CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTREC標準化推進WG 活動報告

主査　渡辺　創
独立行政法人　産業技術総合研究所

CRYPTREC
Cryptography Research and Evaluation Committees

アウトライン

- はじめに
- 標準化推進WGの位置づけ
- 標準化推進WG委員
- 2014年度　活動概要
  1. 暗号技術提案にあたっての俯瞰図のとりまとめ
  2. 提案機会等の見込みのある標準化提案先の選定
  3. 暗号技術を提案する組織にとって当面必要な稼動見積りや交渉方法等
- 今後の課題
- おわりに

はじめに

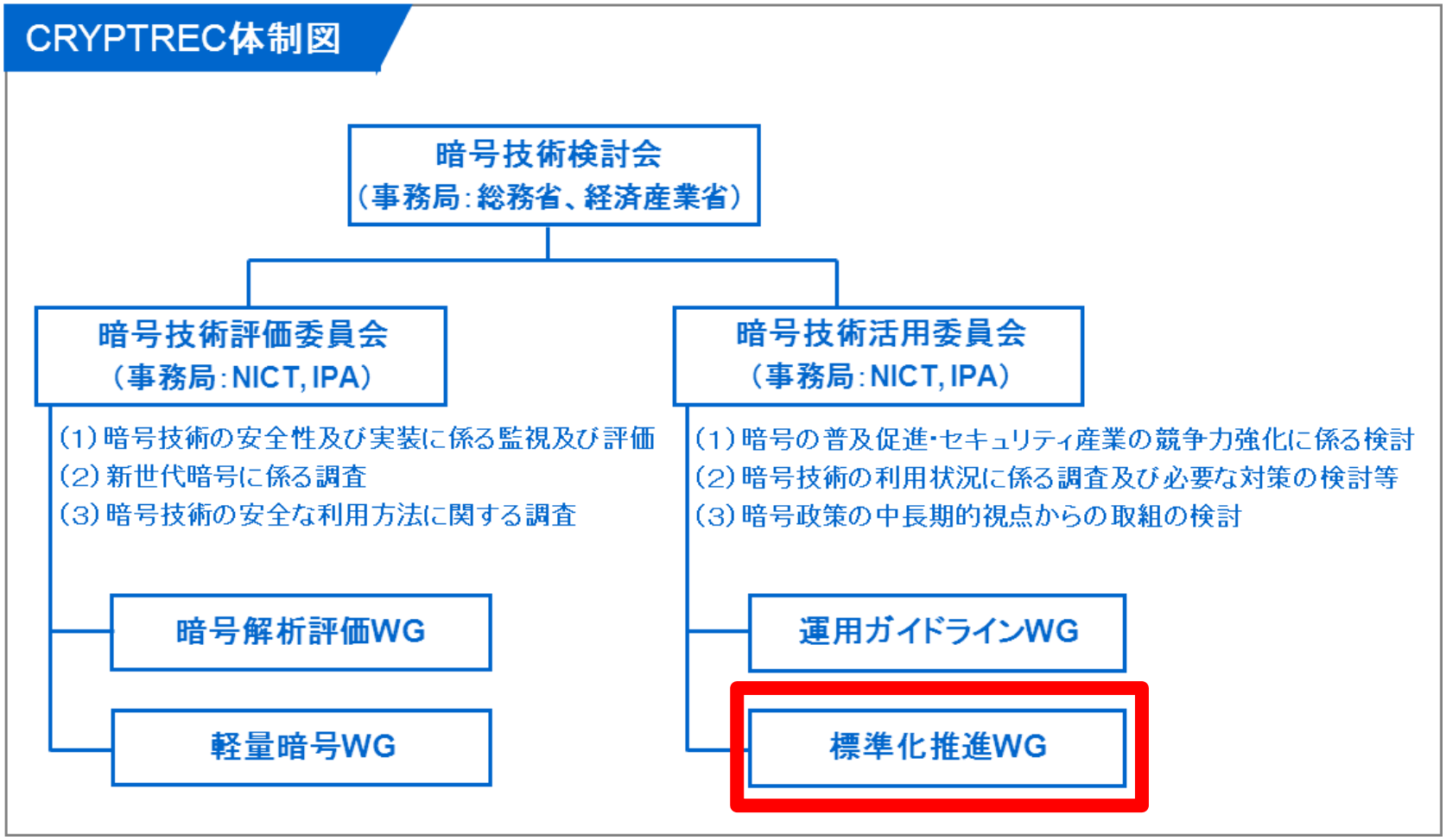
WG設立趣旨

- 様々な標準化団体に対して、日本からの暗号技術が受け入れられるようにするため、標準化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、日本からの暗号技術提案の効率的な横展開を図る

標準化推進WGの位置づけ

CRYPTREC
Cryptography Research and Evaluation Committees

主に日本から提案する暗号技術の横断的な国際標準化の取り組みを支援・意見交換



http://www.cryptrec.go.jp/system.htm

CRYPTREC
Cryptography Research and Evaluation Committees

標準化推進WG　委員

各標準化団体で活躍されている方を委員に選任

標準化推進WG　委員（敬称略）		
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	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

活動概要

2014年度は、2013年度の活動を踏まえ、暗号技術の標準化を検討している組織にとって有益な情報を報告書として作成

1. 暗号技術提案にあたっての俯瞰図のとりまとめ
2. 提案機会等の見込みのある標準化提案先の選定
3. 暗号技術を提案する組織にとって当面必要な稼動見積りや交渉方法等

2014年度開催状況

回	開催日	議題
第1回	2014年10月15日	● WG活動計画報告 ● 各標準化活動状況のアップデート ● 俯瞰図のとりまとめ方法 ● 標準化提案における交渉ノウハウ・課題の整理の方針
第2回	2014年12月11日	● 俯瞰図の完成イメージについて ● 暗号技術提案に有望な標準化提案先について ● 暗号技術の提案に必要な稼働見積り ● 標準化提案における交渉ノウハウ・課題の整理について
第3回	2015年2月23日	● 報告書のとりまとめ ● 暗号技術参照関係の俯瞰図のとりまとめ ● 標準化提案におけるノウハウ・課題及び基本的な情報の整理

1.暗号技術提案にあたっての俯瞰図のとりまとめ

どの規格に採用されれば、どこの規格で
利用されるようになるのか？

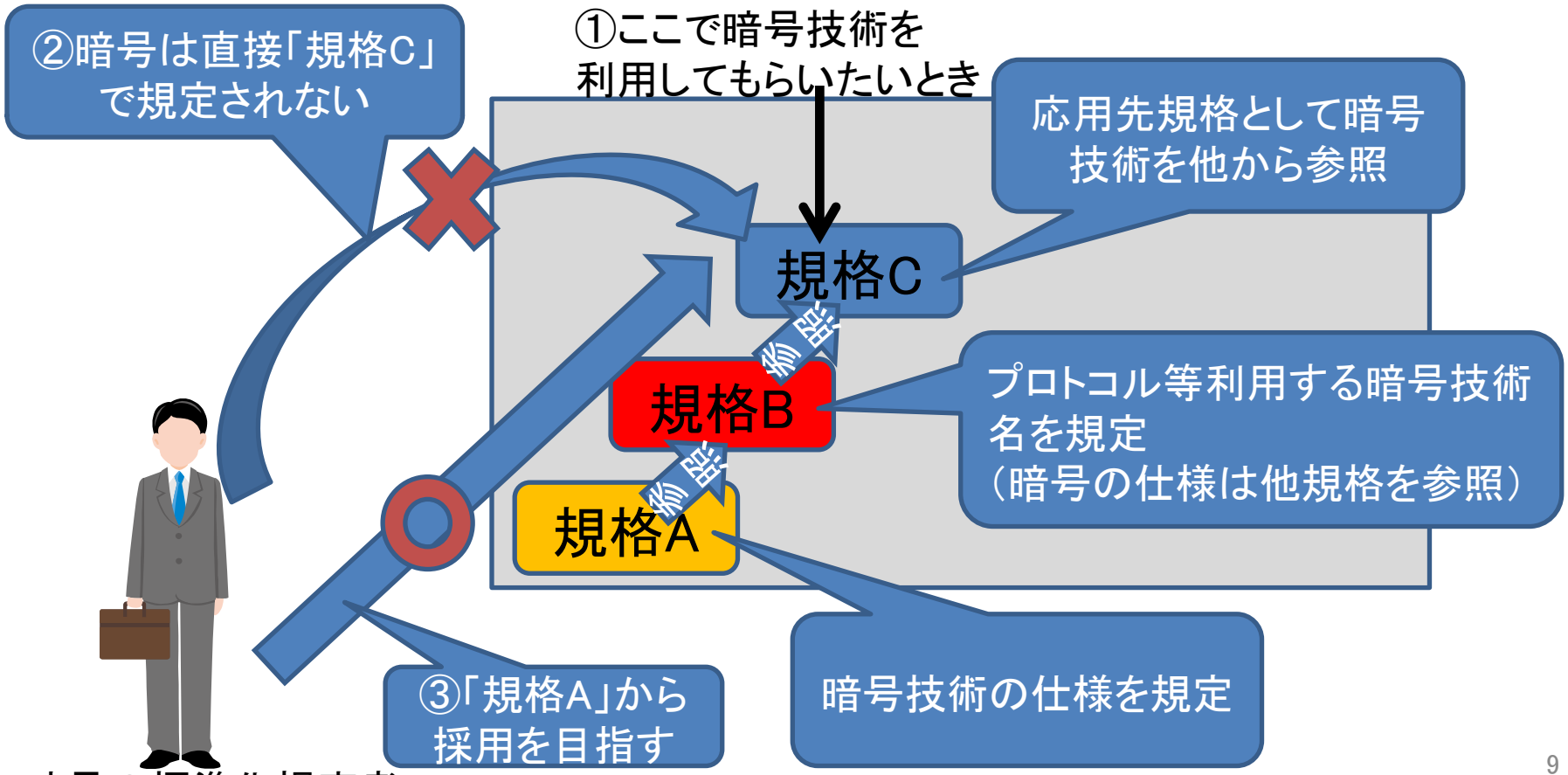
俯瞰図を作成し、規格の参照関係を整理

2014年度は・・・

1st STEPとして、俯瞰図のとりまとめ方法を検討
及びサンプル例の作成

暗号技術参照関係の俯瞰図について

今後暗号技術を提案する人が提案先を選定するために参考となるように規格の参照関係について整理



暗号技術参照関係の俯瞰図（対象団体）

原則委員が関与している標準化団体の規格を対象
（暗号標準化に影響力の強いNIST, ANSI, ITUの規格も調査）

今回調査対象とした標準化団体
ISO/IEC（JTC1/　SC27, SC17, SC31 ,SC6）
ISO（TC215, TC154）
IEC（TC57, TC65）
IEEE（IEEE802, IEEE1888）
ISA（ISA-99, ISA-100）
TCG
ARIB
ETSI
IETF
ANSI
NIST
ITU（ITU-T）

暗号技術参照関係の俯瞰図（とりまとめ方法）

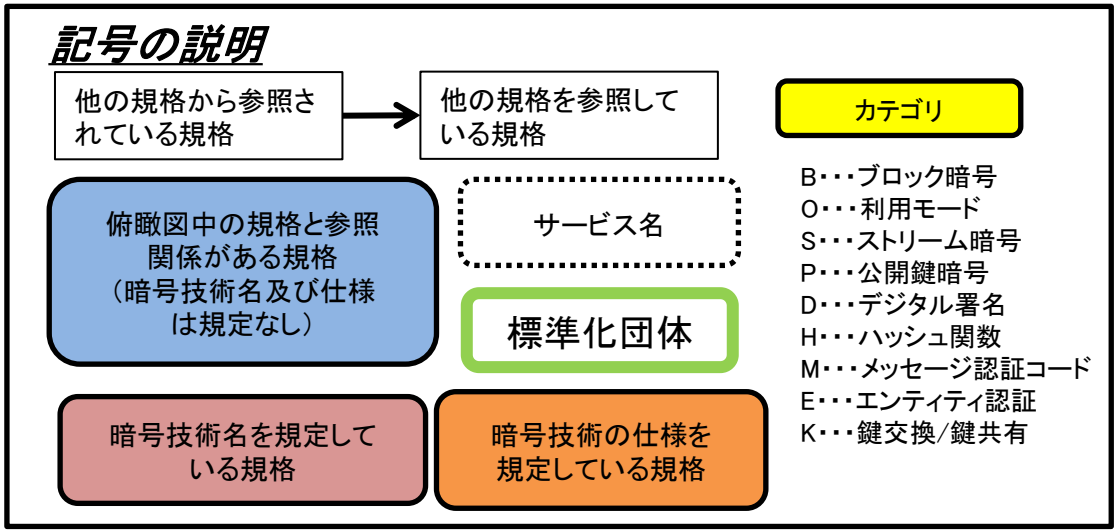
俯瞰図の整理方法について検討を実施

① 「暗号技術の仕様を規定している規格」、「利用する暗号技術名を規定している規格」、「応用先規格」及び「サービス名」に分類

② 「暗号技術の仕様を規定している規格」に技術カテゴリを付記

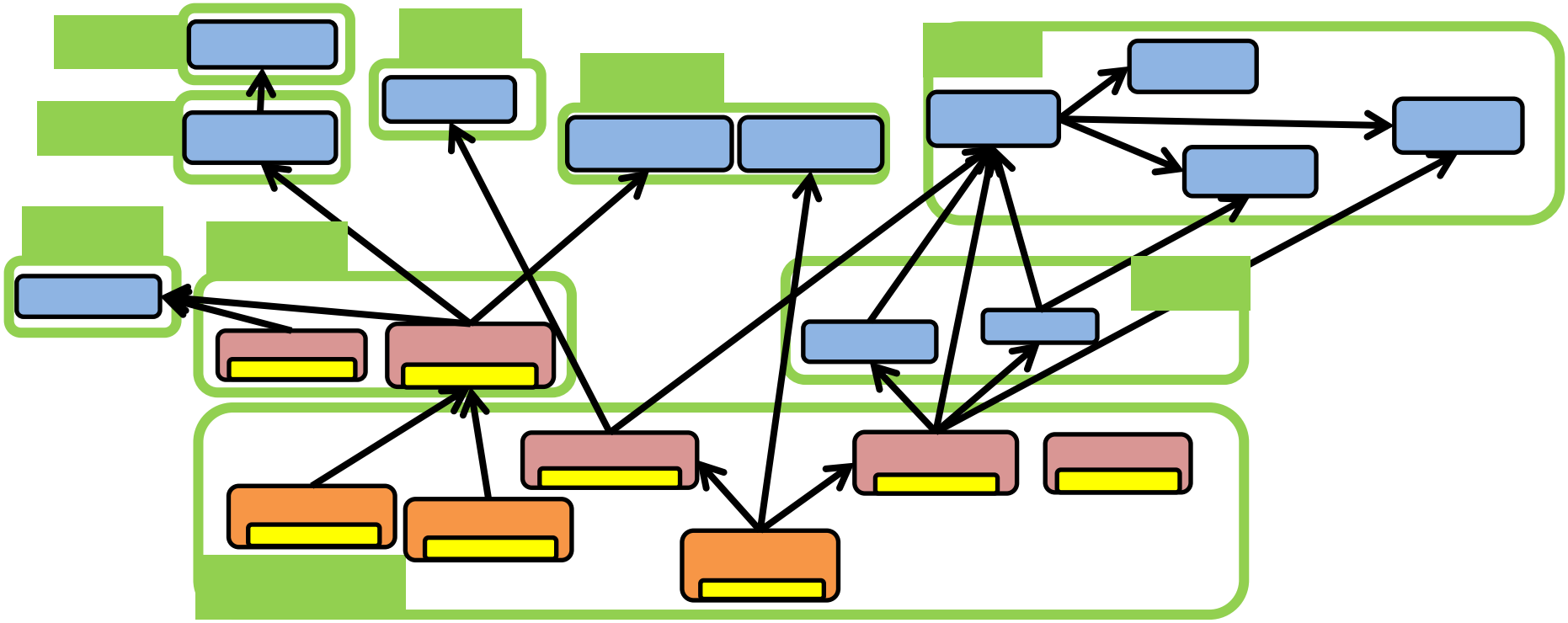
③ 参照関係：「参照される側」から「参照する側」への矢印で表示

④ 標準化団体毎にまとめて配置



暗号技術参照関係の俯瞰図（イメージ）

検討した整理方法に基づき調査範囲内で規格の参照関係を表す俯瞰図を試作



2.提案機会等の見込みのある標準化提案先の選定

CRYPTREC
Cryptography Research and Evaluation Committees

標準化提案先規格として、丁度よい提案タイミングにある規格はあるか？

提案先に関する情報収集が必要

2014年度は・・・

1st STEPとして、
団体毎に提案できるタイミング等の情報を収集

2.提案機会等の見込みのある標準化提案先について情報整理

提案先規格を見つける手がかりとなりうる情報について「3.」と併せて整理

- 規格改定のタイミング
- 技術を提案できるタイミング
- 関連するノウハウ（Preliminary Work Itemの登録状況を確認する等）

3. 暗号技術を提案する組織にとって当面必要な稼動見積りや交渉方法等

CRYPTREC
Cryptography Research and Evaluation Committees

①提案にあたって必要な稼動は？
②ノウハウ等は？

①稼動を見積るために必要な情報収集
②ノウハウ等は委員の知見を集約

2014年度は・・・

1st STEPとして、
①稼動見積りの参考となる情報をとりまとめる
②暗号技術提案に限らず標準化活動についてのノウハウをとりまとめ

3. 暗号技術を提案する組織にとって当面必要な稼動見積りや交渉方法等

CRYPTREC Cryptography Research and Evaluation Committees

委員の知見に基づいて情報収集（下記は対象団体）

今回調査対象とした標準化団体
ISO/IEC（JTC1/　SC27, SC17, SC31 ,SC6）
ISO（TC215, TC154）
IEC（TC57, TC65）
IEEE（IEEE802, IEEE1888）
ISA（ISA-99, ISA-100）
TCG
ARIB
ETSI
IETF
ANSI
NIST
ITU（ITU-T）

3.①暗号技術を提案する組織にとって当面必要な稼動見積り

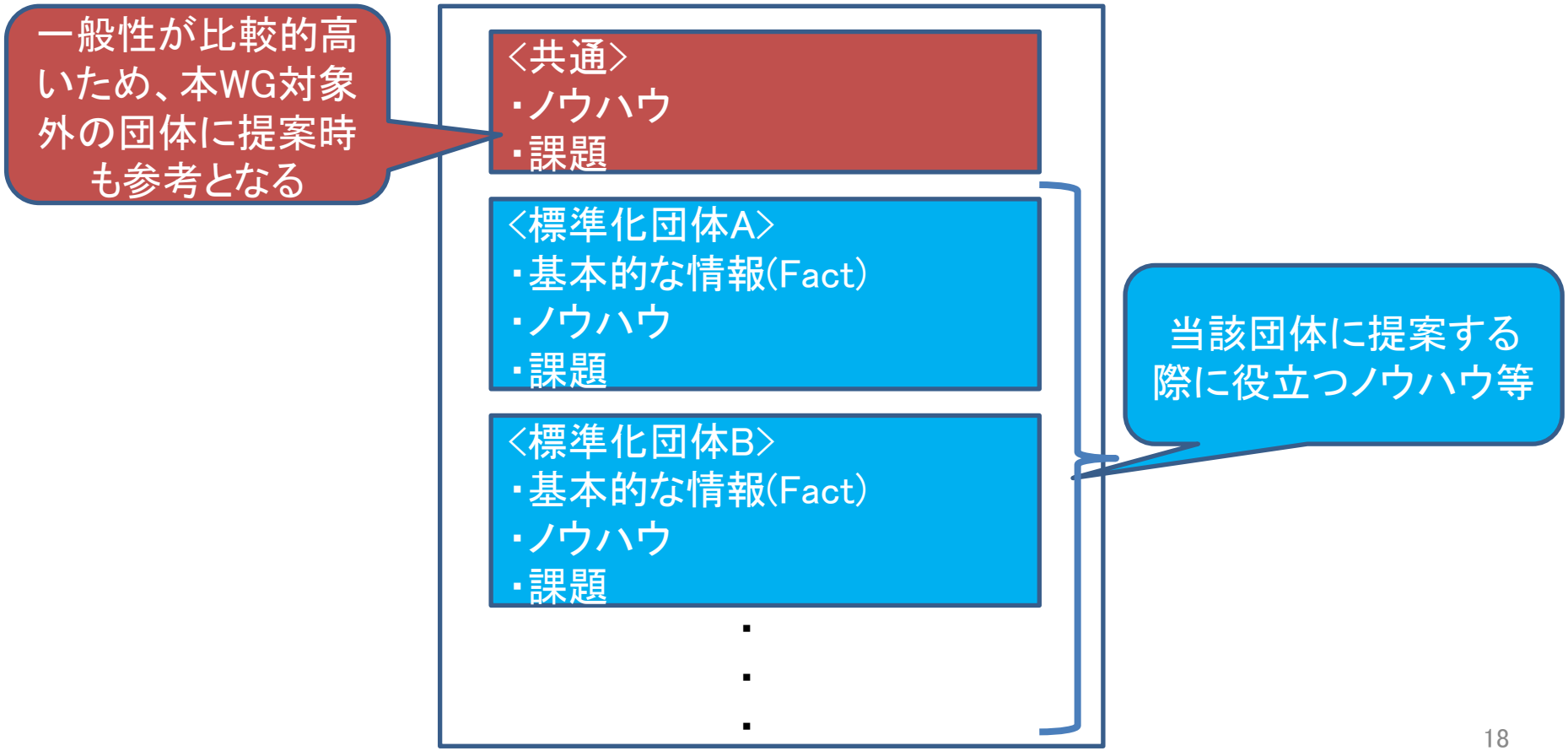
同一標準化機関内でもプロジェクト毎に大きく稼動が異なるため、稼動見積りの参考となるよう最低限のFactを整理（「2.」及び「3.②」と併せて整理）

- 規格が発行されるまでの期間
- 遠隔会議（電話会議）の時間帯（及びその決め方）
- 会議の年間回数（及び場所）
- 標準化プロセス
- 投票権獲得条件（及び投票権所有者）
- 利用するツール

etc・・・

3.②標準化提案における交渉方法・ノウハウ・課題等の整理

団体間に共通する項目と団体特有の項目に分けて整理
（「2.」及び「3.①」と併せて整理）



今後の課題

- 委員会での情報提供や意見を元に多くの課題を抽出
  - 暗号技術参照関係の俯瞰図について
  - ノウハウ等の整理について

今後の課題(暗号技術参照関係の俯瞰図)

① 作成方法
- レイヤの分け方
- 暗号技術の範囲
- 俯瞰図の見方、利用方法等

② 網羅性
- 暗号に関する規格の網羅的調査ではない

③ メンテナンス方法
- 一枚の平面図では見難い、さらに情報量が増加すると破綻。データベースを用いた必要な情報の抽出表示ができるとよい？
- 規格改訂や新規格をどのように反映するか？

今後の課題(ノウハウ等の整理)

① 網羅性
- 今回対象外の中にも暗号技術に関係する団体は存在。特に応用先は網羅できていない。

② 暗号技術提案に特化したノウハウ等の抽出
- 今回は標準化活動のおけるノウハウ

③ メンテナンス方法
- 今回のような整理方法でよいか？

おわりに

- 暗号技術提案に関して標準化活動の横展開を議論する場がない状況下で、初の試みとして標準化推進WGを設置した。
- 暗号技術参照関係の俯瞰図作成や委員の知見に基づくノウハウ等の情報の集約を行った。
- 活動の中で多くの課題点を抽出した。それを踏まえて、今後日本としてどのような活動をすべきかを検討していきたい。