暗号技術活用委員会活動報告

2015年3月20日

暗号技術活用委員会委員長

松本 勉

（横浜国立大学）

CRYPTREC
Cryptography Research and Evaluation Committees

目次

CRYPTREC
Cryptography Research and Evaluation Committees

1. 暗号技術活用委員会の概要

CRYPTREC体制

CRYPTREC体制図

暗号技術検討会
（事務局：総務省、経済産業省）

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**検討課題を担当

暗号技術評価委員会
（事務局：NICT, IPA）

（1）暗号技術の安全性及び実装に係る監視及び評価
（2）新世代暗号に係る調査
（3）暗号技術の安全な利用方法に関する調査

- **暗号解析評価WG**
- **軽量暗号WG**

暗号技術活用委員会
（事務局：NICT, IPA）

（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
（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

- **運用ガイドラインWG**
- **標準化推進WG**

CRYPTREC
Cryptography Research and Evaluation Committees

2014年度暗号技術活用委員会委員

委員長	松本　勉	横浜国立大学　大学院環境情報研究院　教授
委員	上原 哲太郎	立命館大学　情報理工学部情報システム学科　教授
委員	遠藤 直樹	東芝ソリューション株式会社　技術統括部　技監
委員	川村　亨	日本電信電話株式会社　研究企画部門　プロデュース担当（セキュリティ） 担当部長／チーフプロデューサ
委員	菊池 浩明	明治大学　総合数理学部　先端メディアサイエンス学科　教授
委員	鈴木 雅貴	日本銀行　金融研究所　情報技術研究センター　主査
委員	高木　繁	株式会社三菱東京UFJ銀行　システム部システム企画室　次長
委員	角尾 幸保	日本電気株式会社　パブリックビジネスユニット　宇宙・防衛事業推進本部 主席技術主幹
委員	手塚　悟	東京工科大学　コンピュータサイエンス学部　教授
委員	松井　充	三菱電機株式会社　情報技術総合研究所　技師長
委員	満塩 尚史	内閣官房　IT総合戦略室　政府CIO補佐官
委員	八束 啓文	EMCジャパン株式会社　RSA事業本部　技術統括部 システムズ・エンジニアリング部　部長
委員	山口 利恵	東京大学　大学院情報理工学系研究科　ソーシャルICT研究センター　特任准教授
委員	山田　勉	株式会社日立製作所　日立研究所　エネルギーマネジメント研究部　ES3ユニット ユニットリーダ主任研究員
委員	山本 隆一	東京大学　大学院医学系研究科　医療経営政策学講座　特任准教授

CRYPTREC
Cryptography Research and Evaluation Committees

2014年度暗号技術活用委員会活動内容

(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

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行った。2013年度に続き、議論を行う上で有用な基礎データの収集を上期に実施し、これをもとに、下期に検討を実施した。

(2) 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同時に検討した。

(3) 標準化推進

様々な組織が日本からの暗号アルゴリズムの提案を行う場合に、その成果が効果的に得られるようにするための有望な標準化提案先の選定、当面必要とされる稼働見積りや交渉方法、提案活動における課題等を、標準化推進WGにおける検討をもとに取りまとめている。

(4) 運用ガイドライン作成

2013年度にドラフト版を作成した「SSL/TLSサーバ構築ガイドライン」について、引き続き運用ガイドラインWGで作業を行い内容を大幅に改良し、委員会として成果物を取りまとめている。

2014年度暗号技術活用委員会審議状況

回	開催日時	主な議題
—	メール審議	● WG活動計画案の審議・承認
第1回	2014. 10. 30	● 活用委員会活動計画の確認 ● RC4の注釈について ● 「暗号利用環境に関する動向調査」紹介 ● 最終報告書とりまとめに向けた論点整理 ● 各ワーキンググループからの報告・審議
第2回	2015. 1.26	● RC4の注釈について ● 標準化推進WGからの報告・審議 ● SSL/TLS暗号設定ガイドライン（旧名：SSL/TLSサーバ構築ガイドライン）の審議 ● 最終報告書内容についての中間審議
第3回	2015. 3. 10	● 各ワーキンググループからの活動報告・審議 ● 課題解決に向けた分析結果・対策を取りまとめた最終報告書の審議

CRYPTREC
Cryptography Research and Evaluation Committees

2014年度暗号技術活用委員会
活動概要

2014年度暗号技術活用委員会活動内容（再掲）

(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

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行った。2013年度に続き、議論を行う上で有用な基礎データの収集を上期に実施し、これをもとに、下期に検討を実施した。

(2) 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同時に検討した。

(3) 標準化推進

様々な組織が日本からの暗号アルゴリズムの提案を行う場合に、その成果が効果的に得られるようにするための有望な標準化提案先の選定、当面必要とされる稼働見積りや交渉方法、提案活動における課題等を、標準化推進WGにおける検討をもとに取りまとめている。

(4) 運用ガイドライン作成

2013年度にドラフト版を作成した「SSL/TLSサーバ構築ガイドライン」について、引き続き運用ガイドラインWGで作業を行い内容を大幅に改良し、委員会として成果物を取りまとめている。

活動概要

ヒアリング等

幅広く現況を俯瞰するために実施

【ヒアリング対象】
- 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）

参考資料

国内外政府動向等の把握

IPA「暗号利用環境に関する動向調査」報告書（※現時点では未公表）

NISC「我が国のサイバーセキュリティ戦略」

暗号技術活用委員会での審議

- **以下の項目における課題等について意見や見解をとりまとめ**

A) 製品市場に関するもの
  - A-1) 暗号アルゴリズムとセキュリティ製品・システムとの関係
  - A-2) 暗号アルゴリズムについての顧客からのニーズ
  - A-3) 暗号アルゴリズムについての政府調達からのニーズ

B) 標準化活動における課題に関するもの
C) 組織体制（所管官庁・法制度・権限等）に関するもの
D) 暗号アルゴリズムの位置づけに関するもの
E) 国産暗号アルゴリズムの普及阻害要因に関するもの
F) 人材育成に関するもの

CRYPTREC
Cryptography Research and Evaluation Committees

ヒアリング情報

ヒアリング先

カテゴリ	対象
政府関係	政府CIO
	X省
	Y省
業界団体	S団体
	T団体
暗号ライブラリ製造ベンダ	A社
	B社
	C社
暗号製品製造ベンダ	D社
	E社
	F社
セキュリティ製品製造ベンダ	G社
	H社
	I社

ヒアリング項目の概要

- 担当業務において、暗号を利用したり、利用するように指示・取りまとめをした場面がありましたか
- 暗号製品の市場はどのように変化していますか
- どのような観点で利用する暗号アルゴリズムを決めましたか
- 暗号アルゴリズムの選択に関してどのようなニーズがありますか
- 電子政府推奨暗号リストを活用していますか
- 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
- 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
- 暗号アルゴリズムの選択等に対する目利き人材としてどのような人材が必要ですか

CRYPTREC
Cryptography Research and Evaluation Committees

例： ヒアリングでいただいた意見①

- 製品市場に関連するもの
  - 一般的なベンダは、暗号機能の入出力インタフェース仕様は理解していても、暗号アルゴリズムそのものはブラックボックスとして使っている
  - 利用する暗号機能は、暗号アルゴリズム自身の安全性だけでなく、実装難度が低く実装しやすいかとか、実用化スケジュールとかも含めて検討
  - 暗号アルゴリズムの主な実装先は暗号ライブラリであるが、以前とは異なり暗号ライブラリ市場がビジネスとしては成立しにくくなっている
  - 様々なセキュリティ機能が搭載された統合型セキュリティ製品が主流で、機能単体型セキュリティ製品市場は横ばいまたは縮小の傾向と予想
  - 暗号アルゴリズムの違いは製品やシステムの購入に影響を与えるような差別化要因にはならず、採用している暗号アルゴリズムが理由で製品やシステムの購入が決まるケースはないのが現実
  - セキュリティ認証を取得するもともとの目的は、製品に付加価値をつけるためではなく、国内外での調達要件に対応するため

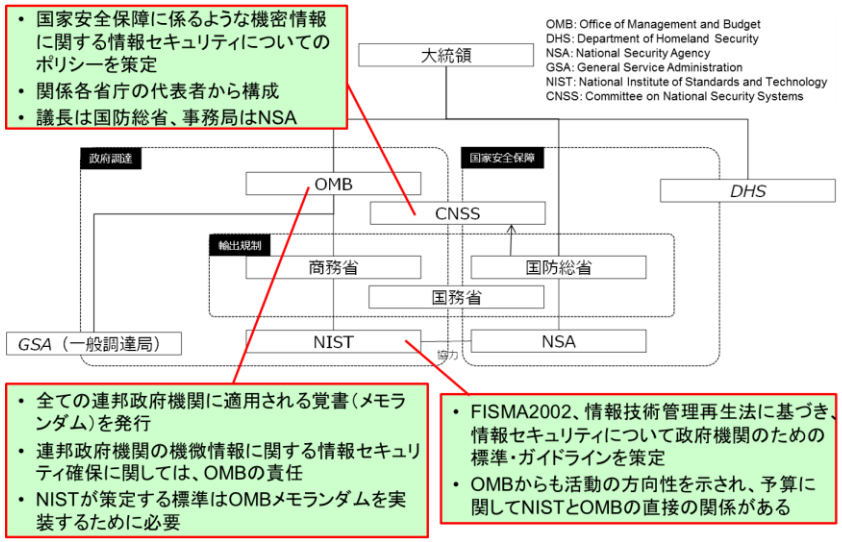
例： ヒアリングでいただいた意見②

- 国産暗号アルゴリズムの普及阻害要因に関連するもの
  - 製品やシステムでの暗号アルゴリズムの採用基準は、あくまでも調達・設計要件を満たしているかどうかであって、技術優位性は比較項目のなかの一つに過ぎない
  - ビジネス上は、基本的には国際標準化されていて広く採用されている暗号アルゴリズムを使うのが大前提であり、国内市場であっても、国産暗号アルゴリズムかどうかはほとんど関係がない
  - 現在の政府統一基準群では安全かつ実装性に優れている「電子政府推奨暗号リストの利用」を指定しているため、国産暗号アルゴリズムだけを明示的に指定して調達を行うことはできない
- 人材育成に関連するもの
  - 技術力ばかりに注目するのではなく、経営層やオピニオンリーダへのロビー活動等も含め、標準化や普及展開を行う上で重要な技術以外の視点での的確な展開戦略の検討・実施する人材が不足
  - システム構築・運用にあたって、暗号アルゴリズムを適切に利用するためのノウハウをもつ人材が不足

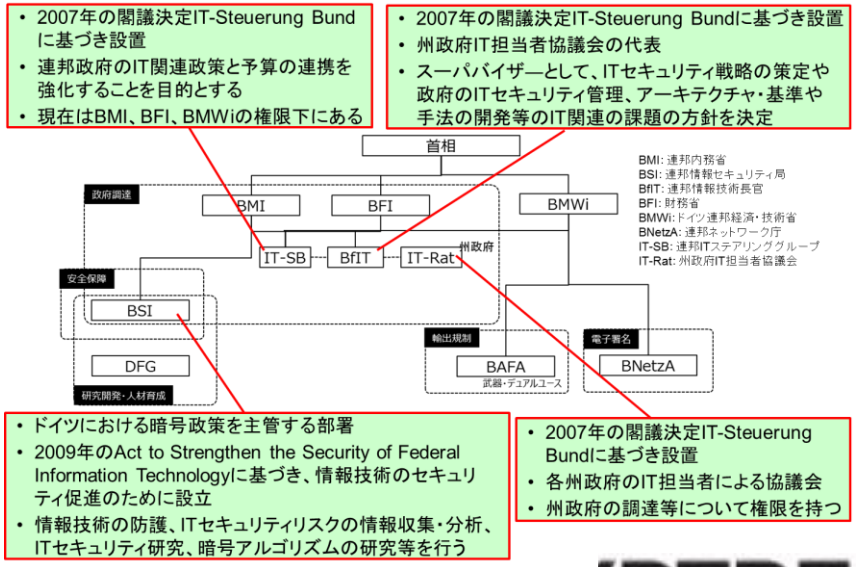
例： 暗号利用環境調査報告書の指摘事項①

■ 組織体制（所管官庁・法制度・権限等）について

- 欧米諸国などでは、暗号政策を国家安全保障もしくは情報保全と位置づけている国が多いうえ、暗号政策を議論しているのは上位の組織体（国家安全保障会議、大統領府、閣議、セキュリティ戦略委員会など）
- 暗号政策として決められた目的を実現するための具体的な実務執行機関としての所管官庁及び権限が決められている
- 米国・ドイツ等は財務省などの予算権限を持つ省庁も直接関与しており、暗号政策の施策実行における財政面についても議論されていると推測



米国の体制



ドイツの体制

例： 暗号利用環境調査報告書の指摘事項②

■ 暗号アルゴリズムの位置づけについて

- 国家安全保障や情報保全のための高セキュリティ調達製品で利用する暗号アルゴリズムは、デファクトスタンダードの暗号アルゴリズムとは異なるものを指定している国（米・英・仏・露・中・韓など）もある
- 政府の情報保全のために強力な暗号アルゴリズムを必要とする一方、国家安全保障・テロ対策の観点から暗号アルゴリズムの利用制限や司法権の行使による強制解除といった項目を含めて、暗号アルゴリズムの位置づけを決めている国（米・仏・露・中など）もある

■ 製品市場動向について

- 米国以外でも、国家安全保障や情報保全などに関わる高セキュリティシステムや製品の政府調達においては、セキュリティ認証製品を使うように義務付けている国（英・仏・露・中・韓など）も多い

続きはCRYPTREC Report 2014でご覧ください

今はこの段階

ヒアリング結果や報告書等を参考に
暗号技術活用委員会で議論
委員会としての意見や見解をとりまとめ

↓

とりまとめ内容を暗号技術検討会に報告・審議

↓

とりまとめ内容を
CRYPTREC Report 2014（暗号技術活用委員会）
にて公表

CRYPTREC
Cryptography Research and Evaluation Committees

2014年度暗号技術活用委員会活動内容（再掲）

(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

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行った。2013年度に続き、議論を行う上で有用な基礎データの収集を上期に実施し、これをもとに、下期に検討を実施した。

(2) 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同時に検討した。

(3) 標準化推進

様々な組織が日本からの暗号アルゴリズムの提案を行う場合に、その成果が効果的に得られるようにするための有望な標準化提案先の選定、当面必要とされる稼働見積りや交渉方法、提案活動における課題等を、標準化推進WGにおける検討をもとに取りまとめている。

(4) 運用ガイドライン作成

2013年度にドラフト版を作成した「SSL/TLSサーバ構築ガイドライン」について、引き続き運用ガイドラインWGで作業を行い内容を大幅に改良し、委員会として成果物を取りまとめている。

標準化推進ワーキンググループ(WG)

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・意見交換する場として設置

■委員

主査	渡辺　創	独立行政法人産業技術総合研究所
委員	江原　正規	東京工科大学
委員	河野　誠一	レノボ・ジャパン株式会社
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
委員	坂根　昌一	シスコシステムズ合同会社
委員	佐藤　雅史	セコム株式会社IS研究所
委員	武部　達明	横河電機株式会社
委員	廣川　勝久	ISO/IEC JTC 1/SC 17国内委員会　委員長
委員	真島　恵吾	NHK放送技術研究所
委員	真野　浩	コーデンテクノインフォ株式会社
委員	茗原　秀幸	三菱電機株式会社

標準化推進WG

詳細は後ほど
渡辺主査より報告

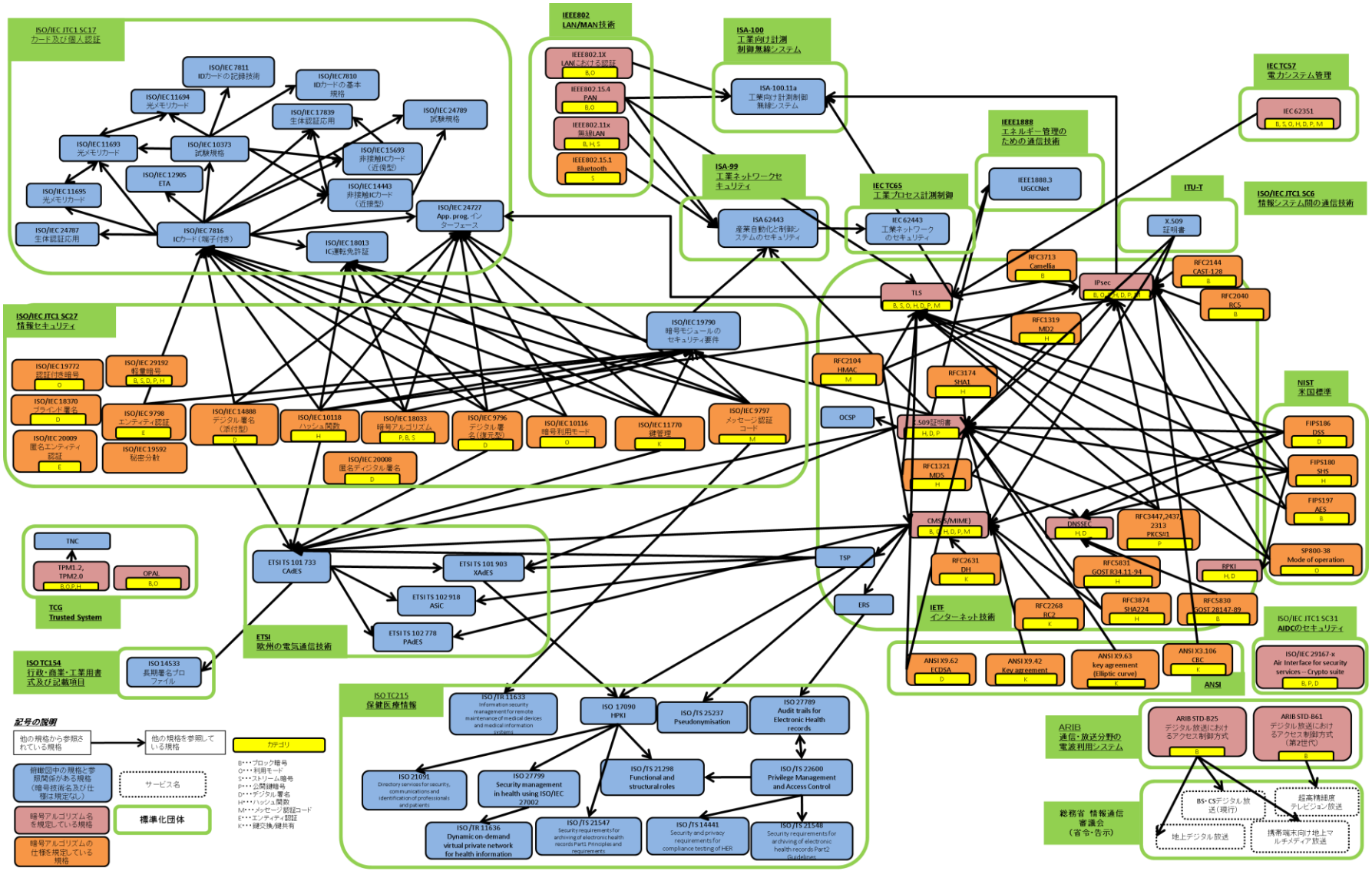
■活動概要

- 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並びに交渉ノウハウや課題等を共有（2013年度）
- WG委員の知見を集約して標準化活動に関する俯瞰図やノウハウをどのように取りまとめていくのがよいかを検討（2014年度）

■成果

- 標準化機関に暗号アルゴリズム提案を検討している企業・機関にとって有益な情報となるように整理
  - 暗号技術参照関係の俯瞰図
  - 標準化提案における交渉ノウハウ・課題及び参考情報

暗号技術参照関係の俯瞰図 （全体像の例）



CRYPTREC
Cryptography Research and Evaluation Committees

標準化提案における交渉ノウハウ・課題の例

A）団体間で共通するノウハウや課題

ノウハウ＜共通①＞
標準化提案を受け入れてもらうためには、標準化に関わる他の「人」との関わりが必要不可欠である。 例えば、一方的に提案するのではなく、周りの人たちとの協力関係を築き、ネゴシエーションしながら標準化を行うと提案がスムーズに受け入れられやすい。 また、過去の審議経緯や利害関係等を十分に把握していると審議を進めるのに有利である。継続的に規格策定の場に関わっている人とコミュニケーションをとり、審議の経緯等を知っておくとよい。

課題＜共通①＞
日本の場合、企業が標準化団体に参加するため、それまでの担当者が異動してしまうと担当者が変わるが、欧米の場合、個人が標準化の仕事として参加しているので、企業を移っても所属企業名が変わるだけでその人物は引き続き参加する。このように、欧米では、日本に比べて、継続して標準化活動に携わる人が多い。

B）団体毎の基本的な情報、ノウハウ及び課題

■ ISO/IEC JTC1 SC27

技術提案の手続き等
NB (National Body)提案とする場合、Expert提案とする場合が考えられる。日本において暗号技術の提案を行う場合は、どちらの場合であっても、日本の国内委員会である情報処理学会情報規格調査会のSC27/WG2小委員会に参加し、委員会で合意を得る必要がある。

ノウハウ①
学術論文や国家的なプロジェクトでの評価が大きく信頼されているので、学術論文等で評価された技術であるとよい。

2014年度暗号技術活用委員会活動内容（再掲）

(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

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行った。2013年度に続き、議論を行う上で有用な基礎データの収集を上期に実施し、これをもとに、下期に検討を実施した。

(2) 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同時に検討した。

(3) 標準化推進

様々な組織が日本からの暗号アルゴリズムの提案を行う場合に、その成果が効果的に得られるようにするための有望な標準化提案先の選定、当面必要とされる稼働見積りや交渉方法、提案活動における課題等を、標準化推進WGにおける検討をもとに取りまとめている。

(4) 運用ガイドライン作成

2013年度にドラフト版を作成した「SSL/TLSサーバ構築ガイドライン」について、引き続き運用ガイドラインWGで作業を行い内容を大幅に改良し、委員会として成果物を取りまとめている。

CRYPTREC
Cryptography Research and Evaluation Committees

運用ガイドラインワーキンググループ(WG)

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ガイドライン案を作成

■委員

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IS研究所
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	東京大学

運用ガイドラインWG

詳細は後ほど
菊池主査より報告

■活動概要

- 2015年3月時点でのSSL/TLS通信の安全性と可用性（相互接続性）のバランスを踏まえた暗号設定方法をとりまとめ
- ガイドラインの主な対象読者：
  サーバ構築者、サーバ管理者、システム担当者

■成果

- SSL/TLS暗号設定ガイドライン（案）
- SSL/TLS暗号設定ガイドラインチェックリスト（案）

SSL/TLS暗号設定ガイドライン（考え方）

設定基準	概要	安全性
高セキュリティ型	**とりわけ高い安全性を必要とする明確な理由があるケース**	標準的な水準を**大きく上回る高い安全性水準**を達成
推奨セキュリティ型	ほぼすべての**一般的な利用形態で使う**ことを想定	**標準的な安全性水準**を実現
セキュリティ例外型	**安全性よりも相互接続性に対する要求をやむなく優先**させるような場合	**短期的な利用を前提に許容可能な最低の安全性水準**を満たす

それぞれの設定基準に応じた要求設定を規定

- プロトコルバージョン
- サーバ証明書
- 暗号スイート

プロトコルバージョンの要求設定

	TLS1.2	TLS1.1	TLS1.0	SSL3.0	SSL2.0
高セキュリティ型	◎	×	×	×	×
推奨セキュリティ型	◎	○	○	×	×
	ー	◎	○	×	×
	ー	ー	◎	×	×
セキュリティ例外型	◎	○	○	○	×
	ー	◎	○	○	×
	ー	ー	◎	○	×
対象外	ー	ー	ー	○	×

○：設定有効（◎：優先するのが望ましい）　×：設定無効化　ー：実装なし

CRYPTREC Cryptography Research and Evaluation Committees

SSL/TLS暗号設定ガイドライン・チェックリスト(抜粋)

		参照章	済
①要求設定確認	チェック項目なし		
②プロトコルバージョン設定	②-1) TLS1.0を設定有効にしたか	4.1節	□
	②-2) SSL2.0及びSSL3.0を設定無効(利用不可)にしたか	4.1節	□
	□ ②-3) TLS1.2が実装されている場合には左の□と以下の項目をチェック		
	②-4) TLS1.2について設定を有効にしたか	4.1節	□
	□ ②-5) TLS1.1が実装されている場合には左の□と以下の項目をチェック		
	②-6) TLS1.1について設定を有効にしたか	4.1節	□
	□ ②-7) プロトコルバージョン優先順位を設定できる場合には左の□と以下の項目をチェック		
	②-8) 設定有効になっているプロトコルバージョンのうち、もっとも新しいバージョンによる接続を最優先にしたか。接続できない場合に、順番に一つずつ前のプロトコルバージョンでの接続するようにしたか	4.1節	□
③サーバ証明書設定	③-1) SHA256withRSAで鍵長2048ビット以上、またはSHA256withECDSAで鍵長256ビット以上のサーバ証明書を利用したか (もしくは、現時点で利用中のSHA256withDSAで鍵長2048ビット以上のサーバ証明書をそのまま継続利用したか)	5.1節	□
	③-2) サーバ証明書の発行・更新をした際に、鍵情報のペアを新たに生成したか	5.1節	□
	③-3) サーバ証明書の発行・更新をする際に、鍵情報のペアを新たに生成する旨の指示を仕様書・運用手順書等に記載したか	5.1節	□
	③-4) 接続することが想定されている全てのクライアントに対して、警告表示が出ないように対策するか、警告表示が出るブラウザはサポート対象外であることを明示したか	5.1節	□

		参照章	済
④暗号スイート設定	□ ④-i) 楕円曲線暗号を利用しない場合は左の□と以下の項目をチェック		
	④-i-1) 表2記載の暗号スイート(網掛けを除く)の全部または一部を設定したか	6.1節／6.5.2節	□
	④-i-2) 表2記載のグループA及びグループBそれぞれの暗号スイート(網掛けを除く)から少なくとも一つずつは設定したか	6.1節／6.5.2節	□
	□ ④-i-3) 金融サービスや電子商取引サービスなど、不特定多数に公開されるサービス等において使用されるサーバである場合には左の□と以下の項目をチェック		
	④-i-4) AES128-SHAの暗号スイートを設定したか	6.1節／6.5.2節	□
	④-i-5) 表2記載の暗号スイートのグループ順番(グループAの暗号スイートの次にグループBの暗号スイートが並ぶ、以下同様)を守っているか	6.1節／6.5.2節	□
	④-i-6) 表2記載の暗号スイート以外は、すべて利用不可の設定をしたか	6.1節／6.5.2節	□
	□ ④-ii) 楕円曲線暗号を利用する場合は左の□と以下の項目をチェック		
	④-ii-1) パテントリスクを考慮したうえで楕円曲線暗号を利用すると決めたか	6.1節	□
	④-ii-2) 表2記載の暗号スイート(網掛けを含む)の全部または一部を設定したか	6.1節／6.5.2節	□
	④-ii-3) 表2記載のグループA及びグループBそれぞれの暗号スイート(網掛けを含む)から少なくとも一つずつは設定したか	6.1節／6.5.2節	□
	□ ④-ii-4) 金融サービスや電子商取引サービスなど、不特定多数に公開されるサービス等において使用されるサーバである場合には左の□と以下の項目をチェック		
	④-ii-5) AES128-SHAの暗号スイートを設定したか	6.1節／6.5.2節	□
	④-ii-5) 表2記載の暗号スイートのグループ順番(グループAの暗号スイートの次にグループBの暗号スイートが並ぶ、以下同様)を守っているか	6.1節／6.5.2節	□
	④-ii-6) 表2記載の暗号スイート以外は、すべて利用不可の設定をしたか	6.1節／6.5.2節	□

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術活用委員会・活動報告（まとめ）

実施事項

(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

(2) 暗号政策の中長期的視点からの取組の検討

(3) 標準化推進

(4) 運用ガイドライン作成

詳細は、暗号技術検討会の審議を経て
CRYPTREC Report 2014
により公表予定

CRYPTREC
Cryptography Research and Evaluation Committees