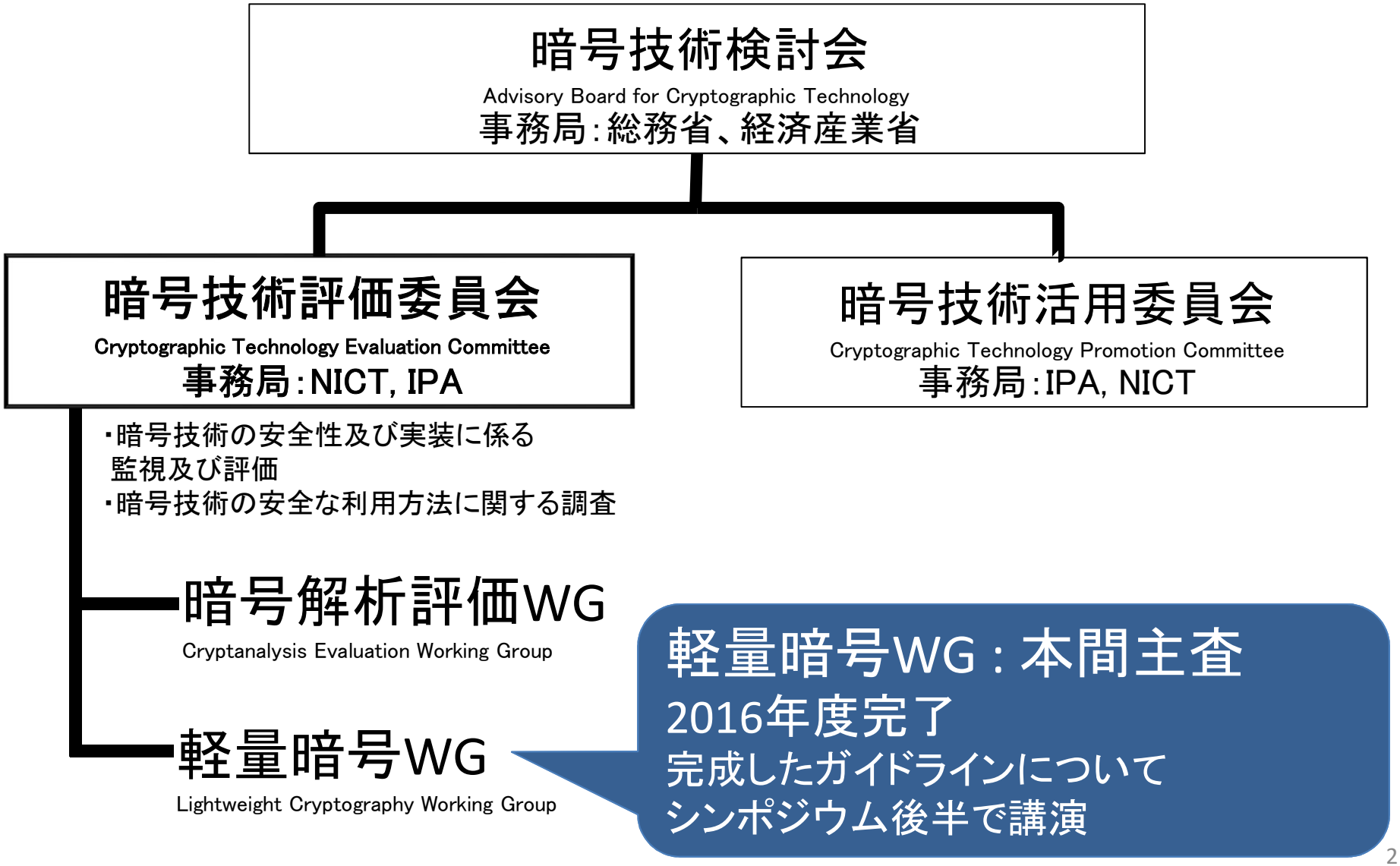
CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術評価委員会
活動報告

暗号技術評価委員会 委員長
(電気通信大学 教授)
太田 和夫

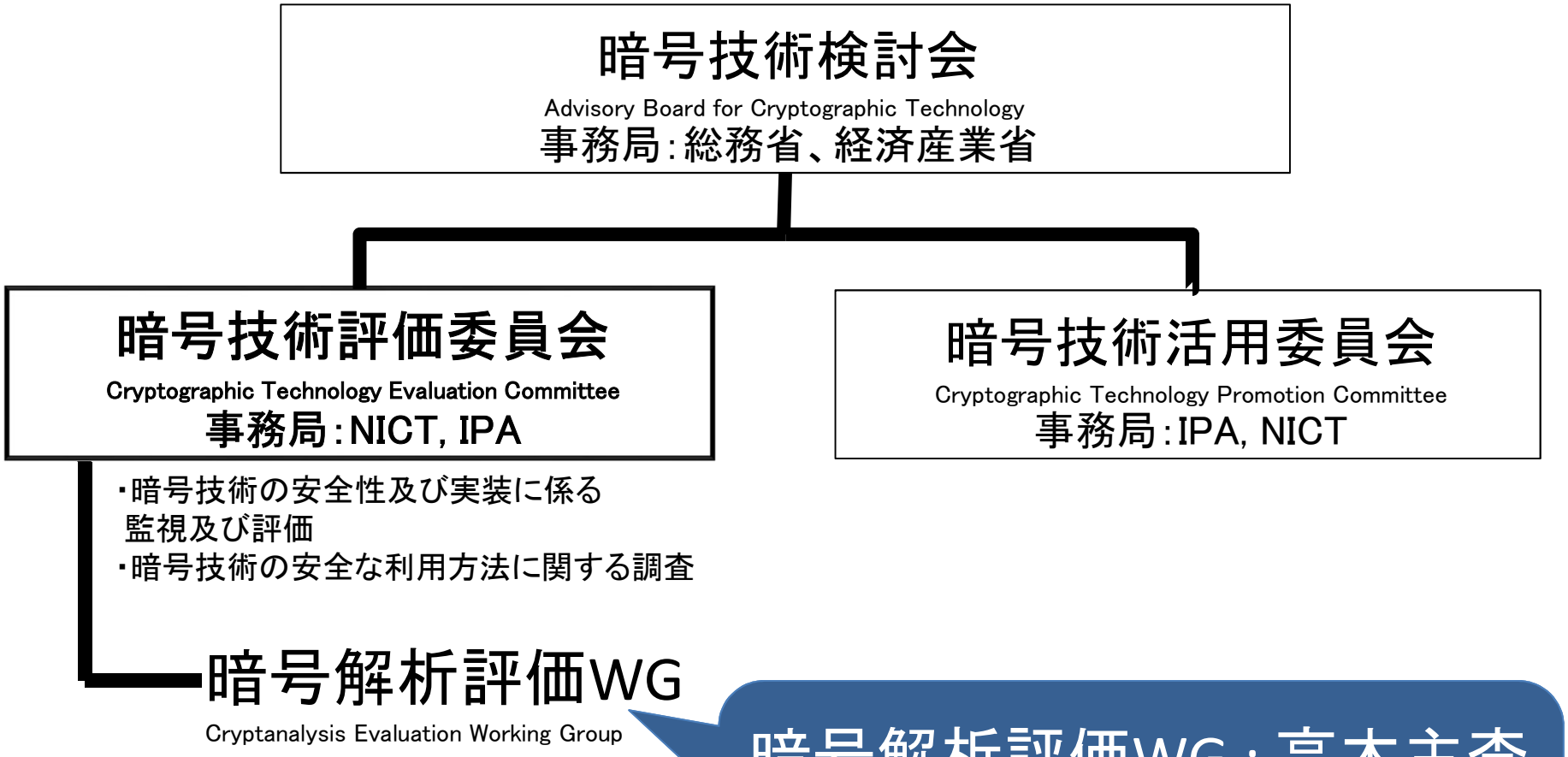
CRYPTREC
Cryptography Research and Evaluation Committees

2016年度 CRYPTREC 体制



CRYPTREC
Cryptography Research and Evaluation Committees

2017年度 CRYPTREC 体制



暗号解析評価WG：高木主査
2017年度継続
この後講演

CRYPTREC
Cryptography Research and Evaluation Committees

2016～2017年度 暗号技術評価委員会 委員

委員長	太田　和夫	国立大学法人電気通信大学 大学院情報理工学研究科 教授
委員	岩田　哲	国立大学法人名古屋大学 大学院工学研究科　准教授
委員	上原　哲太郎	立命館大学 情報理工学部　教授
委員	金子　敏信	東京理科大学 理工学部　教授
委員	佐々木 良一	東京電機大学 未来科学部 教授
委員	高木　剛	国立大学法人東京大学 大学院情報理工学系研究科 数理情報学専攻 教授
委員	手塚　悟	慶應義塾大学 大学院政策・メディア研究科　特任教授
委員	本間　尚文	国立大学法人東北大学　電気通信研究所　教授
委員	松本　勉	国立大学法人横浜国立大学 大学院環境情報研究院　教授
委員	松本　泰	セコム株式会社 IS研究所 コミュニケーションプラットフォームディビジョン ディビジョン　マネージャー
委員	盛合　志帆	国立研究開発法人情報通信研究機構 サイバーセキュリティ研究所　セキュリティ基盤研究室長
委員	山村　明弘	国立大学法人秋田大学 大学院理工学研究科数理・電気電子情報学専攻 教授
委員	渡邊　創	国立研究開発法人産業技術総合研究所 情報・人間工学領域研究戦略部 研究企画室長

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術評価委員会活動目的

CRYPTREC 暗号リストに掲載されている暗号技術や
電子政府システム等で利用される暗号技術の
安全性維持及び信頼性確保のために安全性及び
実装に係る監視及び評価を行う。

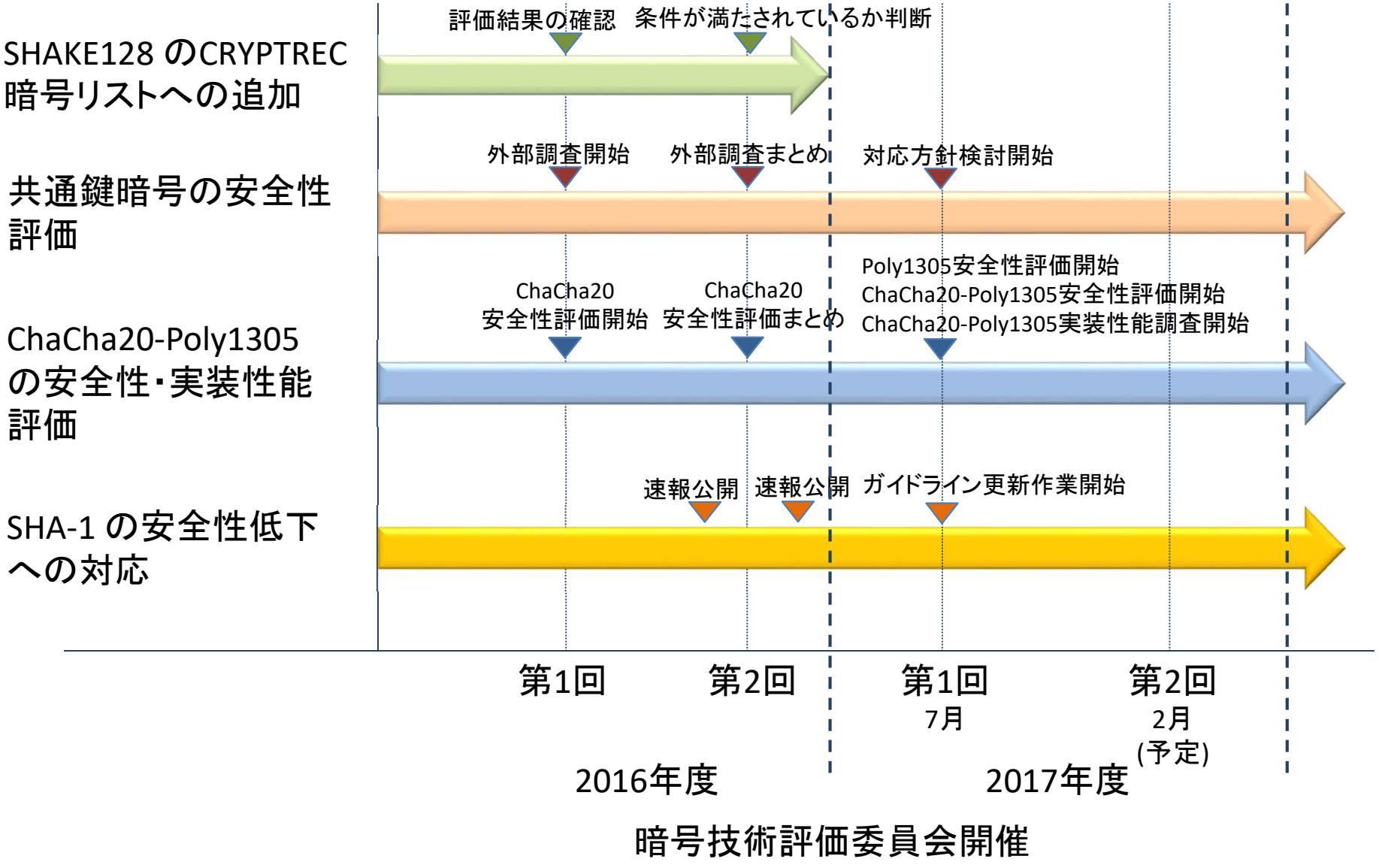
CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術評価委員会活動概要

- 暗号技術の安全性及び実装に係る監視及び評価
  - **CRYPTREC 暗号等の監視**
  - 電子政府推奨暗号リスト及び推奨候補暗号リストからの運用監視リストへの降格および運用監視暗号リストからの危殆化が進んだ暗号の削除
  - **CRYPTREC 注意喚起レポートの発行**
  - **推奨候補暗号リストへの新規暗号(事務局選出)の追加**
  - **新技術などに関する調査及び評価**
- 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・公表など)
  - **暗号アルゴリズムの危殆化に向けた対応**

CRYPTREC
Cryptography Research and Evaluation Committees

主な活動内容



SHAKE128 のCRYPTREC暗号リストへの追加

- 2016年度
  - 2015年度までに実施した安全性及び実装性能評価をもとに、CRYPTREC 暗号リストへの追加条件を満たしていると判断

➡ 検討会審議により、
CRYPTREC 推奨候補暗号リストへ追加

SHAKE128 のセキュリティ強度

推奨候補暗号リスト掲載のハッシュ関数 SHA-3 アルゴリズム

アルゴリズム	出力長 (bits)	セキュリティ強度 (bits)		
		衝突攻撃への耐性	原像攻撃への耐性	第 2 原像攻撃への耐性
SHA3-256	256	128	256	256
SHA3-384	384	192	384	384
SHA3-512	512	256	512	512
SHAKE128 (注)	d	min(d/2,128)	≧min(d,128)	min(d,128)
SHAKE256 (注)	d	min(d/2,256)	≧min(d,256)	min(d,256)

(注)「 ハッシュ長は 256 ビット以上とすること。」

64ビットブロック暗号の動向

- MISTY1 に対する解析の進展
  - CRYPTO2016
    - 解読にほぼすべて2^{64}組の(平文, 暗号文)を集める必要があるが、鍵の全数探索よりも少ない計算量(2^{70})で鍵が導出可能
- 64ビットブロック暗号の安全性
  - ACM CCS 2016
    - TLSやOpenVPN等の実プロトコルで、64ビットブロック暗号により同じ鍵で2^{32}ブロック以上暗号化した場合、cookieやpassword等の秘密情報が導出可能 (https://sweet32.info, CVE-2016-2183, -6329)
      - Open VPN, Mozilla, OpenSSL, Microsoft等も対応
  - NIST (2017.7)
    - TripleDES による暗号化上限回数を 2^{32} から 2^{20} に引き下げたガイドライン(SP800-68_rev2)のドラフト公開、パブリックコメント募集 (2017.10.1まで)

CRYPTREC
Cryptography Research and Evaluation Committees

共通鍵暗号の安全性評価

- 2016年度
  - 外部専門家による調査を実施
    - 攻撃法の発展（暗号解読に必要な計算量・データ量・メモリ量等の低下）の調査
    - 解読手法の進展や計算機能力の向上を勘案した共通鍵暗号の今後の危殆化に関する考察
- 2017年度
  - 64ビットブロック暗号利用時の安全な利用方法(同一鍵での暗号化上限回数)についての指針を検討中

CRYPTREC
Cryptography Research and Evaluation Committees

ChaCha20-Poly1305 の安全性・実装性能評価

- 2016年度
  - ChaCha20 に関する安全性評価実施
    ➡ 現時点で重大な脅威は見つかっていない
- 2017年度
  - Poly1305 の安全性評価
  - ChaCha20-Poly1305 の安全性評価
  - ChaCha20-Poly1305 の実装性能に関する調査

SHA-1 の安全性低下への対応

CRYPTREC
Cryptography Research and Evaluation Committees

ENGLISH

- CRYPTRECとは
- CRYPTRECの体制
- CRYPTRECの沿革
- CRYPTRECの報告書
- 技術報告書
- CRYPTREC暗号リスト（電子政府推奨暗号リスト）
- CRYPTREC暗号の仕様書
- 関連機関等のご案内

トピックス

SHA-1の安全性低下について

平成29年3月1日
CRYPTREC暗号技術評価委員会

2017年2月23日に、CWI AmsterdamとGoogle Researchの共同研究チームが、ハッシュ関数SHA-1の衝突発見に初めて成功したと発表しました[1]。ハッシュ関数とは、入力データに対して固定長のハッシュ値を出力するアルゴリズムで、電子署名等多くの用途で利用されています。ハッシュ関数の衝突を発見するということは、同じハッシュ値を出力する複数の異なる入力データを見つけるということで、安全なハッシュ関数に対しては現実的な計算量では衝突が見つけられないようになっています。今回の発表では、全数探索の計算量(2^{80})よりも10万倍速い$2^{63.1}$回のSHA-1の計算量で衝突を発見したと報告されています。これはCPU 6500年分とGPU 100年分を合わせた計算量に相当するとのことです。ハッシュ関数の衝突が見つけられるようになると、電子署名の偽造が可能となるなどの脅威が考えられます。

これまでCRYPTRECでは、SHA-1の安全性低下について継続的に監視、評価、報告を行ってきました[2] [3]。現在、CRYPTRECでは、SHA-1を「CRYPTREC暗号リスト」の「運用監視暗号リスト」[4]に掲載し、互換性維持以外の目的での利用を推奨していません。また、情報セキュリティ政策会議からも2008年に移行指針[5]が発表されています。このよ

SHA-256等、より安全なハッシュ関数への速やかな移行を

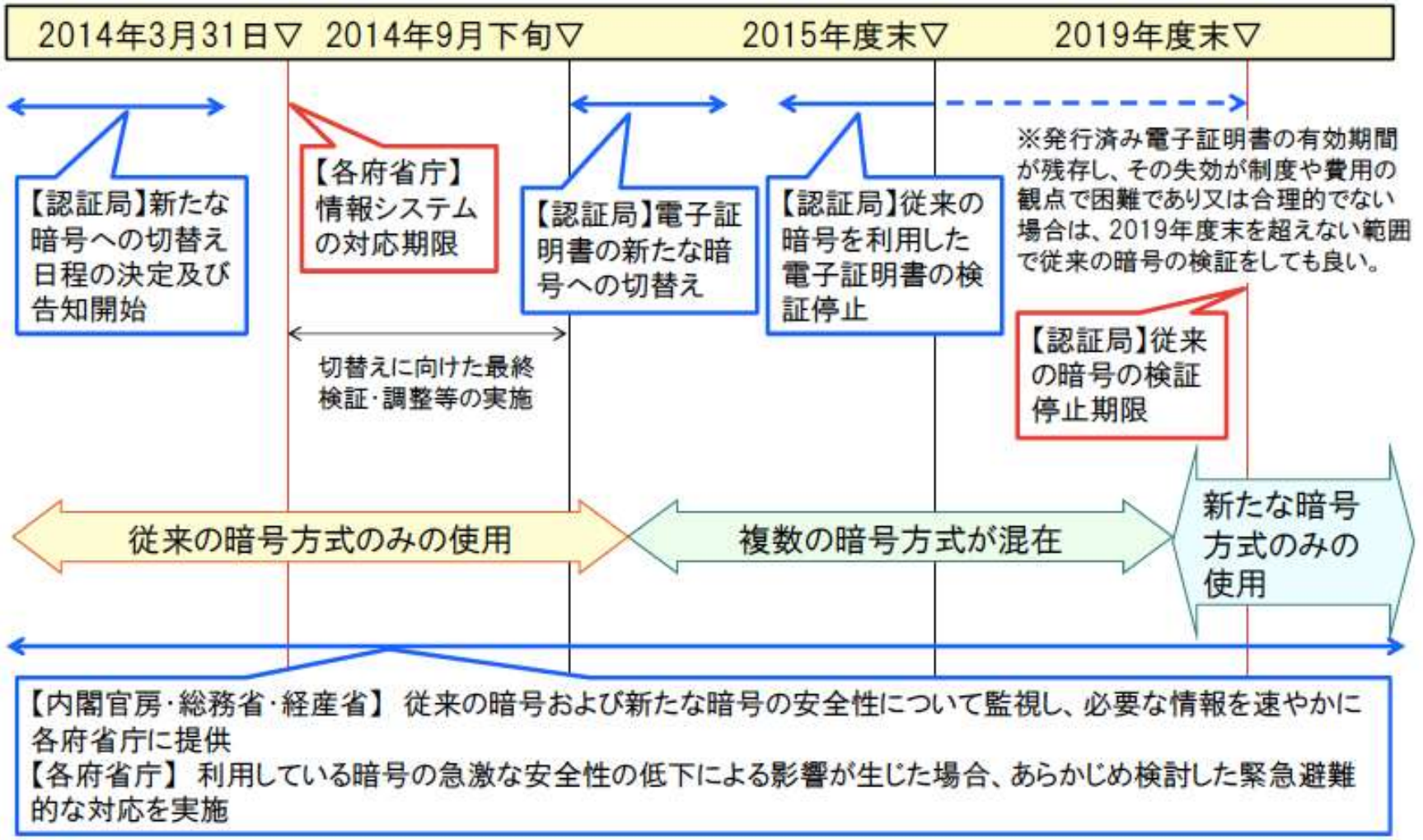
政府機関の情報システムにおいて使用されている暗号アルゴリズムSHA-1及びRSA1024に係る移行指針

CRYPTREC
Cryptography Research and Evaluation Committees

内閣官房情報セキュリティセンター(NISC) より2008年4月22日 公開

2008年 情報セキュリティ政策会議

（参考）政府機関における暗号移行スケジュール



CRYPTREC
Cryptography Research and Evaluation Committees

SHA-1の安全性低下に伴う影響

- CRYPTREC 暗号リストに掲載されている暗号技術に対する影響を調査中
  - 東京工業大学 田中圭介氏に協力依頼

現時点で、見解が得られている暗号技術

技術分類		名称
公開鍵暗号	守秘	RSA-OAEP
	署名	DSA
		ECDSA
		RSA-PSS

公開鍵暗号_守秘

- RSA-OAEP 
  - 用いられているハッシュ関数に衝突攻撃への耐性が保証されていなかったとしても、IND-CCA2 安全性が保たれる [KNTX10]
    - 第 2 原像攻撃 や 原像攻撃への耐性が保証されない場合についても、IND-CCA2 安全性が保たれる

[KNTX10] Security of Encryption Scheme in Weakened Random Oracle Models,
Akinori Kawachi, Akira Numayama, Keisuke Tanaka, Keita Xagawa, Public Key Cryptography 2010: 403-419

公開鍵暗号_署名

- DSA, ECDSA, (RSA-FDH) 
  - 用いられているハッシュ関数に衝突攻撃への耐性が保証されていないと、選択的文書攻撃に対して存在的偽造不可能性が保たれない

- RSA-PSS 
  - 十分に長い salt をとることにより、安全性は保たれる[KNTX08][LN09]

[KNTX08] Security of Digital Signature Schemes in Weakened Random Oracle Models.
Akira Numayama, Toshiyuki Isshiki, Keisuke Tanaka:, Public Key Cryptography 2008: 268-287
[LN09] How Risky Is the Random-Oracle Model? Gaëtan Leurent, Phong Q. Nguyen, CRYPTO 2009: 445-464

CRYPTREC
Cryptography Research and Evaluation Committees

SHA-1 に対する CRYPTREC の見解と対応方針

- SHA-1は、「CRYPTREC暗号リスト」の「運用監視暗号リスト」に掲載している(2013年3月策定)
- 互換性維持以外の目的での利用を推奨しない
- SHA-1 の安全性低下が進んでいることから、SHA-256 等のより安全なハッシュ関数への移行を推奨する
- 「CRYPTREC暗号技術ガイドライン(SHA-1)」の更新作業中

CRYPTREC
Cryptography Research and Evaluation Committees

CRYPTREC 暗号技術ガイドライン(SHA-1)

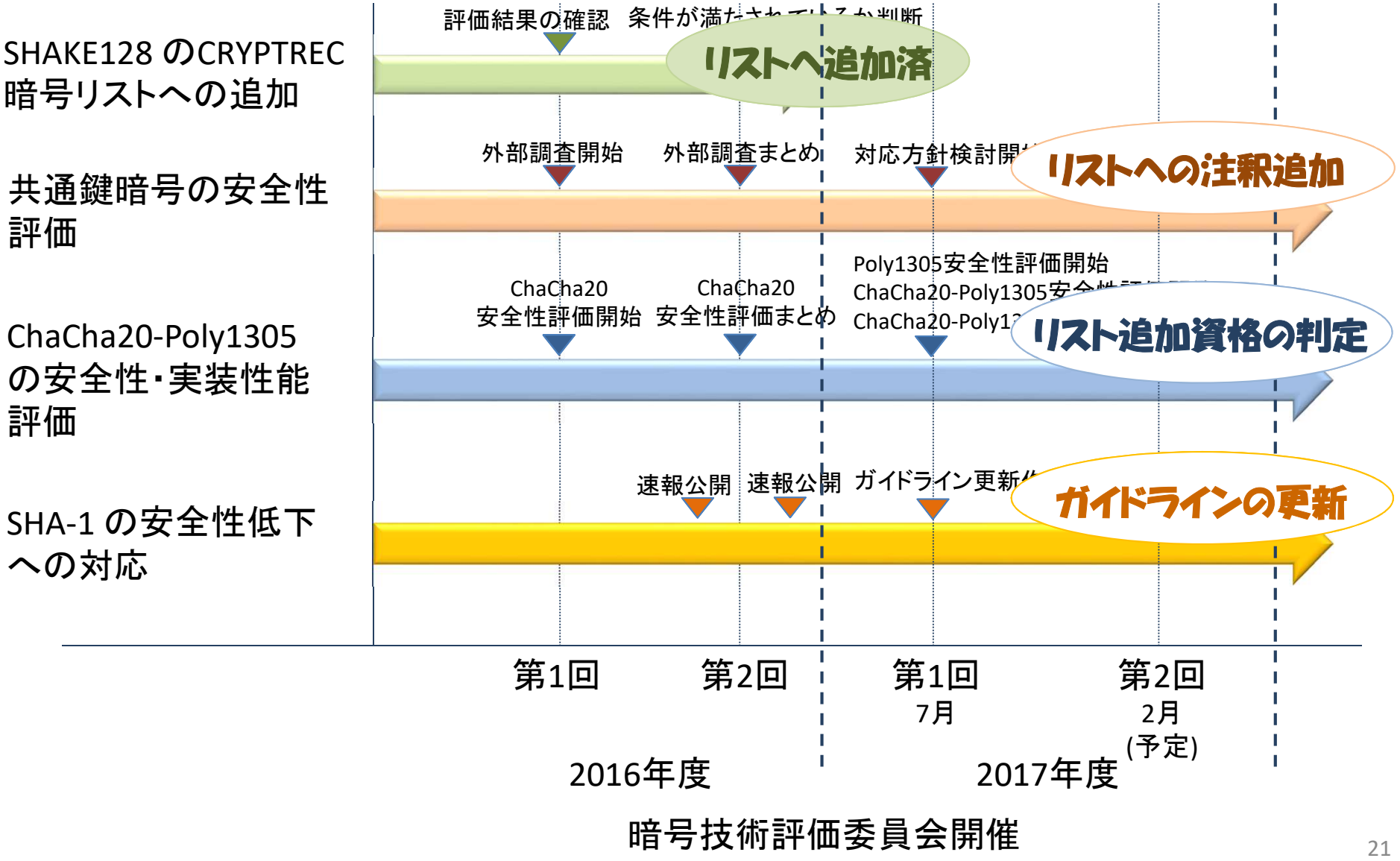
- 2014年3月発行
- 更新版を今年度末に公開予定
  - 有識者のご協力のもと更新版を作成
    - セコム IS 研究所　松本泰氏
      佐藤雅史氏
      島岡政基氏
  - 外部関連組織のレビューも予定
  - 暗号技術評価委員会による審議

CRYPTREC
Cryptography Research and Evaluation Committees

2017年度暗号技術評価委員会活動予定

- 共通鍵暗号の安全性評価
  - 64ビットブロック暗号の安全な利用方法に関する注釈の追加
- ChaCha20-Poly1305 の安全性・実装性能評価
  - 安全性・実装性能ともに CRYPTREC 暗号リストへの追加に十分な条件を満たしているかの判断
  - CRYPTREC 暗号リストへの新規カテゴリ新設の検討
- SHA-1 の安全性低下への対応
  - CRYPTREC 暗号技術ガイドライン(SHA-1)更新版公開

主な活動内容


SHAKE128 のCRYPTREC暗号リストへの追加
共通鍵暗号の安全性評価
ChaCha20-Poly1305の安全性・実装性能評価
SHA-1 の安全性低下への対応
評価結果の確認
リストへ追加済
外部調査開始
外部調査まとめ
対応方針検討開
リストへの注釈追加
ChaCha20
安全性評価開始
ChaCha20
安全性評価まとめ
Poly1305安全性評価開始
ChaCha20-Poly1305安全
ChaCha20-Poly1
リスト追加資格の判定
速報公開
速報公開
ガイドライン更新
ガイドラインの更新
第1回
第2回
第1回
7月
第2回
2月
(予定)
2016年度
2017年度
暗号技術評価委員会開催

付録

64ビットブロック暗号 MISTY1の安全性に関する速報

2015年8月12日速報

CRYPTREC
Cryptography Research and Evaluation Committees

ENGLISH

- CRYPTRECとは
- CRYPTRECの体制
- CRYPTRECの沿革
- CRYPTREC報告書
- 技術報告書
- CRYPTREC暗号リスト
- CRYPTEC暗号の仕様書
- 関連機関等のご案内

トピックス

64ビットブロック暗号MISTY1の安全性について（続報）

平成27年8月12日
CRYPTREC暗号技術評価委員会

CRYPTREC暗号リストの推奨候補暗号リスト[1]に掲載されている64ビットブロック暗号MISTY1 に対する解析結果を示した論文が発表され[2]、CRYPTRECより本論文に対する見解[3]を7月16日に出したところですが、このたび、この解読計算量をさらに削減した新たな解析結果が国際暗号学会（International Association for Cryptologic Research (IACR)）のアーカイブサイトIACR ePrint Archive にて7月30日に発表されました[4]。

新たな解析結果では、解読に必要なデータ量は2^{64}と非常に多く、すべての（平文, 暗号文）の組を集める必要があるものの、$2^{69.5}$回の暗号化演算に相当する現実的な計算量でMISTY1の128ビットの鍵を導出することができると示されています。しかしながら、この攻撃は、解読に必要なデータ量が膨大であることから、現実的な脅威ではないと考えられます。CRYPTREC では、MISTY1の安全性に関して引き続き調査を行い、CRYPTREC Webサイトにて報告する予定です。

表：Integral Cryptanalysis によるMISTY1の解読計算量

	解読に必要なデータ量[5]	解読に必要な計算量[6]
藤堂による解析結果[2]	$2^{63.58}$	2^{121}
藤堂による解析結果[2]	$2^{63.994}$	$2^{107.9}$
Bar-Onによる解析結果[4]	2^{64}	$2^{69.5}$

※詳細は下記サイト参照

http://www.cryptrec.go.jp/topics/cryptrec_20150812_misty1_cryptanalysis.html

暗号アルゴリズムの脆弱性に関する情報発信フロー