- 前者の場合、どの程度の知識やスキルを持つ人材がどの程度の規模（人数）で必要だと思いますか。また、組織体として暗号についての知識やスキルを伝承・維持するための仕組みがありますか。
- 後者の場合、どういった組織体であることを期待しますか。また、そのような組織体が出す情報について、どの程度の効力を期待しますか。

2013 年度には、政府 CIO、政府機関・公的機関、並びにいくつかの業界団体についてヒアリングを実施した。また、2013 年度にヒアリングが実施できなかった、ユーザ（電子商取引関係（ショッピングモール等）等）やサプライヤ（SIer、ベンダ等）、2013 年度にヒアリングを実施しなかった業界団体については、2014 年度上期にもヒアリングを継続実施する予定である。

なお、ヒアリングの内容については、継続実施する予定のヒアリング調査結果と合わせ、2014 年度の最終報告書の中で取り扱うものとする。

2.3.2 標準化推進 WG 概要報告

標準化推進 WG は、様々な標準化機関に対して日本から提案する暗号アルゴリズムが受け入れられるようにするため、標準化活動の取り組みを横断的に支援・意見交換し、日本からの

暗号アルゴリズム提案の効率的な横展開を図ることを目的として、設置された。

具体的には、委員が活動に関わる各標準化団体における自らの活動状況や日本からの提案事項における交渉ノウハウや課題等を共有・蓄積し、暗号アルゴリズムの標準化提案に当たっての俯瞰図を取りまとめる。併せて、今後様々な組織が日本から暗号アルゴリズムの提案を行う場合に、その成果が効率的に得られるようにするため、提案機会等の見込みがある標準化団体の選定（提案時期も含む）、提案する組織に当面必要な稼働見積もりや交渉方法等を検討する。

【委員構成】

標準化推進 WG の委員は以下のとおり。

	委員氏名	所属	担当領域
主査	渡辺　創	独立行政法人産業技術総合研究所	ISO/IEC JTC1/SC27
委員	江原　正規	東京工科大学	ISO/IEC JTC1/SC31
委員	河野　誠一	レノボ・ジャパン株式会社	TCG
委員	木村　泰司	一般社団法人日本ネットワークインフォメーションセンター	IETF
委員	坂根　昌一	シスコシステムズ合同会社	M2M/IoT
委員	佐藤　雅史	セコム株式会社	長期署名（ETSI）
委員	武部　達明	横河電機株式会社	制御機器・制御システム
委員	廣川　勝久	ISO/IEC JTC1/SC17 国内委員会	ISO/IEC JTC1/SC17
委員	真島　恵吾	日本放送協会	放送
委員	真野　浩	コーデンテクノインフォ株式会社	IEEE802.11
委員	茗原　秀幸	三菱電機株式会社	医療

【活動概要】

2013 年度は、標準化活動の現状を整理するため、各標準化団体における、自らの活動状況や日本からの提案事項における交渉ノウハウや課題等を共有・蓄積した。

各々の標準化団体の活動概要は参考資料として添付する。

【開催状況】

標準化推進 WG の開催状況は次のとおり。

表 2　2013 年度標準化推進 WG 開催状況

回	開催日	議案
第 1 回及び第 2 回	2014 年 2 月 10 日	● 委員からの各標準化団体の概要についての報告

2.3.3 運用ガイドライン WG 概要報告

暗号システムとして安全に利用できるようにするための運用ガイドラインを作成する。2013 年度は、利用者が非常に多く、また暗号に関するリテラシーのレベルにも大きな差がある「SSL/TLS」について作成する。

【委員構成】

運用ガイドライン WG の委員は以下のとおり。

	委員氏名	所属
主査	菊池 浩明	明治大学
委員	阿部 貴	株式会社シマンテック
委員	漆嶌 賢二	富士ゼロックス株式会社
委員	及川 卓也	グーグル株式会社
委員	加藤 誠	一般社団法人 Mozilla Japan
委員	佐藤 直之	株式会社イノベーションプラス
委員	島岡 政基	セコム株式会社
委員	須賀 祐治	株式会社インターネットイニシアティブ
委員	高木 浩光	独立行政法人産業技術総合研究所
委員	村木 由梨香	日本マイクロソフト株式会社
委員	山口 利恵	国立大学法人東京大学

【活動概要】

従来の CRYPTREC が作成してきた報告書等とは異なり、暗号技術の記述を中心としたガイドラインではなく、暗号技術をシステムの中での一要素とみなしたうえでの運用ガイドラインを目指したものである。その心は、読者がある程度の暗号技術の知識を有していなくても内容を正しく理解できること、またガイドラインの有効性の面からも実際に設定ができることを重視したガイドラインを作り上げることにある。

本年度は、多くのユーザが利用している「SSL/TLS」を題材に取り上げた。

なお、対象読者の考え方として、当初は、ブラウザを使う一般のユーザも対象読者に含めることを想定していたが、最近のブラウザではユーザに様々な設定をあえてさせないブラックボックス化を進めることで安全性を高めていること、サーバ側の設定で一定程度のブラウザのコントロールができること、一般のユーザにこの種のガイドラインを読ませることは現実には難しいこと、などの指摘が委員からなされた。これらの指摘を考慮して、WG としては、想定読者から一般のユーザは外し、主に SSL/TLS サーバを実際に構築するにあたって具体的

な設定を行うサーバ構築者、実際のサーバ管理やサービス提供に責任を持つことになるサーバ管理者、並びに SSL/TLS サーバの構築を発注するシステム担当者とすることにした。

これに合わせ、SSL/TLS サーバの構築時に注意すべき点をまとめたガイドラインであることを明確にすることから名称を「SSL/TLS サーバ構築ガイドライン」とした。

本ガイドラインのポイントは、「暗号技術以外の様々な利用上の判断材料も加味した合理的な根拠」を重視して、現実的な利用方法をまとめたガイドラインを目指したことである。

例えば、実現すべき安全性についても、必要となる相互接続性とのトレードオフを考慮する観点から、相互接続性を損なってでも極めて高い安全性を重視する「特高セキュリティ型（仮称）」の SSL/TLS サーバを構築するケースから、一定水準の安全性を維持しながら極力相互接続性を確保する「ベースラインセキュリティ型（仮称）」の SSL/TLS サーバを構築するケースまで、複数の設定例を提示している。

また、最低限の安全性を確保するために、ブラウザ等との相互接続をあえて拒否すべき最低基準（バッドプラクティス）を明確にしたのも本ガイドラインの特長である。

【開催状況】

運用ガイドライン WG の開催状況は次のとおり。

表 3　2013 年度運用ガイドライン WG 開催状況

回	開催日	議案
第 1 回	2013 年 10 月 10 日	● CRYPTREC 活動体制について ● 2013 年度活動計画について ● SSL/TLS 運用ガイドラインの作成方針・作業分担について
第 2 回	2013 年 12 月 4 日	● SSL/TLS サーバ構築ガイドライン（骨子案）のとりまとめ
第 3 回	2014 年 3 月 12 日	● 2013 年度運用ガイドライン WG 報告（案）について ● 今後のスケジュールについて ● SSL/TLS サーバ構築ガイドライン（ドラフト仮版）の技術的とりまとめ

第 3 章　今後に向けて

今後、暗号に関する様々な課題解決に向けた政策立案等を行う際に役立てるために、2014 年度は、2013 年度の活動内容を継続して実施し、各検討項目における最終報告書を取りまとめる。

(A) 暗号の普及促進・セキュリティ産業の競争力強化に係る検討

本委員会では、2013 年度と 2014 年度の 2 年間をかけて、「暗号政策上の課題の構造」や「暗号と産業競争力の関連性」などの課題に対する分析を行い、暗号アルゴリズムの普及促進やセキュリティ産業の競争力強化に向けた障壁が何かを明らかにするとともに、その解決策を取りまとめる活動をしている。

2014 年度は、2013 年度に引き続いて、議論を行ううえで有用な基礎データの収集を上期も継続して実施する。下期には、2013 年度及び 2014 年度上期に収集したデータをもとに、暗号の普及促進・セキュリティ産業の競争力強化に向けた具体的な課題分析や解決策の検討を実施し、報告書に取りまとめる。

(B) 暗号政策の中長期的視点からの取組の検討

上記の「暗号の普及促進・セキュリティ産業の競争力強化に係る検討」のなかで、様々なシステムを安全に動かしていくための暗号に関連する人材育成についても一緒に検討していくことにより、CRYPTREC として取り組むべき課題を明らかにし、報告書に取りまとめる。

(C) 標準化推進

2013 年度の成果を踏まえ、今後、様々な日本の組織が国際的に影響力を持つ標準化機関へ日本からの暗号アルゴリズムの提案を行う場合に、提案する組織を横断的に支援し、意見交換を行っていけるように、以下の議論を継続し、2014 年度に報告書としてまとめる。

- 暗号アルゴリズム提案に当たっての俯瞰図の取りまとめ
- 提案機会等の見込みがある標準化提案先の選定（提案時期も含む）
- 暗号アルゴリズムを提案する組織にとって当面必要な稼働見積りや交渉方法等

(D) 運用ガイドライン作成・公開

本ガイドラインは、SSL/TLS サーバの構築において広範囲に活用してもらうべき性質のものであることを考慮し、今後、2013 年度の WG での審議内容を確定する前に外部からの意見聴取等も取り入れ、引き続き運用ガイドライン WG にて作業を行い、成果物を暗号技術検討会に報告する。

参考

A. ISO/IEC JTC1/SC27

体制

ISO/IEC JTC1/SC27（以下、SC27 という）は、セキュリティ技術の国際標準化を行っている委員会であり、5 つのワーキンググループ（以下、WG という）から構成されている。5 つの WG は、それぞれ「WG 1: Information security management systems」、「WG 2 : Cryptography and security mechanisms」、「WG 3: Security evaluation, testing and specification」、「WG 4: Security controls and services」、及び「WG 5: Identity management and privacy technologies」である。特に、暗号技術に関する国際標準化は、WG2 が担当している。

標準化の概要

SC27 で標準化された規格数は全体で 130 に上る。標準化のプロセスは順に WD、CD、DIS、FDIS を経て進み、提案後 2 年から 4 年ほどで規格（IS）として出版される。CD 以降は投票により、プロセスが進むか否かが決定される。また、投票に参加する P-member は 53 か国、オブザーバを務める O-member は、16 か国である。投票権は 1 か国 1 票であるため、国数が多い欧州が規格の制定に有利な状況である。

SC27 への規格提案では、基本的には 1 規格につき、1 か国で 1 技術までの提案となっている。2 つ目の技術を標準化するには、強い理由が必要である。そのため、同じ国で複数の提案者がいる場合、国内委員会でも調整を行う必要がある。

国際委員会では学術界に近い暗号の専門家が中心となって議論が行われる。規格への採用において、安全性が保証されていることが重要な要件である。ただし、SC27 自体は安全性評価を行わないため、他の機関等の評価結果を基に議論を行う。CRYPTREC による評価の信頼性は高い。また、標準化の際の評価として国内標準になっていることは国際標準化の強い理由となり得る。

暗号に関連する規格等

- 暗号アルゴリズム:ISO/IEC 18033
- デジタル署名：ISO/IEC 14888（添付型）, ISO/IEC 9796（復元型）
- ハッシュ関数：ISO/IEC 10118
- メッセージ認証コード：ISO/IEC 9797
- エンティティ認証：ISO/IEC 9798
- 認証付暗号：ISO/IEC 19772
- 鍵管理：ISO/IEC 11770
- 暗号利用モード：ISO/IEC 10116
- 乱数ビット生成：ISO/IEC 18031
- 素数生成：ISO/IEC 18032
- 楕円曲線ベース暗号技術：ISO/IEC 15946

- 軽量暗号：ISO/IEC 29192
- 匿名デジタル署名：ISO/IEC 20008
- 匿名認証：ISO/IEC 20009

<u>その他</u>

ISO/IEC の標準に掲載されている日本の暗号技術は次のとおりである。

- ISO/IEC 18033 Encryption algorithms
  - Part 2 Asymmetric ciphers（非対称暗号）
    - PSEC-KEM
    - HIME(R)
  - Part 3 Block ciphers（ブロック暗号）
    - MISTY1（64 ビットブロック暗号）
    - Camellia（128 ビットブロック暗号）
  - Part 4 Stream ciphers（ストリーム暗号）
    - MUGI（鍵ストリーム生成）
    - KCipher-2（鍵ストリーム生成）
    - MULTI-S01（出力関数）
- ISO/IEC 29192 Lightweight cryptography
  - Part 2 Block ciphers（ブロック暗号）
    - CLEFIA
  - Part 3 Stream ciphers（ストリーム暗号）
    - Enocoro
- ISO/IEC 14888 Digital signatures with appendix
  - Part 2 Integer factorization based mechanisms（素因数分解問題ベースのメカニズム）
    - ESIGN
- ISO/IEC 20008 Anonymous digital signatures
  - Part 2 Mechanisms using a group public key（グループ公開鍵を用いたメカニズム）
    - Mechanisms 5 and 6

B. ISO/IEC JTC1/SC17

体制

ISO/IEC JTC1/SC17（以下、SC17 という）は、カード及び個人識別について標準化を行っている委員会であり、9 の WG から構成されている。SC17 国内委員会には WG 国内委員会に加え、WG 間及び国内関係機関との連携を図るための SWG 委員会を設置して活動しており、それらの活動成果の国際標準への反映を図るとともに国際役職の引受等も含めて貢献している。以下に、SC17 国内委員会の構成図を示す。

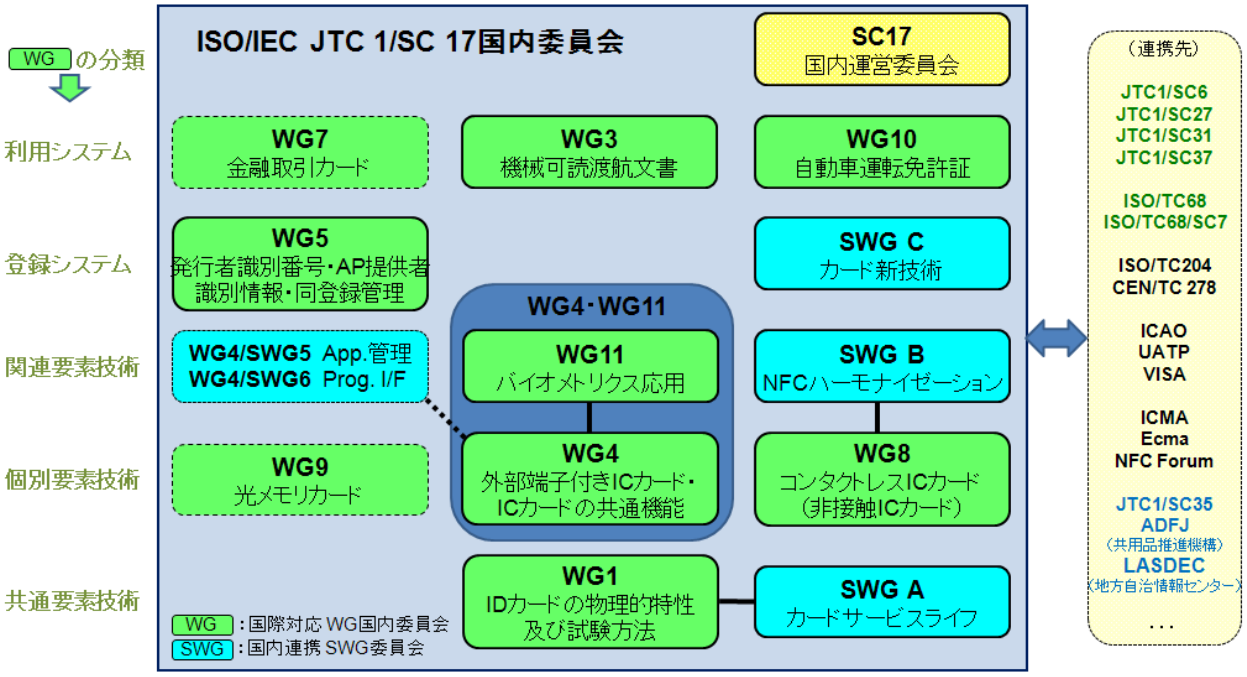


図 1. SC17 国内委員会の構成

標準化の概要

SC17 は、カード及び個人識別を対象とし、その要素技術から利用システム（クレジット・IC 旅券・運転免許証等）までに関する国際標準化と登録管理を担当している。この分野では、アプリケーション面からの標準化ニーズが高まっている。また、既に標準化された要素技術についても機能や性能に関わる追加標準化のニーズが生じている。これはカードが単体ではなくシステムとして利用される段階に進み、広範囲な互換性が求められるようになったことを示している。日本は、実装の実現性・後方互換を含めた互換性・今後の拡張性・全体的整合性等の観点からの詳細レビューと考察及び実験データに基づき意見の反映を図っている。ISO/IEC 7816、ISO/IEC 14443 等の主要規格には日本提案の技術が反映され国際的にも広く活用されており、IC カードの事業基盤形成に貢献している。技術面・アプリケーション面で関係の深まっている JTC1 の各 SC、ISO の各 TC、及びその他関係機関との連携を強化しているが、その範囲は拡がる方向にある。

暗号に関連する規格等

IC カード（SIM 等含む）が色々な応用分野で SE（Secure Element）としての機能を提供するにあたって暗号技術は必須の技術である。SC17 では、IC カードへの暗号技術利用のために、格納すべき暗号関連情報等の識別のための Tag 等を定めるが、暗号技術自体の標準化は行わない。基本的に、SC27 で標準化された暗号技術を前提に、各種の応用分野が求める利用方法をサポートするための IC カード用条件を必要に応じて標準化している。

その他

- 主要な国際標準
  - ID カードの基本規格　：ISO/IEC 7810（ID-1 カード、SIM カード等）
  - ID カードの記録技術：ISO/IEC 7811（エンボス、磁気記録）
  - IC カード（端子付き）：ISO/IEC 7816（Part-1～3, 10,12）
  - 非接触 IC カード：ISO/IEC 14443（近接型）、ISO/IEC 15693（近傍型）
  - IC カードの共通機能:ISO/IEC 7816（Part-4～9, 11,13,15）
  - 光メモリカード：ISO/IEC 11693、ISO/IEC 11694、ISO/IEC 11695
  - 発行者識別番号・同登録管理： ISO/IEC 7812
  - アプリケーション提供者識別情報：ISO/IEC 7816（Part-5）
  - IC 旅券・査証：ISO/IEC 7501
  - IC 運転免許証：ISO/IEC 18013
  - 生体認証応用：ISO/IEC 7816-11、ISO/IEC 17839、ISO/IEC 24787
  - アクセシビリティ：　ISO/IEC 7811-9（TIM）、ISO/IEC 12905（ETA）
  - アプリケーションプログラミングインターフェース：ISO/IEC 24727
  - ヒューマンインタフェース付き IC カード：ISO/IEC 18328
  - 試験規格：ISO/IEC 10373、ISO/IEC 24789、ISO/IEC 18745

C. ISO/IEC JTC1/SC31

体制

ISO/IEC JTC1/SC31（以下、SC31という）の担当分野は、「Automatic identification and data capture techniques」であり、バーコードやRFID等に関する標準化を行っている。ISO/IEC JTC1/SC6、SC17等と関連がある。また、SC31はWGの下にさらにSGと呼ばれるサブグループを設置している。

組織のメンバーは、米国、欧州、中国が企業中心であるのに対し、韓国は研究機関が中心である。

以下、特にWG7に限定して説明を行う。

標準化の概要

SC31/WG7ではAutomatic identification and data capture techniquesのセキュリティに関する標準化を行っている。例えば、エアインターフェースの暗号化や低リソースチップにおける暗号化についての標準として、ISO/IEC 29167がある(次項目で示す)。WG7では暗号の決定の基準がStanding Documentとして次のように規定されている。

- 世界各国、多様な産業において利用されること。
- ISOのパテントポリシーに準拠すること。
- ビジネスニーズがあること。
- 実装可能であること。
- 既存の標準にないものであり、安全・頑丈であること。

暗号に関連する規格等

- ISO/IEC 29167-10 : AES-128
- ISO/IEC 29167-11 : Present-80
- ISO/IEC 29167-12 : ECC-DH
- ISO/IEC 29167-13 : Grain-128A
- ISO/IEC 29167-14 : AES-OFB
- ISO/IEC 29167-15 : XOR
- ISO/IEC 29167-16 : ECDSA-ECDH
- ISO/IEC 29167-17 : cryptoGPS
- ISO/IEC 29167-19 : RAMON

その他

- RFIDのセキュリティ標準に関して、例えば、乱数、鍵交換、及び電子署名等のような技術課題がある。

D. 制御機器・制御システム（ISA-99・IEC TC65/WG10）

制御システムのセキュリティ標準について

制御機器・制御システムのセキュリティ標準を行っている団体は数多くあるが、ここでは ISA-99 及び ISA-99 の規格である ISA-62443 を国際標準化している IEC/TC65 WG10 について取り上げる。

標準化の概要

ISA-99 の制御システムのセキュリティ標準である ISA-62443 では、ISA-62443-1「一般」(青)、ISA-62443-2「ポリシー・手順」(緑)、ISA-62443-3「システム」(橙)、ISA-62443-4「コンポーネント」（ピンク）の 4 層で構成されている。

現在 IEC TC65 WG10 では、制御システムのセキュリティについての標準として ISA-62443 等が参照され IEC 62443 の制定が行われている。

以下は ISA-62443 及び IEC 62443 の標準化の状況を示した表である。

ISA Reference	IEC Reference	Title	Status	IEC Status	頁数
ISA-62443-1-1	IEC/TS 62443-1-1	用語・概念・モデル	Published 2007第2版作成中	DC 2013Q1	92
ISA-TR62443-1-2	IEC/TR 62443-1-2	基準用語・略語	執筆中	DTR: 2013Q4	41
ISA-62443-1-3	IEC 62443-1-3	システムセキュリティ適合メトリックス	DC/コメント対応中	CDV: 2013:09.13 PUB: 2014Q2	77
ISA-TR62443-1-4	IEC/TR 62443-1-4	IACSセキュリティライフサイクル・適用例	提案された	未定	
ISA-62443-2-1	IEC 62443-2-1	IACSセキュリティプログラムの確立	Published	CDV: 2013Q3 FDIS: 2014Q1	149
ISA-TR62443-2-2	IEC/TR 62443-2-2	IACSセキュリティプログラムの運用	提案された	CDV:2013Q1	68
ISA-TR62443-2-3	IEC/TR 62443-2-3	IACS環境でのパッチ管理	DC/コメント対応中	DTR: 2013.10.13 PUB: 2014Q2	59
ISA-62443-2-4	IEC 62443-2-4	ベンダーセキュリティ能力	CDV投票中	CDV: 2013Q2 FDIS: 2013Q4	75
ISA-TR62443-3-1	IEC/TR 62443-3-1	IACSのセキュリティ技術	Published	PUB: 2009.07	97
ISA-62443-3-2	IEC 62443-3-2	セキュリティリスク評価とシステム設計 (Zones & Conduits)	DC/コメント対応中	CDV: 2013Q4 FDIS: 2014Q3	28
ISA-62443-3-3	IEC 62443-3-3	システムセキュリティ要件とセキュリティ保証レベル	ISA Published	PUB:2013Q2	74
ISA-62443-4-1	IEC 62443-4-1	プロダクト開発要件	DC/コメント対応中	DC:2012Q2 CDV:2013Q1	74
ISA-62443-4-2	IEC 62443-4-2	IACS構成部品のセキュリティ技術要件	DC/コメント対応中	DC:2012Q1 CDV:2013Q1	137

表 1. ISA-62443 及び IEC 62443 の標準化の状況

表中の 62443-2-4「ベンダーセキュリティ能力」、62443-3-3「システムセキュリティ要件とセキュリティ保証レベル」及び 62443-4-2「IACS 構成部品のセキュリティ技術要件」には暗号の利用に関する記述がある。

暗号に関連する規格等

ISA-62443（IEC 62443）では、直接暗号アルゴリズムの指定はないが、暗号アルゴリズムを規定した他の規格を参照することで、間接的に利用するアルゴリズムを指定している。次に示すのは、ISA-62443（IEC 62443）に記述されている暗号アルゴリズムに関する規格である。

- ISA-62443-3-3
  - IEEE802.11x
  - IEEE802.15.4（Zigbee 、IEC62591-WirelessHART、ISA-100.11a）
  - IEEE802.15.1（Bluetooth）
  - RFC3647
- ISA-62443-4-2
  - ISO/IEC 19790:2012

その他

- 制御システム業界からの暗号技術への要望
  制御組込機器の CPU は、一般の PC 等に搭載されている CPU よりも性能が 1 ケタから 2 ケタ程度劣る。さらに、制御システムはその性質上、処理速度に対する実時間制約が非常に厳しい。そのため、市場（開発側及び購入者側の両方）からはパフォーマンスに優れ、知名度があり、攻撃に対する改善実績や危殆化に対する配慮のある暗号が求められている。特に、制御システムの開発側では暗号の開発・導入に割ける工数が非常に限られるため、暗号を透過的に導入・利用できる開発環境やライブラリ等がパッケージとしてほしいという要求がある。よって、制御システム業界では、軽量な暗号技術や超軽量な暗号技術のシリーズが望まれている。

E. IEEE802.11

体制

IEEE（米国電気電子学会）は、一般的な学会活動の他に IEEE-SA（IEEE Standards Association）にて標準化活動を行っている。IEEE-SA の下には様々な委員会があり、IEEE802 LMSC では LAN/MAN の標準化が行われている。委員会の下には WG が設置されているが、特に IEEE802.11 WG では、無線 LAN の標準化が行われている。また、IEEE802.11 WG は 8 つのタスクグループ（TG）、5 つのスタンディングコミッティ（SC）、及びスタディグループ（SG）から構成されている（2014 年 2 月 10 日現在）。

標準化の概要

IEEE802.11 の会合は年 6 回開催され、会合での議決と書面投票によって意思決定が行われる。議決は多数決によって行われ、技術的な事項の議決には 75%の支持を得なければならない。投票は投票権所有者のみが行うことができ、投票権は企業や団体ではなく、「個人」に付与される。議事運営は、ロバートルールによる。

ロバートルールでは、4 つの権利が守られる。①多数決の権利（過半数の賛成）②少数者の権利（少数意見の尊重）③個人の権利（プライバシーの権利擁護）④不在者の権利（不在投票）である。また、その他に守るべきルールとして、例えば、次のようなものがある。

- 発言者は議長とのみ話すことができる。
- 動議提案には 2 人以上の賛成が必要。
- 不十分な動議は棚上げされ、会議満了で失効する。
- 一度議決されたものは審議できない。

投票権は 4 回の連続する Plenary のうち、3 回目の出席で、取得できる。3 回のうち 1 回は Interim で代用できるが、投票権の付与は Plenary のみである。セッションの 75%以上に出席しなければ、「出席」とは認められない。投票権の維持には、直近 4 回の Plenary 中 2 回に出席が必要である。

標準化の具体的な策定作業は TG が行う。TG を作るためには、図 2 に示すように、まず、SG を作り、「Project Authorization Request」及び 5 つの Criteria に関する付随文書を作成しなければならない。5 つの Criteria は、次のようになる。

- その規格を作ることによって、市場が伸びるのか（Broad Market Potential）
- 現在の技術と互換性があるのか（Compatibility）
- その技術は 802.11 WG で標準化すべき技術なのか（Distinct Identity）
- 技術面で実現可能性があるか（Technical Feasibility）
- 経済面で実現可能性があるか（Economic Feasibility）

その後、標準化は、図 3 のプロセスに従って行われる。

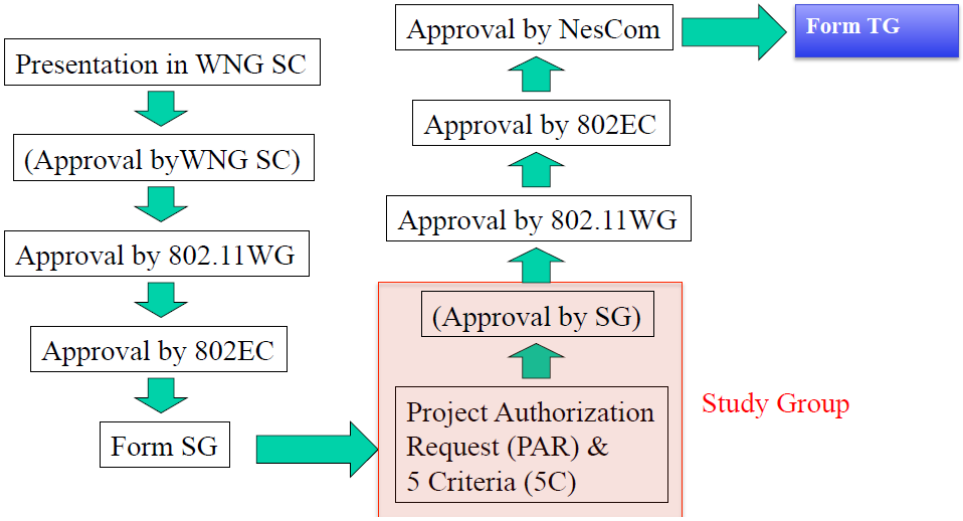


図 2. TG ができるまで

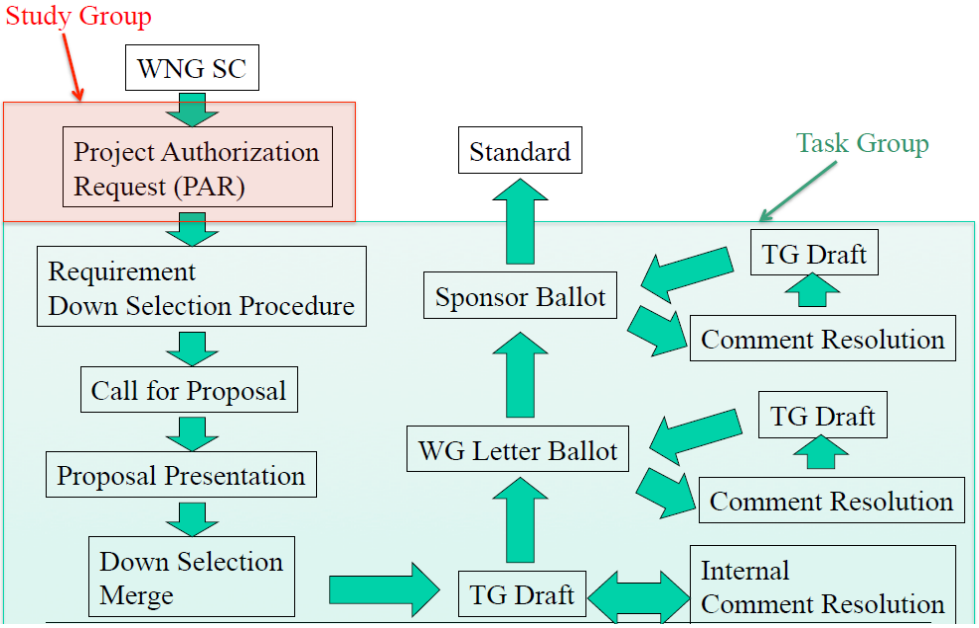


図 3. 標準化のプロセス

暗号に関連する規格等

IEEE802.11 は当初 WEP を採用したが、セキュリティの脆弱性が指摘され、802.11i によって修正された。IEEE802.11 はセキュリティに対して非常に慎重であり、規格化のためにはセキュリティエキスパートと呼ばれる著名な人のレビューが必要である。また、暗号化アルゴリズム等の採用については NIST の承認が絶対的に支持されている。

F. TCG

体制

Trusted Computing Group （以下、TCG）は、国際業界標準規格制定のための組織である。TCG では、会員によって技術仕様の策定が行われ、完成した仕様書は、社会での利用と実装が可能となるよう一般に公開される。TCG の会員による実装は、結果として TCG 技術の実用例となる。TCG の組織は、個々の技術分野の専門家が共同で仕様を開発可能にするため、ワーキンググループモデルで組織されている。このワーキンググループモデルは、協業及び競合の立場にある企業がベンダーに中立的かつ相互運用性のある最も良い仕様を開発できる中立的な環境を保ち続ける。TCG の体制図を次に示す。

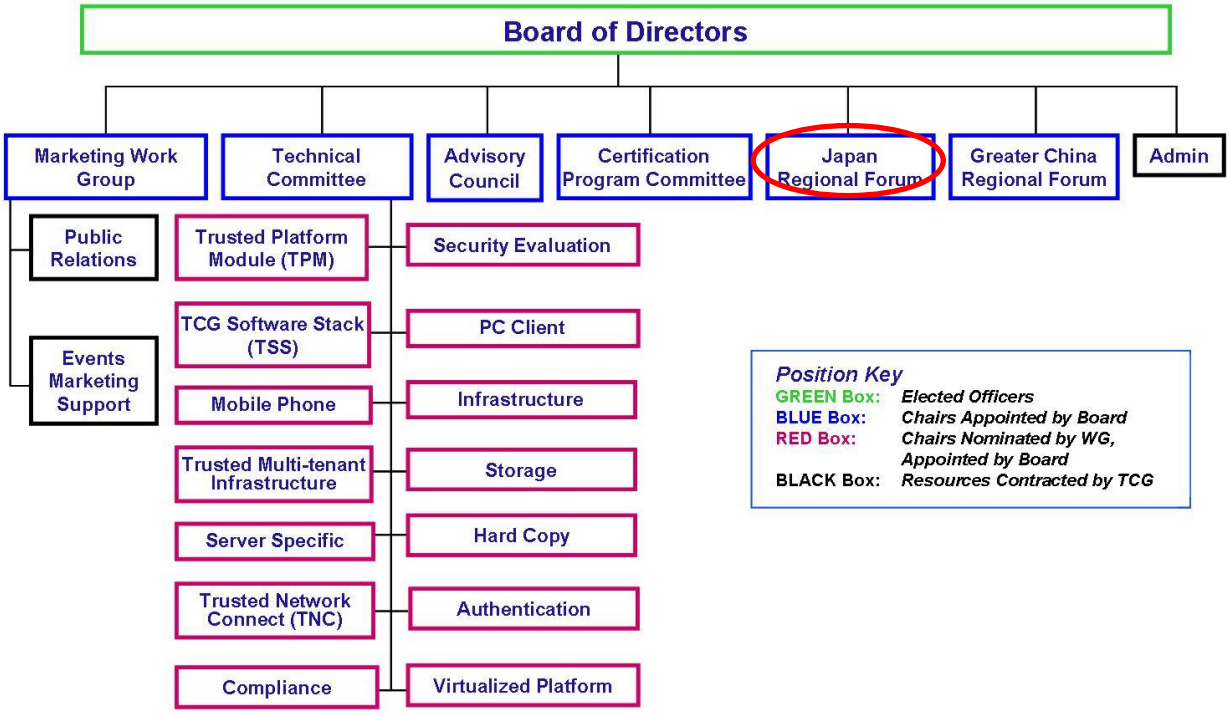


図 4. TCG の体制

Japan Regional Forum（以下、JRF）は TCG 内部の組織であり、日本の TCG 会員により構成される。JRF の目的は、TCG 技術の日本での普及及び採用働きかけ、日本政府・業界・市場と TCG の橋渡し、日本にいる TCG 会員の日本語での TCG 技術に関する情報交換の場を提供することである。

標準化の概要

TCG で策定する標準規格は次のような事項が考慮されている。

- 標準規格のインターフェースを用いた実装による、全世界での相互運用性と互換性の促進。
- TCG 技術による製品を提供する側と利用する側の双方でのコスト削減。

- 標準規格のプロトコルや機構による開発の効率化。
- 標準規格で公開され、専門家による綿密な評価、協力等により国際的に認められたセキュリティのプロトコルや暗号技術の利用。
- ハードウェアとソフトウェアのうまい組み合わせによる、安全なコンピューティング環境の構築。

暗号に関連する規格等

TPM[2]

その他

現在、METI 及び IPA が TPM 2.0 仕様書への日本の暗号アルゴリズム採用に向けた取り組みを行っている。TCG はこの仕様書を、ISO 国際標準とすべく活動をする予定である。METI/IPA は、2012 年 11 月、2013 年 2 月、3 月に Registry 仕様書へのレビュー及びコメントを行い、2013 年 5 月に JRF を通じて TCG の Board of Directors に Camellia 及び KCipher-2 の採用の打診を行った。また、2013 年 10 月には大阪にて、TPM WG へ Camellia の紹介と正式な評価依頼を行った。その後、2014 年 2 月にソルトレークシティ・メンバーミーティングでの活動も含め、現在も採用に向けた取り組みは続いている。

[2] Trusted Platform Module の略

G. 長期署名（ETSI）

体制

日本での電子署名（長期署名を含む）の標準化は日本ネットワークセキュリティ協会（以下、JNSA という）が行っている。電子署名の標準化活動を行う上で、JNSA は、特定認証業務の認定を行う日本情報経済社会推進協会（以下、JIPDEC という）やタイムスタンプ事業者認定等を行う日本データ通信協会（以下、JADAC という）とも調整を行う。また、医療分野における電子署名標準化を行っている保健医療福祉情報システム工業会（以下、JAHIS という）とは専門家同士の交流が行われている。2013 年より、JNSA は ETSI に加入し、日本からの意見を国際標準に反映すべく活動を行っている。

ETSI や CEN は欧州委員会からの標準化の指針に従って技術や運用に関する標準の策定を行う。その標準に従って、欧州内の各国が製品やサービスを開発・運用し、さらには事業者の監査や認定を行う。このようにヨーロッパでは、欧州委員会のトップダウンによる体系化されたアプローチを採り、制度と技術が結びついた整合性のあるフレームワークを目指している。

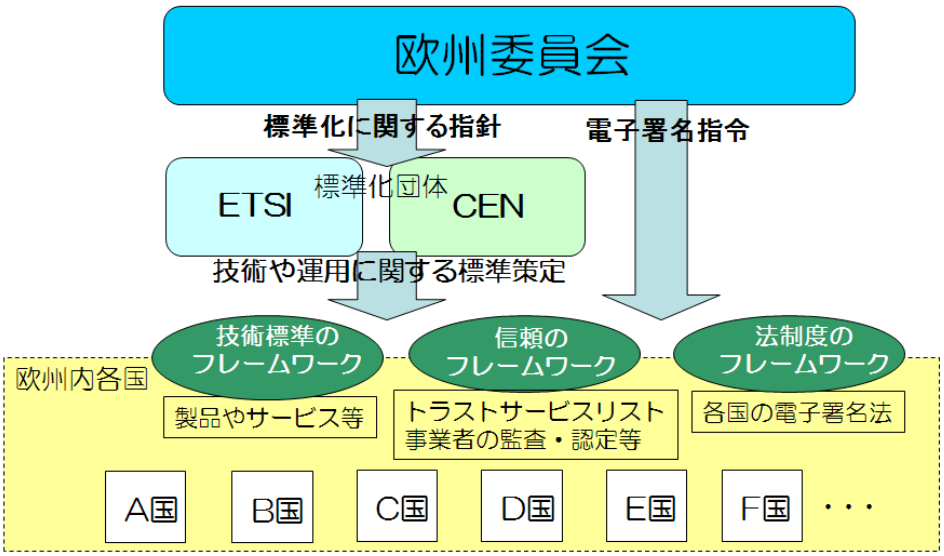


図 5. 欧州の体制

標準化の概要

電子署名は現在、CAdES[3]、 XAdES[4]、 PAdES[5]、ASiC[6]の 4 種類が ETSI で策定されている。このうち CAdES、XAdES については、長期保存のための要件を定めたプロファイル規格を日本が作成し、JIS 化及び ISO 化を行った。このプロファイル規格を元に JAHIS にて医

[3] CMS Advanced Electronic Signature の略
[4] XML Advanced Electronic Signature の略
[5] PDF Advanced Electronic Signature の略
[6] Associated Signature Container の略

療向けの電子署名プロファイルを規格化し、現在 ISO 化の作業を行っている。

- JIS X 5092:2008 CMS 利用電子署名(CAdES)の長期署名プロファイル
- JIS X 5093:2008 XML 署名利用電子署名(XAdES)の長期署名プロファイル
- ISO 14533-1:2012, Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)
- ISO 14533-2:2012, Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)

ISO/DIS 17090-4 Health informatics -- Public key infrastructure -- Part 4: Digital Signatures for healthcare documents

日本の電子署名法は市場主導型の米国の電子署名法ではなく、欧州の規制型の電子署名法に近い。ETSI では、法制度と整合性のとれた技術・運用の電子署名標準規格を作成している。ETSI の電子署名標準は国際的な電子署名規格としての影響力を持ち、実証実験等を通じて「使える標準規格」を目指す意識が強い。

上記のように既に欧州で電子署名標準の枠組みが作られており、日本発の電子署名技術を国際的な影響力を持つ標準にすることは難しい現状であるため、日本は欧州の標準に意見を投じ、国際的な標準へ反映させようとしている。その一環として、ETSI の標準化活動に対して、日本は様々な貢献をしている。例えば、電子署名の相互運用性を検証するための ETSI オンライン実証実験は日本で実施した実証実験がモデルとなっている。また、ETSI 電子署名規格への提言を行い改訂に至った。その他には、PDF に対する長期署名規格の必要性を訴えて PAdES 策定のきっかけを作ったり、CAdES 及び XAdES 長期署名プロファイルの ISO 規格を作成したりする等の様々な働きかけを行い、標準化活動に貢献している。

暗号に関連する規格等

電子署名に関する規格は次のように、参照されている。

表 2.電子署名の規格の参照

	ETSI	JIS	ISO	その他
CAdES	ETSI TS 101 733 (v2.2.1)	JIS X 5092:2008	ISO 14533-1 (2012)	JAHIS HPKI署名規格
XAdES	ETSI TS 101 903(v1.4.2)	JIS X 5093:2008	ISO 14533-2 (2012)	JAHIS HPKI署名規格
PAdES	ETSI TS 102 778 (v1.1.2)	検討中	検討中	なし
ASiC	ETSI TS 102 918 (v1.2.1)	なし	なし	なし

欧州ではこれまでも電子署名の規格だけではなく、署名生成デバイスに関する規格や電子証明書を発行する認証局や、タイムスタンプ発行局の運用に関する規格など周辺の様々な規格策定を行ってきた。現在、これらの規格の体系について見直しが行われている。これまでの規格の統廃合、機能領域の分類と整理を行い、新フレームワークを構築している。この新フレームワークには電子署名に用いられる推奨暗号リストの作成も含まれている。

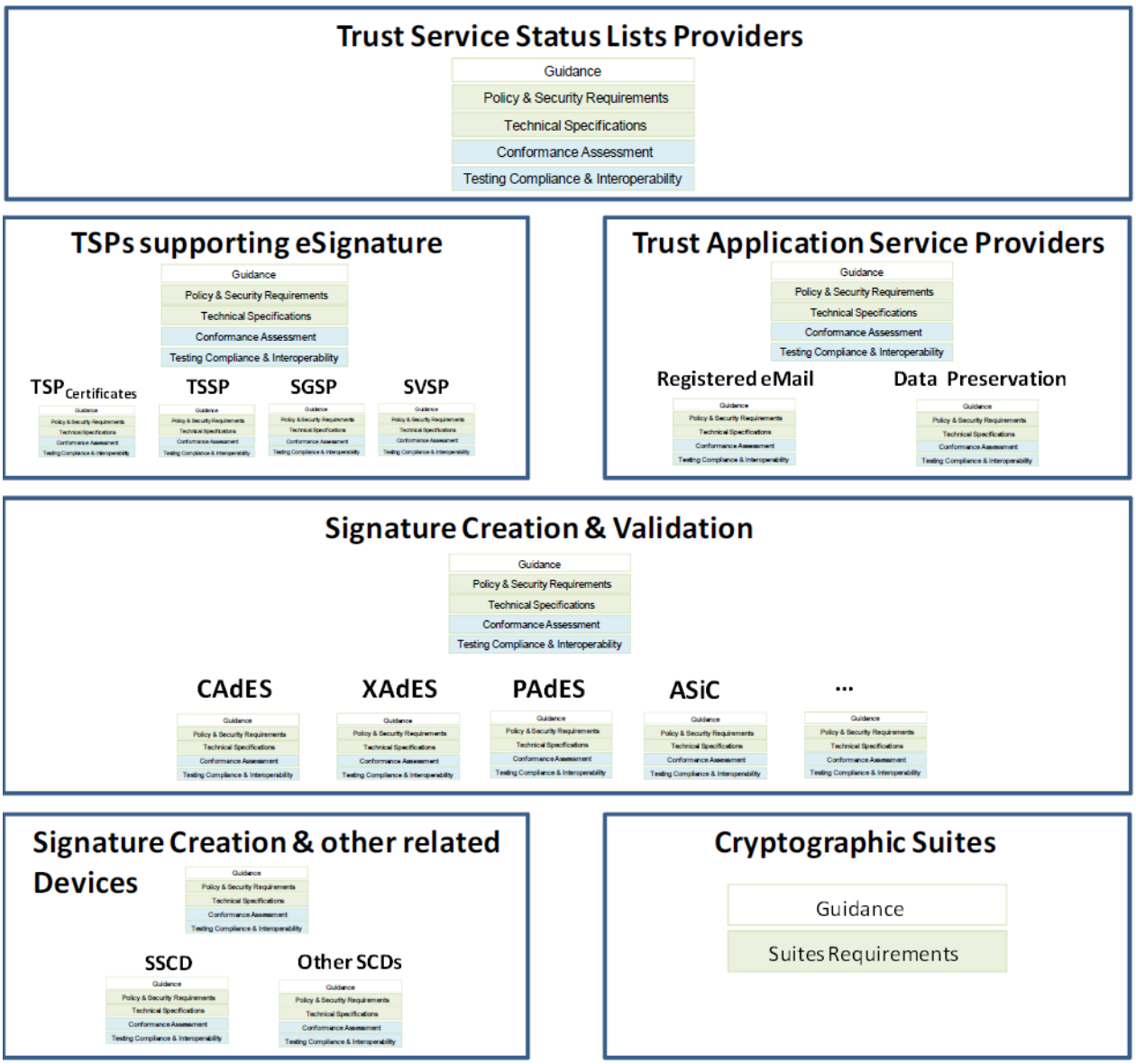


図 6. 欧州の新フレームワーク[7]

[7] 出典：ETSI SR 001 604 V1.1.1 p.17

<u>その他</u>

- 現状の課題

  ETSI の電子署名標準に関しては、EU 独自の仕様が入り込む可能性がある。標準（規格）が国際的な影響力を持つことを意識しているはずだが、EU のトップダウン的な電子署名指令があり、EU の問題であるという意識を持つ傾向がある。日本からも問題点を指摘しているが、全ての意見が反映されるわけではない。

  日本の電子署名に関する課題は、国内に長期的展望で標準技術に関与できる組織がないことである。日本の各省庁、各業界団体はそれぞれのスコープに閉じており、全体を俯瞰して議論をする場、技術標準を取りまとめる場が日本にはない。例えば、電子証明書を発行する認証局の特定認証業務の認定は経済産業省、タイムスタンプは総務省といったように、省庁や業界団体が縦割りであり、それぞれのスコープが限定的でビジョンが共有されていない。欧州の新フレームワークのような体系化されたアプローチは困難な状況にある。

- 電子署名標準化に関する今後の予定
  - ISO 14533-1 (CAdES 方式)の改訂作業

    今年発行された新しい ETSI 規格の内容に合わせた ISO 14533-1 (CAdES 方式)の修正作業を行っている。近々DIS 投票が行われる予定である。
  - PDF 電子署名(PAdES 方式)に関する長期保存のためのプロファイル規格策定

    PDF 電子署名（PAdES 方式）に関する長期保存のためのプロファイル規格を策定し、2 月にドラフトを発表した。今後は本規格の ISO 化を目指す。
  - 電子署名の検証規格

    現在、電子署名の検証方法を明確化した規格を ETSI で定めている。欧州内の事情を色濃く反映したものになっているため、日本が代案を提案している。なお、ISO 規格化も視野に入れている。

H. 放送

体制

- 総務省　情報通信審議会
  - ➢ 情報通信技術分科会
    - ✧ 放送システム委員会
- 電波産業会（ARIB）技術委員会

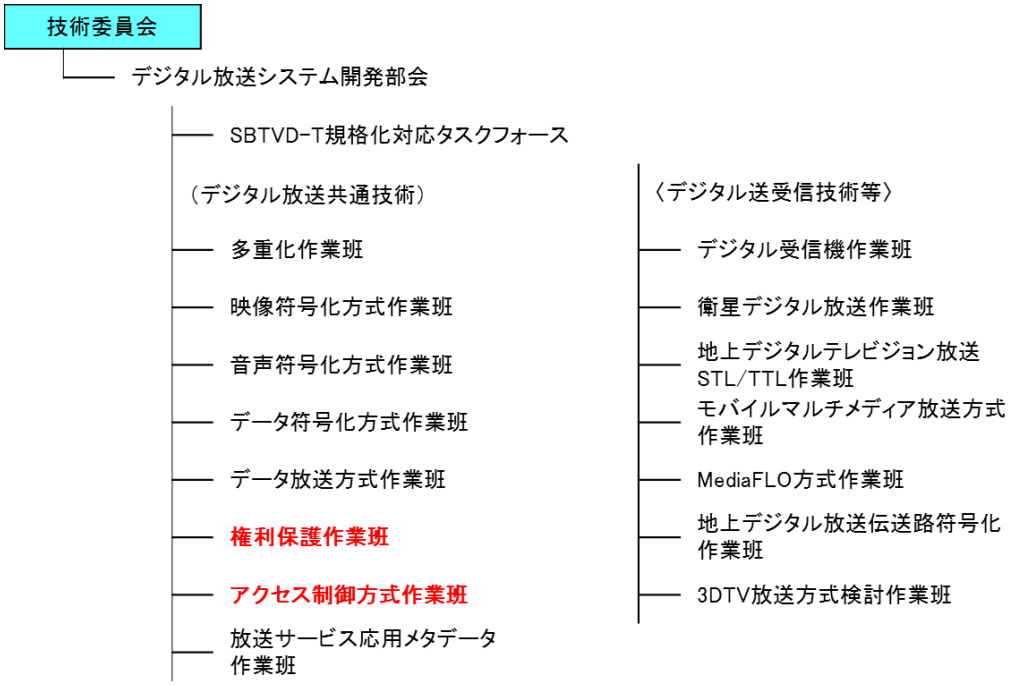


図 7. ARIB 技術委員会 デジタル放送システム開発部会の体制

標準化の概要

放送コンテンツの権利保護とアクセス制御（限定受信方式）には暗号技術が利用されている。現行の BS デジタル放送や地上デジタル放送等のアクセス制御方式（限定受信方式）は、総務省 情報通信審議会で審議され策定された。現在、新たな映像符号化方式等、現行の高精細度テレビジョン放送を超える飛躍的な画質の向上に資する映像技術等の研究開発等の進展に伴って、情報通信審議会では、「超高精細度テレビジョン放送」の実用化、普及促進等を図るため、必要な技術的条件が取りまとめられている。

- 情報通信審議会
  - ➢ 超高精細度テレビジョン放送システム標準化の経緯

    通信・放送サービスに関する今後の取組みについて、平成 24 年 7 月、情報通信審議会から「4K・8K（スーパーハイビジョン）」、「スマートテレビ」、「ケーブル・プラットフォーム」の 3 つの WG についての提言が行われた。その具体化に必要な事項を検討することを目的として「放送サービスの高度化に関する検討会」が開催され、「スーパーハイビジョン WG」「スマートテレビ WG」及び「ケーブル・プラットフォーム WG」の 3 つの WG が設置された。平成 25 年 6

月 11 日に検討結果の取りまとめが公表され、スーパーハイビジョンに関するロードマップが示された。(2014 年に 4K の試験的な放送を開始、2016 年に 8K の試験的なサービスを実施、2020 年に 8K の本放送を開始)

- 情報通信審議会　情報通信技術分科会　放送システム委員会
  5 回にわたり超高精細度テレビジョン放送システム作業班を開催し、2014 年 1 月 31 日に放送システム委員会にて作業班の最終報告を行った。最終報告では、限定受信方式におけるスクランブルサブシステム[8]および関連情報サブシステム[9]の技術的条件等が示された。

- ARIB
  権利保護作業班及びアクセス制御方式作業班（体制図の赤字部）にて、情報通信審議会の答申を受け、超高精細度テレビジョン放送の限定受信方式及びコンテンツ保護方式に関し、A 標準規格「デジタル放送におけるアクセス制御方式」(ARIB STD-B25）を改定する。

暗号に関連する規格等

- BS デジタル放送：MULTI2
- 地上デジタル放送：MULTI2
- 携帯端末向けマルチメディア放送：MULTI2、AES、Camellia
- 超高精細度テレビジョン放送システム：「AES」と「Camellia」の鍵長 128 ビットから選択可能

その他

超高精細度テレビジョン放送システムにおいて、暗号に関して次のような課題がある。

- スクランブル方式の暗号アルゴリズムの選定にあたっては、次の事項に留意することが望まれる。
  - スクランブル方式は、暗号アルゴリズム自身の安全性だけではなく、受信機における実装面、コスト面及び実用化スケジュールの状況、ならびに、長期にわたってセキュリティリスクを抑える送出運用等を考慮して、民間規格や運用規定に関する検討の場において、放送事業者や受信機製造メーカ等の関係者で最終的に選定する必要がある。
  - 長期的視点で見ると、より効率的な暗号解析手法が見つかる可能性も否定できない。CRYPTREC の電子政府推奨暗号リストの改定等、暗号アルゴリズムの最新動向を引き続き注視する必要があり、また、民間規格や運用規定に関す

[8]スクランブルサブシステム：未契約者には信号が受信できないように信号を暗号化して送り、既契約の受信機で復号する仕組み
[9]関連情報サブシステム：デスクランブルを行うか否かを制御するための情報（関連情報※）を処理する仕組み

る検討の場において、必要に応じて、さらなる議論、検討が行われる必要がある。

- 超高精細度テレビジョン放送のスクランブル方式に関して、脆弱性が発見された場合においても適切に対応可能とするため、複数の暗号アルゴリズムから選択可能とすることを検討したが、今後、秘匿性維持の観点で、メディアに対して横断的な利用についても検討することが重要である。その際、現行放送との整合性に留意する必要がある。

I. 医療（ISO TC215）

ISO TC215 の対象範囲

ISO TC215/WG4 では、ヘルスケア情報領域におけるセキュリティとプライバシー保護に関する標準の策定を次のために行う。

① ヘルスケア情報の完全性、機密性、可用性の保持と拡大
② 患者の安全に悪影響を与えるものからのヘルスケア情報システムの防護
③ 個人情報に関わるプライバシー保護
④ ヘルスケア情報システムの利用者に対する責任の明確化

体制

ISO TC215 のコンビナーは、Lori Leed Fourquet（米国）であり、2013 年 6 月より二期目就任を果たしている。副コンビナーは茗原秀幸（日本）であり、2013 年 6 月より新任である。また、セクレタリは、Diana Warner（米国）が 2012 年度より就任している。

国内には、ISO TC215 国内対策委員会があり、その下に WG4 作業部会がある。WG4 作業部会の主なメンバーは、JAHIS、JIRA、JAMI、MEDIS-DC、厚生労働省となっている。

標準化について

JAHIS セキュリティ委員会では、ISO TC215/WG4 に関するエキスパートとして国内対策委員会にメンバーを派遣している。セキュリティ委員会では、各規格の対応の検討や投票コメントの検討等を実施している。さらに詳細な検討が必要な場合には、JAHIS の担当 WG にて具体的な翻訳作業、詳細仕様の検討等を実施する。また、JIRA セキュリティ委員会と積極的に意見交換を実施し、産業界としての統一見解の取りまとめを実施している。日本としての投票の際には、JAHIS の見解として ISO TC215 国内対策委員会 WG4 作業部会(大山部会長：東京工業大学) に対して意見具申を行う。その他には、JAHIS 標準類の ISO 規格への組込みを積極的に実施し、逆に制定済み ISO 規格の JAHIS 標準類への反映も実施している。

ISO TC215/WG4 の主要な規格について

ISO TC215/WG4 の主要な規格の例を次に示す。

- Health Informatics - Guidelines on data protection to facilitate trans-border flows of personal health information (IS22857)
  - IS22857 は国や地域をまたがる個人ヘルスケア情報のやりとりにおける個人情報保護の IS であり、WG4 における最初に策定された国際標準である。EU 指令や HIPAA 法等を参照し、個人情報保護に関する要件を定めている。また、各国の慣習や文化の違いを考慮して、各国の法律と本規格に差異があった場合の対処も記載されている。また、JAHIS セキュリティ委員会の検討結果を受けた日本の要請により死者の情報に対しても情報保護を要求する等、ヘルスケア独自

の要素が組み込まれている。現在は規格成立3年後のシステマティックレビュー（以下SR）の結果として修正されたFDIS投票が完了し、出版待ちの状態である。また、CENの関連規格と統合し新たな規格とする作業項目提案が通過しており IS16864 として検討が開始される予定である。

- **Health informatics - Public key infrastructure (IS17090)**
  - IS17090はヘルスケア部門向けのPKI(HPKI)に関するISである。Part1－Part3は IS として出版され、Part4 は現在策定中である。本規格は日本の厚生労働省の認証局ポリシーと整合性が取られている。
    - ✧ **Part1 Framework and overview**： HPKI のフレームワーク及び概要を記載している。発行対象の種類（自然人、アプリケーション等)、役割の種別等が規定されている。SRの結果､改定版がFDISを通過して出版された。
    - ✧ **Part2 Certificate profile**： HPKIの証明書に記載される内容について記載している。PKI としての標準的な箇所の定義とヘルスケア独特のhcRoleの定義がなされている。SRの結果、改定版のFDIS投票が行われる予定である。
    - ✧ **Part3 Policy management of certification authority**：認証局における認証ポリシー作成のためのガイドラインを記載している。SR でそのまま承認された。
    - ✧ **Part4 Digital Signatures for healthcare documents**：日本の JAHIS標準をそのままISOに提案したものである。日本主導で規格化を行っている。現在DIS投票にかかっている。
- **Health Informatics - Dynamic on-demand virtual private network for health information (TR11636)**
  - TR11636はVPNを医療分野に適用した場合のメリット等について実際の利用例をベースにまとめたTRである。日本のHEASNETの報告書をベースに策定された。

J. M2M/IoT に関係する標準化団体（ISA-100・IEEE1888・ISO/IEC JTC1/SC6/WG7・IETF）

J.1. ISA-100

体制

ISA-100 の体制についての概略図を次に示す。

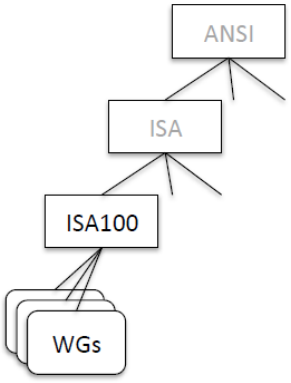


図 8. ISA-100 の体制についての概略図

標準化について

工業向け計測制御無線システムの技術の検討と標準化を行うことを目的としている。データリンク層からアプリケーション層の技術やシステムまでを標準化の対象としている。ISA-100 では、セキュリティは必須項目であり、基本となる技術を規定する ISA100.11a WG では Security Sub-WG が設立された。バックホールを含むシステムについて、ISA-99（工業ネットワークのセキュリティを扱うグループ）とリエゾン関係である。

暗号に関する規格等について

- ISA100.11a では、IEEE802.15.4 で使用する AES128-CCM をエンドノード間の暗号化と認証にも再利用している。
- システム全体では、FW 技術や IPsec、TLS、IEEE802.1X を使用する。
- Wi-Fi Security として WPA/WPA2 を利用する。

J.2. IEEE1888

体制

IEEE1888 の体制についての概略図を次に示す。

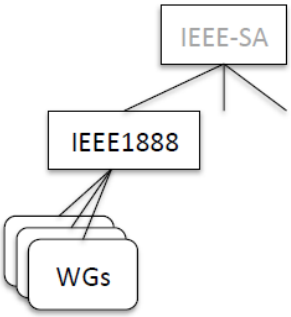


図 9. IEEE1888 の体制についての概略図

標準化について

ビルや設備等の統合エネルギー管理を目的とした通信技術の標準化を行う。トランスポート層からアプリケーション層の技術及びシステムまでを標準化の対象とする。運用実績のある技術を再利用してシステムとして動作する技術を検討している。

暗号に関する規格等について

IEEE1888.3 では、機器の Identifier を定義し、X.509 証明書での表現方法と ACL に対する必須要件、TLS の用法を定義している。トランスポート層のセキュリティとして TLS を参照し、アプリケーション層のセキュリティ技術として X.509 証明書を用いる。

J.3. ISO/IEC JTC1/SC6/WG7

体制

SC6 の体制についての概略図を次に示す。

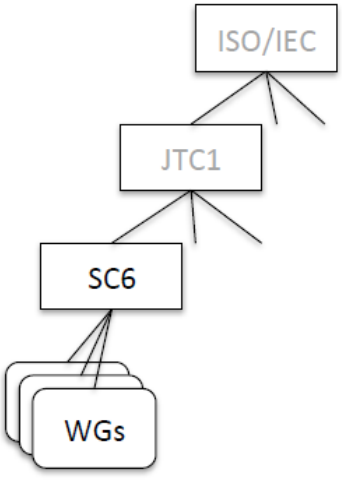


図 10. SC6/WG7 の体制についての概略図

標準化について

情報システム間の通信技術の国際標準化を行うことを目的としている。データリンクより上のレイヤの技術を対象としている。また、“Future Network”も扱う。各国の技術

を標準化する傾向が強いため、運用実績や相互接続性のレベルが異なる。なお、セキュリティの専門家は非常に少ない。

暗号に関する規格等について

IETF で標準化された技術を参照し、リエゾンする場合もある。

J.4. IETF

体制

IETF は 8 つの Area、約 120 の WG から構成される。インターネット全般の技術全般を扱うため WG は非常に多い。Security Area 以外の WG の参加者はセキュリティの知識が少ない傾向にある。セキュリティプロトコルに関しては、他のグループとリエゾンすることが多い。体制図については、K 節（後述）に示す。

標準化について

インターネット技術全般のデファクト標準化を行うことを目的としている。データリンクより上のシステムを標準化の対象としている。また、アプリケーション層の技術を含む場合もある。会社や国の代表としてではなく、個人として議論に参加する。全ての議論や文書が公開されており、誰でも自由に議論に参加でき、文書を発行できる。また、各標準化団体が定める技術に再利用される傾向が強い。

十分に検討された技術は RFC（Request for Comments）として発行される。運用と相互接続の結果、改定されることがある。十分な動作実績のある仕様と相互接続性が最も重要とされている。

暗号に関係する WG について

Security Area でも暗号アルゴリズムの扱いを議論する WG は限られている。例えば、TLS、kitten、IPsec、PKIX 等である。暗号アルゴリズムについては Security Area Advisory Group で議論される。研究段階のものは、CFRG でも議論される場合がある。

J.1 から J.4 のまとめ

ISA-100、IEEE1888、ISO/IEC JTC1/SC6/WG7、IETF は M2M/IoT に関係する標準化団体である。各標準化団体はインターネット技術、セキュリティプロトコル及び暗号アルゴリズムにおいては、IETF が策定した技術を利用する傾向が強い。その結果として、IETF に様々な暗号アルゴリズムが提案されている。なお、データリンク層の技術については、IEEE が定めた技術を利用する傾向が見られる。

K. IETF

体制

IETF はインターネット技術の標準仕様を策定することを目的として組織されたグループであり、IETF における技術仕様は RFC（Request for Comments）という名前で文書化され、公開される。RFC は、IESG の承認後、番号が割り当てられ、IANA レジストリに登録される。その後、RFC Editor によって公開される。IETF の体制図を次に示す。

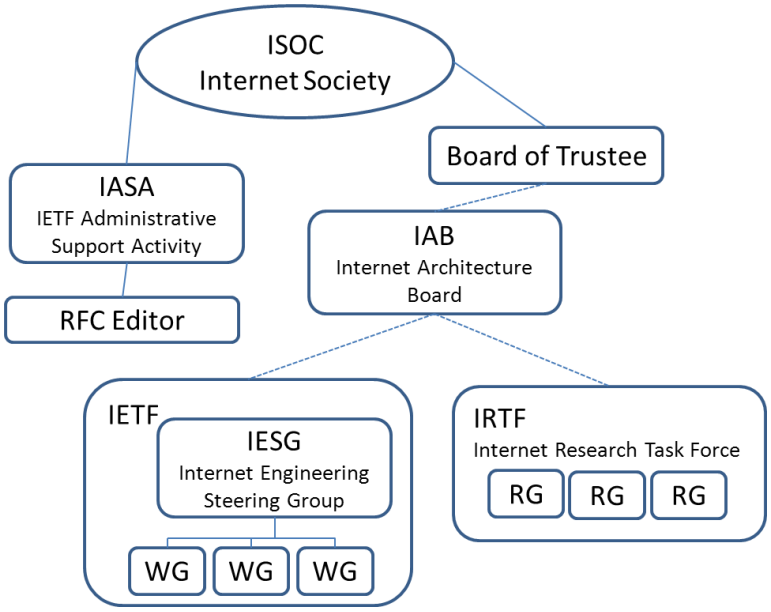


図 11. IETF の体制

標準化の概要

標準化のプロセスを次に示す。

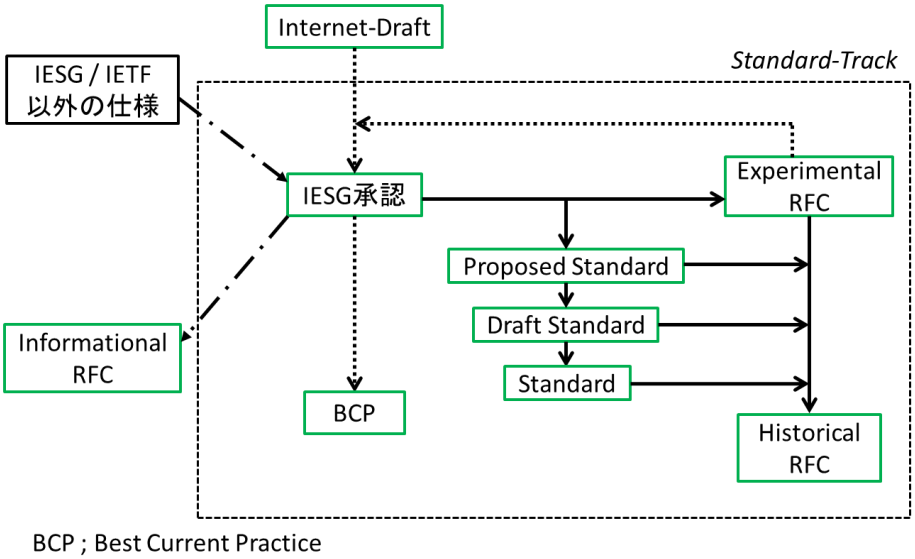


図 12. RFC 化のプロセス[10]

[10] JPNIC https://www.nic.ad.jp/ja/tech/ietf/section4.html

RFC は Informational RFC、Standard Track RFC、Experimental RFC、及び Historical RFC の 4 種類に分かれる。そのうち、標準とされるのは Standard Track である。これは、Working Group でコンセンサスが取られ、業界で国際標準とすべき仕様をまとめたドキュメントである。PS(Proposed Standard)、DS(Draft Standard)を経て、S(Standard)となる。PS は複数の組織での独立な実装テストと相互接続性の確認が条件、DS は実質的かつ広範囲での運用テストが条件となっている。S(Standard)の状態になると、STD 番号が割り振られる。現在、STD 番号を割り振られているドキュメントは非常に少数であり、実質的には、DS の RFC になると、国際標準とみなすことができる。

IETF の標準化活動は、メーリングリスト（以下、ML という）やミーティングにて行われる。ML には、アナウンス ML や WG のディスカッション ML 等がある。IETF のミーティングは年 3 回行われる。その他に WG やワークショップの中間（Interim）ミーティングも行われる。

暗号に関連する規格等

- TLS
  AES-CCM (AES-counter with CBC-MAC) が 2012 年 12 月に RFC6655 として追加された。
  また、2013 年 11 月の IETF88 にて、ChaCha20 の追加に向けた動きがあった。
- DNSSEC
  特に大きな動きはなく、既存の RSA、GOST、ECDSA 等が IANA レジストリに登録されている。2013 年 4 月に RFC6944 にて、RSA/MD5 が「MUST NOT」となった。
- IPsec
  特に大きな動きはなく、AES-CBC、Camellia-CBC 等が利用可能である。
- RPKI
  2012 年 2 月 RFC6485 にて、RSA2048、SHA-256 のみが指定されている。

以上

発行日　2014 年 7 月 14 日　第 1 版
発行者
・〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
独立行政法人 情報処理推進機構
（技術本部　セキュリティセンター　暗号グループ）
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
2-28-8 HONKOMAGOME, BUNKYO-KU
TOKYO, 113-6591 JAPAN

・〒184-8795
東京都小金井市貫井北町四丁目 2 番 1 号
独立行政法人 情報通信研究機構
（ネットワークセキュリティ研究所
セキュリティ基盤研究室、セキュリティアーキテクチャ研究室）
NATIONAL INSTITUTE OF
INFORMATION　AND COMMUNICATIONS TECHNOLOGY
4-2-1 NUKUI-KITAMACHI, KOGANEI
TOKYO, 184-8795 JAPAN