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

2015年度 CRYPTREC 体制

暗号技術検討会

2015年度新設

CRYPTRECの在り方に関する検討グループ（H27.6～H27.8）

重点課題検討タスクフォース（H27.11～）

暗号技術評価委員会

（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

暗号技術活用委員会

（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

情報システムにおける暗号技術のセキュリティ確保の全体俯瞰図

CRYPTREC
Cryptography Research and Evaluation Committees

情報システム全体のセキュリティ

システム開発のセキュリティ

- システム仕様
  - 暗号製品仕様
    - 暗号プロトコル仕様
      - 暗号プリミティブ仕様
- 実装
  - 暗号製品実装
    - 暗号プロトコル実装
      - 暗号プリミティブ実装

運用段階のセキュリティ

- システム運用規程
  - 暗号製品運用規程
    - 脆弱性対応規程
      - 危殆化対応規程
- 実運用
  - 暗号製品運用
    - 脆弱性対応
      - 危殆化対応

暗号技術評価委員会の主活動範囲

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 総合情報学専攻(セキュリティ情報学コース) 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 情報理工学部情報システム学科 教授
委員	金子 敏信	東京理科大学 理工学部電気電子情報工学科 教授
委員	佐々木 良一	東京電機大学 未来科学部情報メディア学科 教授
委員	高木 剛	国立大学法人九州大学 マス・フォア・インダストリ研究所 教授
委員	手塚 悟	東京工科大学 コンピュータサイエンス学科 教授
委員	本間 尚文	国立大学法人東北大学 大学院情報科学研究科 准教授
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 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 室長
委員	山村 明弘	国立大学法人秋田大学 大学院工学資源学研究科情報工学専攻 教授
委員	渡辺 創	国立研究開発法人産業技術総合研究所 情報技術研究部門 上級主任研究員

（五十音順、敬称略、所属は2015年度末時点もの）

CRYPTREC
Cryptography Research and Evaluation Committees

2015年度暗号技術評価委員会活動

① 暗号技術の安全性及び実装に係る監視及び評価

② 暗号技術に関する注意喚起レポートの公表

③ 新世代暗号に係る調査

2015年度暗号技術評価委員会活動

① 暗号技術の安全性及び実装に係る監視及び評価

- **CRYPTREC 暗号リスト**の安全性及び実装に係る技術に関する監視
- 標準化動向に鑑み電子政府システム等での利用が見込まれると判断される暗号技術の追加を検討

CRYPTREC 暗号リストの位置づけ

電子政府推奨暗号リスト

- CRYPTREC により安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリスト

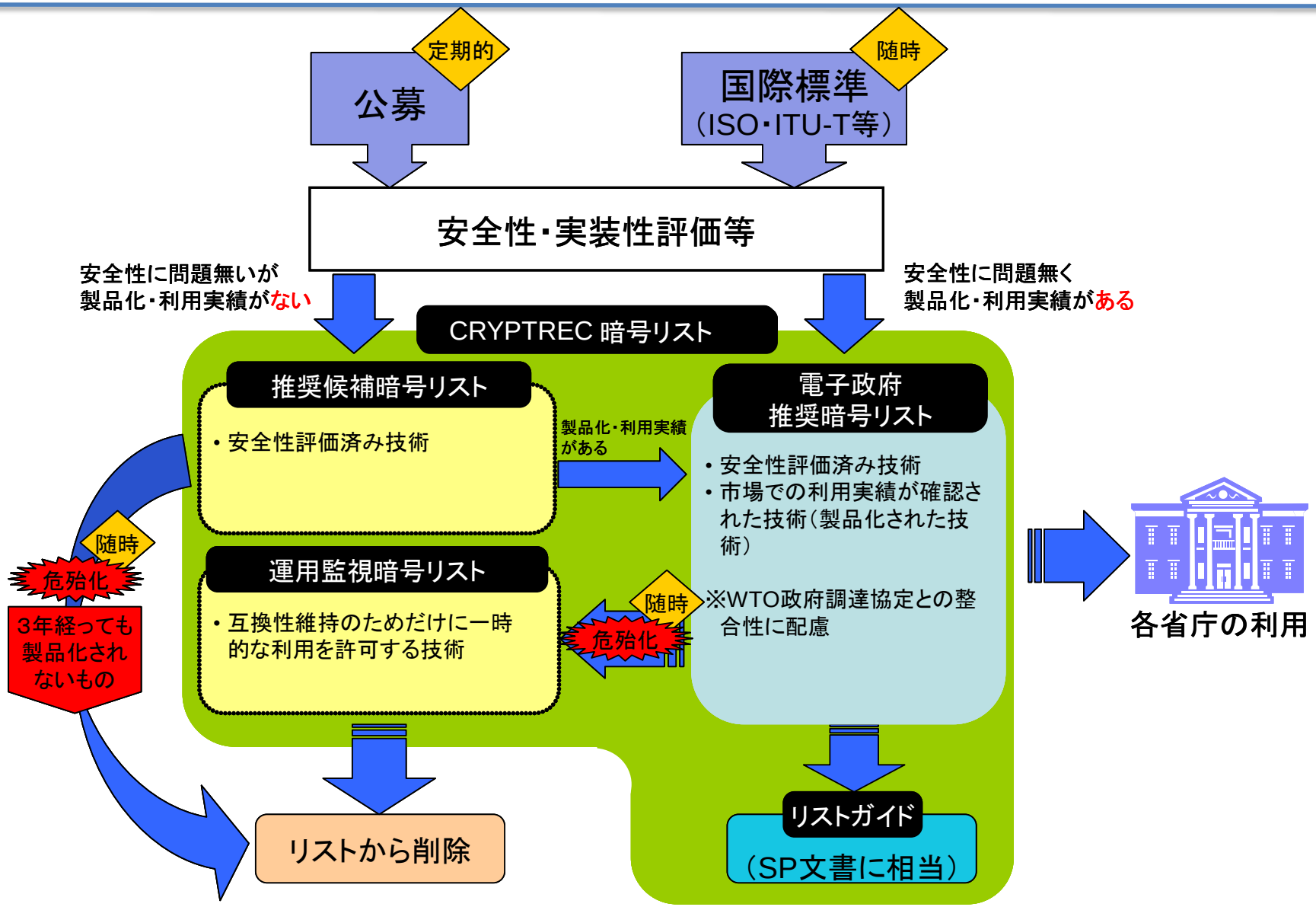
推奨候補暗号リスト

- CRYPTREC により**安全性**及び**実装性能**が確認され、今後、電子政府推奨暗号リストに掲載される可能性のある暗号技術のリスト

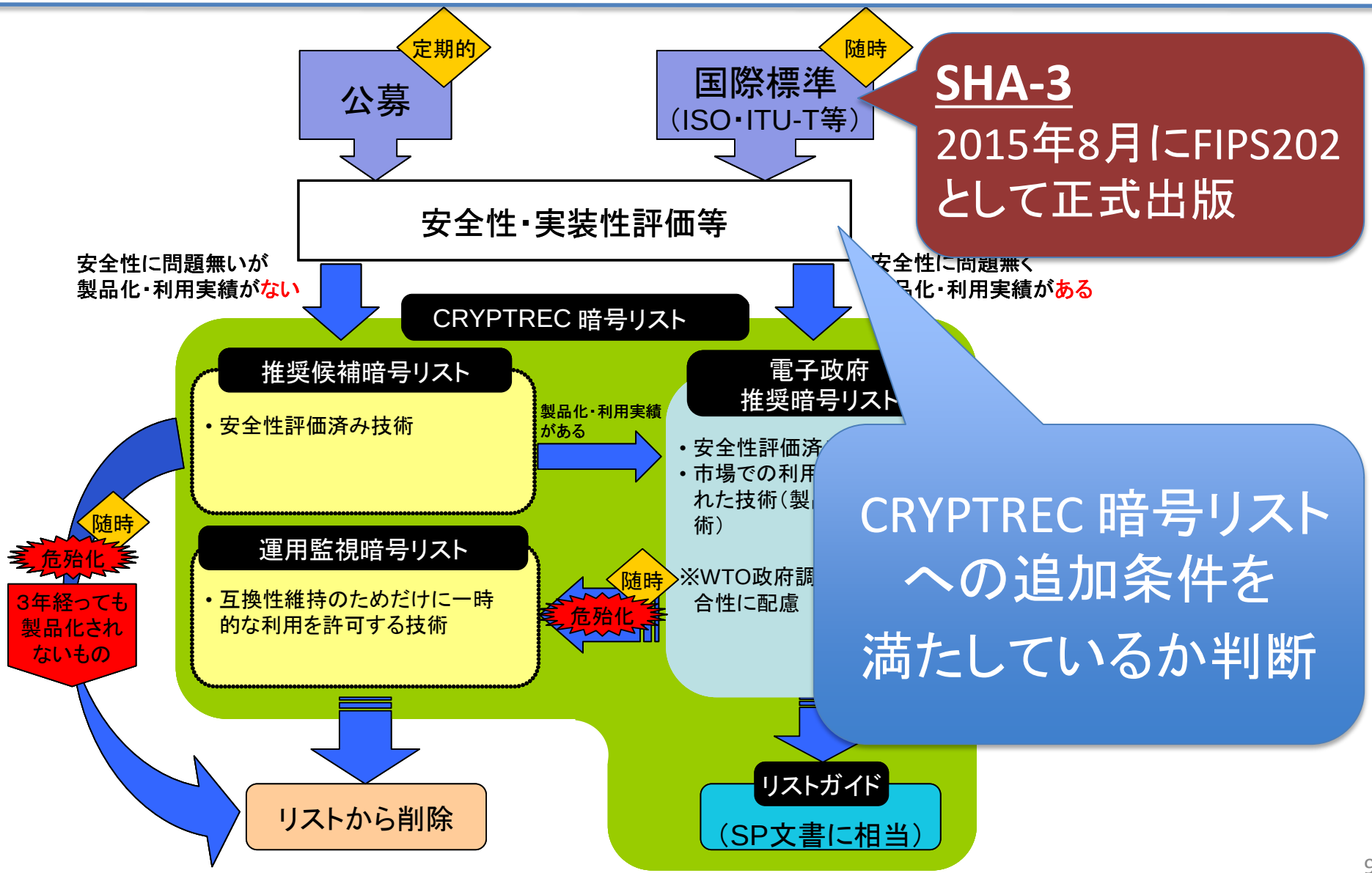
運用監視暗号リスト

- 実際に解読されるリスクが高まるなど、推奨すべき状態ではなくなった暗号技術のうち、互換性維持のために継続利用を容認するもののリスト。互換性維持以外の目的での利用は推奨しない

CRYPTREC 暗号リストの構成



CRYPTREC 暗号リストへの追加の検討：SHA 関連



ハッシュ関数 SHA-3 (および SHA-2) の評価結果

CRYPTREC
Cryptography Research and Evaluation Committees

安全性評価 : 安全性に対して十分なマージンがあり、現実的な脅威の観点から大きな問題点は見つかっていない

実装性能評価: ソフトウェア実装、ハードウェア実装ともに実用上、十分な実装性能を有する

※詳細は付録参照 (p25-30)

下記の5アルゴリズムについて

CRYPTREC暗号リストへの追加条件を満たしている

と判断した

- SHA-512/256
- SHA3-256
- SHA3-384
- SHA3-512
- SHAKE256(※)

(※) ハッシュ長は 256 ビット以上とする。

暗号技術検討会による審議

第2回暗号技術検討会決議 (2016年3月29日)
「推奨候補暗号リスト」に掲載し、
然るべきタイミングで実績調査を実施し、調査結果に応じて
「電子政府推奨暗号リスト」への掲載を検討する。

安全性に問題無いが
製品化・利用実績がない

安全性に問題無く
製品化・利用実績がある

CRYPTREC 暗号リスト

推奨候補暗号リスト
- 安全性評価済み技術

製品化・利用実績がある

電子政府
推奨暗号リスト
- 安全性評価済み技術
- 市場での利用実績が確認された技術（製品化された技術）

※WTO政府調達協定との整合性に配慮

運用監視暗号リスト
- 互換性維持のためだけに一時的な利用を許可する技術

随時
危殆化

随時
危殆化

3年経っても
製品化されないもの

リストから削除

リストガイド
（SP文書に相当）

各省庁の利用

CRYPTREC 暗号リスト

CRYPTREC Cryptography Research and Evaluation Committees

推奨候補暗号リスト

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM
共通鍵暗号	64ビット ブロック暗号	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
	128ビット ブロック暗号	CIPHERUNICORN-A
		CLEFIA
		Hierocrypt-3
		SC2000
	ストリーム暗号	Enocoro-128v2
		MUGI
		MULTI-S01
ハッシュ関数		該当なし
暗号利用 モード	秘匿モード	該当なし
	認証付き 秘匿モード	該当なし
メッセージ認証コード		PC-MAC-AES
エンティティ認証		ISO/IEC 9798-4

2016年3月29日付変更

ハッシュ関数	SHA-512/256
	SHA3-256
	SHA3-384
	SHA3-512
	SHAKE256(注12)

(注12)ハッシュ長は256ビット以上とすること。

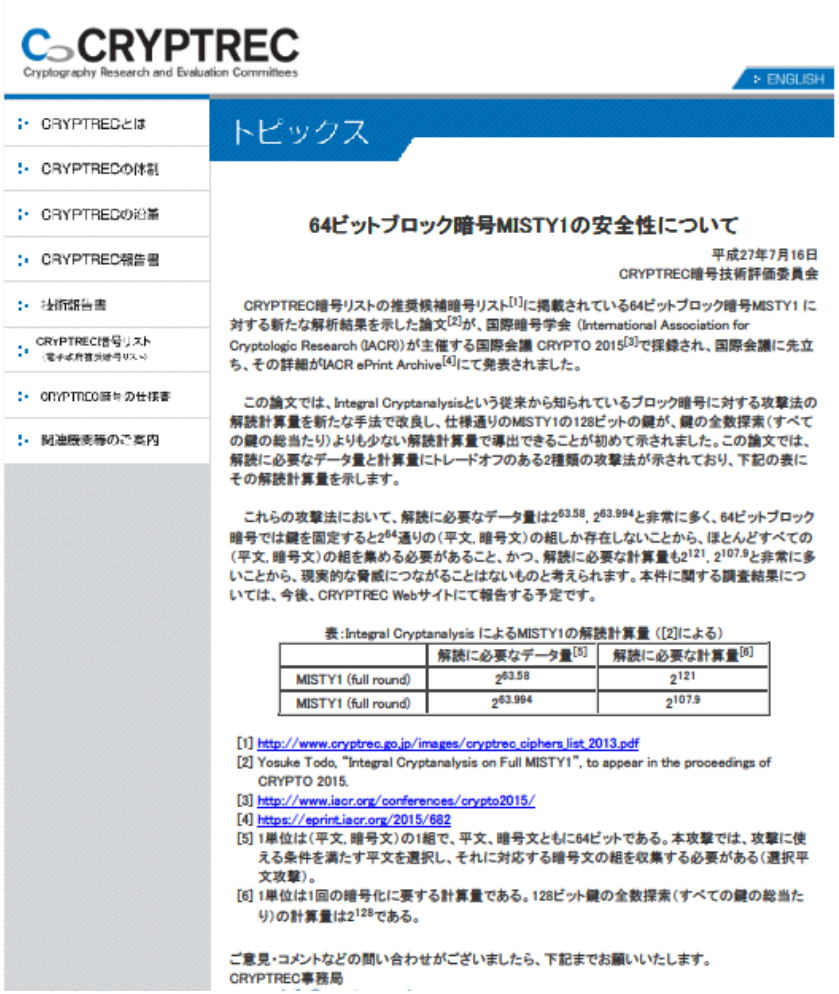
2015年度暗号技術評価委員会活動

② 暗号技術に関する注意喚起レポートの公表

- MISTY1 に関する解析の速報および続報
- SHA-1 の安全性に関する速報

64ビットブロック暗号 MISTY1 の安全性について

2015年7月16日



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（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

64ビットブロック暗号MISTY1の安全性について

平成27年7月16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 に対する新たな解析結果を示した論文[2]が、国際暗号学会（International Association for Cryptologic Research (IACR)）が主催する国際会議 CRYPTO 2015[3]で採録され、国際会議に先立ち、その詳細がIACR ePrint Archive[4]にて発表されました。

この論文では、Integral Cryptanalysisという従来から知られているブロック暗号に対する攻撃法の解読計算量を新たな手法で改良し、仕様通りのMISTY1の128ビットの鍵が、鍵の全数探索（すべての鍵の総当たり）よりも少ない解読計算量で導出できることが初めて示されました。この論文では、解読に必要なデータ量と計算量にトレードオフのある2種類の攻撃法が示されており、下記の表にその解読計算量を示します。

これらの攻撃法において、解読に必要なデータ量は$2^{63.58}$, $2^{63.994}$と非常に多く、64ビットブロック暗号では鍵を固定すると2^{64}通りの（平文, 暗号文）の組しか存在しないことから、ほとんどすべての（平文, 暗号文）の組を集める必要があること、かつ、解読に必要な計算量も2^{121}, $2^{107.9}$と非常に多いことから、現実的な脅威につながることはないものと考えられます。本件に関する調査結果については、今後、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（[2]による）

	解読に必要なデータ量[5]	解読に必要な計算量[6]
MISTY1 (full round)	$2^{63.58}$	2^{121}
MISTY1 (full round)	$2^{63.994}$	$2^{107.9}$

[1] http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2013.pdf
[2] Yosuke Todo, "Integral Cryptanalysis on Full MISTY1", to appear in the proceedings of CRYPTO 2015.
[3] http://www.iacr.org/conferences/crypto2015/
[4] https://eprint.iacr.org/2015/682
[5] 1単位は（平文, 暗号文）の1組で、平文、暗号文ともに64ビットである。本攻撃では、攻撃に使える条件を満たす平文を選択し、それに対応する暗号文の組を収集する必要がある（選択平文攻撃）。
[6] 1単位は1回の暗号化に要する計算量である。128ビット鍵の全数探索（すべての鍵の総当たり）の計算量は2^{128}である。

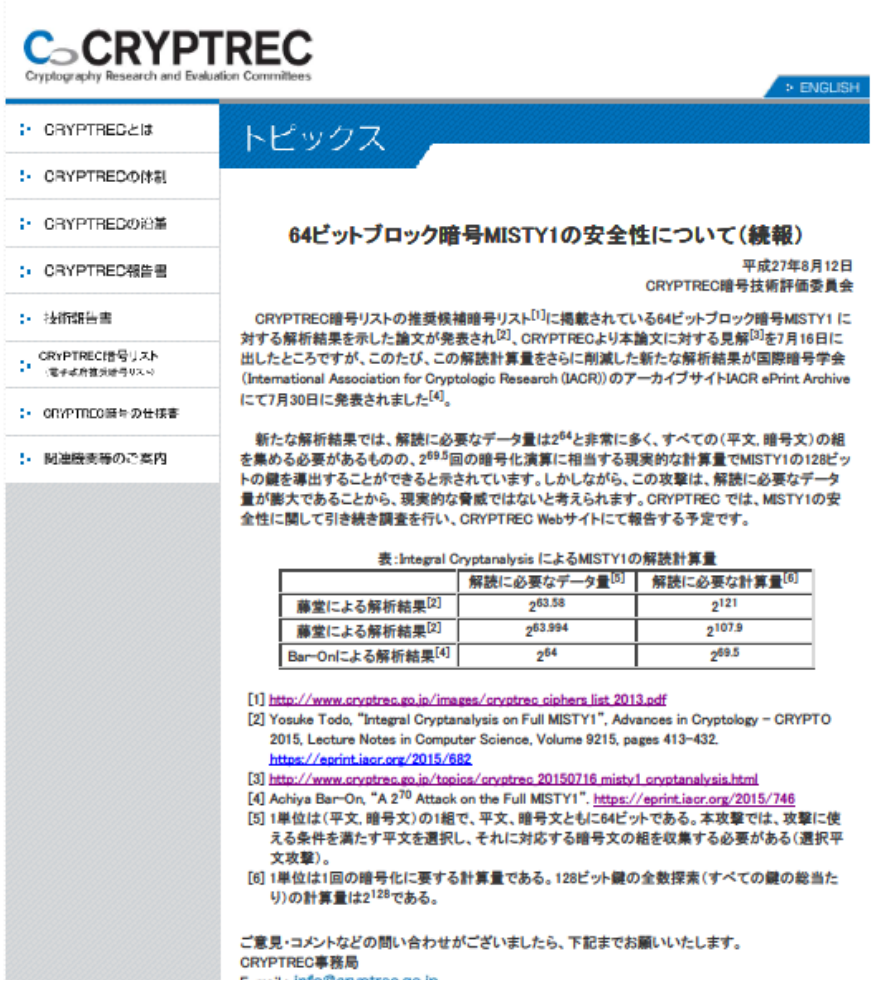
ご意見・コメントなどの問い合わせがございましたら、下記までお願いいたします。
CRYPTREC事務局

※詳細は下記サイト参照
http://www.cryptrec.go.jp/topics/cryptrec_20150716_misty1_cryptanalysis.html

64ビットブロック暗号 MISTY1 の安全性について

2015年7月16日

2015年8月12日



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}	$2^{69.5}$

[1] http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2013.pdf
[2] Yosuke Todo, "Integral Cryptanalysis on Full MISTY1", Advances in Cryptology – CRYPTO 2015, Lecture Notes in Computer Science, Volume 9215, pages 413–432. https://eprint.iacr.org/2015/682
[3] http://www.cryptrec.go.jp/topics/cryptrec_20150716_misty1_cryptanalysis.html
[4] Achiya Bar-On, "A 2^{70} Attack on the Full MISTY1". https://eprint.iacr.org/2015/746
[5] 1単位は（平文, 暗号文）の1組で、平文、暗号文ともに64ビットである。本攻撃では、攻撃に使える条件を満たす平文を選択し、それに対応する暗号文の組を収集する必要がある（選択平文攻撃）。
[6] 1単位は1回の暗号化に要する計算量である。128ビット鍵の全数探索（すべての鍵の総当たり）の計算量は2^{128}である。

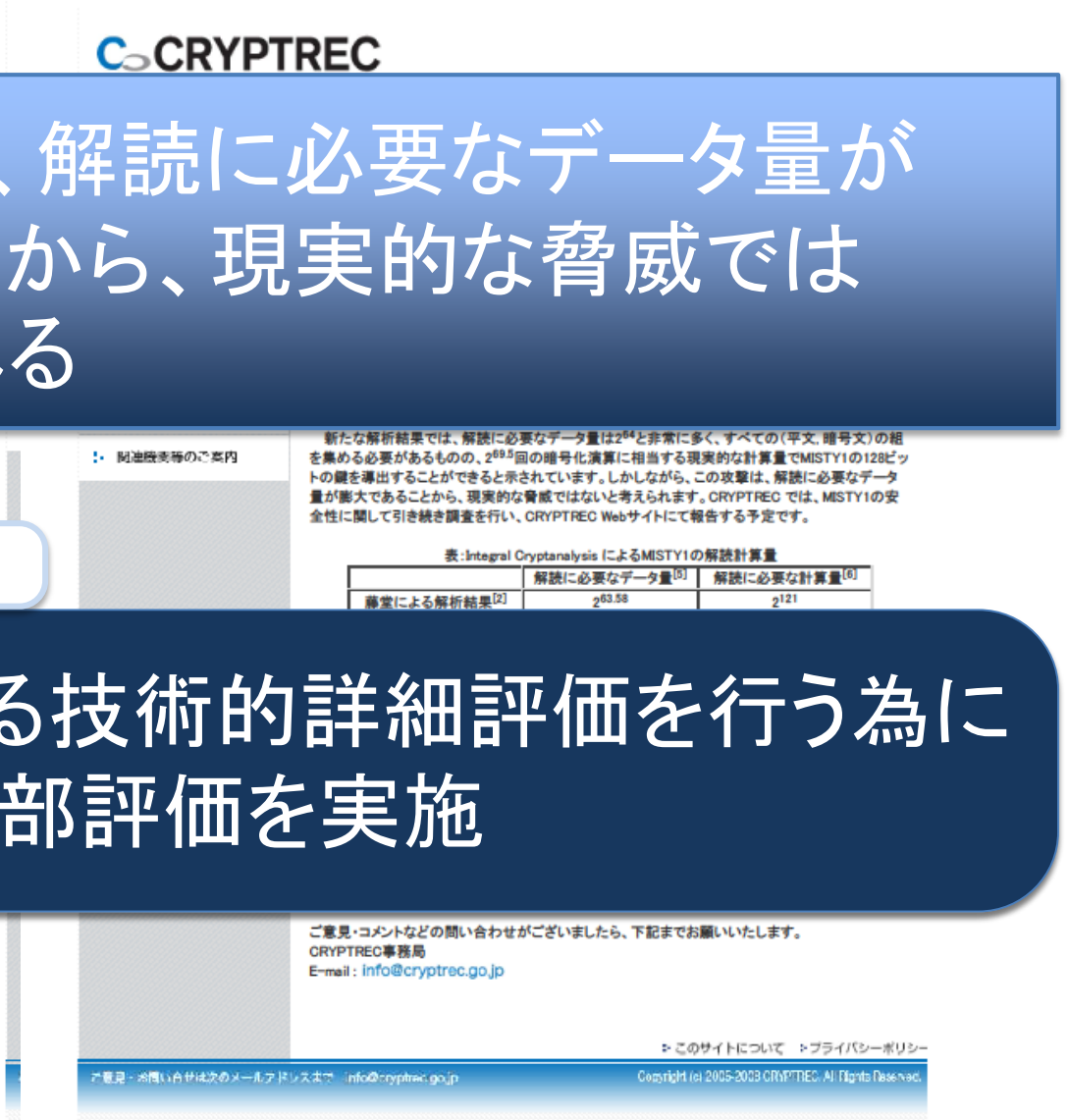
ご意見・コメントなどの問い合わせがございましたら、下記までお願いいたします。
CRYPTREC事務局

※詳細は下記サイト参照
http://www.cryptrec.go.jp/topics/cryptrec_20150812_misty1_cryptanalysis.html

64ビットブロック暗号 MISTY1 の安全性について

速報での見解

今回の攻撃は、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る


CRYPTREC

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}

ご意見・コメントなどの問い合わせがございましたら、下記までお願いいたします。
CRYPTREC事務局
E-mail : info@cryptrec.go.jp

このサイトについて　プライバシーポリシー

Copyright (c) 2005-2023 CRYPTREC. All Rights Reserved.

H27 年度に行った評価

本攻撃に関する技術的詳細評価を行う為に外部評価を実施

外部評価：Integral 攻撃の最新動向と MISTY1 等への適用

- 評価者

  藤堂　洋介 氏 (NTTセキュアプラットフォーム研究所)

- 評価者の見解
  - 現段階では、MISTY1 の現実的な利用における安全性を脅かすものではないと考えられる
  - 現段階では、AES の安全性には影響はないと考えられる
  - 攻撃手法の改良可能性がある

※詳細は下記サイト参照
http://www.cryptrec.go.jp/estimation.html

今後の方針：MISTY1 について

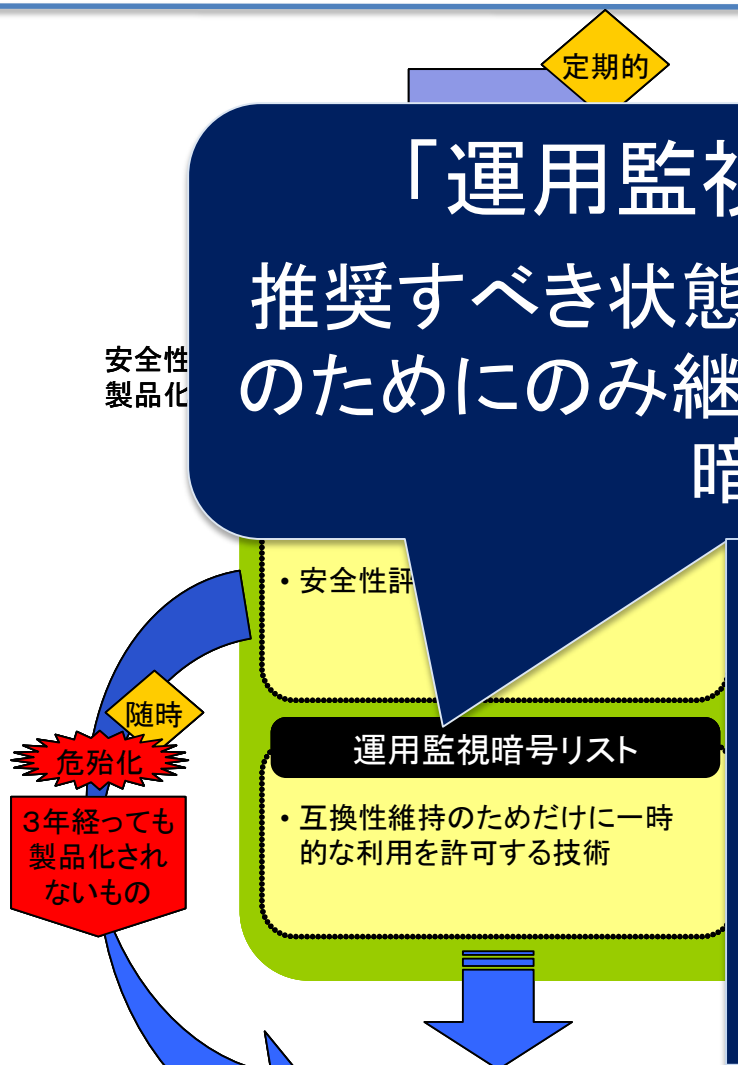
MISTY1 の安全性について

「解読に必要なデータ量が膨大（2^{64}）である
ことから、現実的な脅威ではない」
という見解を継続する

H28 年度予定

当面は、本見解を維持しつつ、
本年度(H28)も検討を継続し、
技術的根拠が揃った時点で新たな見解を示す

SHA-1 の現状



「運用監視リスト」に掲載

推奨すべき状態ではなく、互換性維持のためにのみ継続利用を容認している暗号技術

CRYPTREC 暗号技術ガイドライン (SHA-1)

SHA-1 の利用用途に応じた注意事項、推奨されない利用範囲、許容される利用範囲などを掲載

※詳細は下記サイト参照

http://www.cryptrec.go.jp/report/c13_tech_guideline_SHA-1_web.pdf

SHA-1 に対する解析の進展

2015年12月15日

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（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の安全性について

平成27年12月18日
CRYPTREC暗号技術評価委員会

2015年10月8日に、CWI(オランダ)、INRIA(フランス)、NTU(シンガポール)の共同研究チームは、ハッシュ関数SHA-1のフルラウンド(全80ステップ中80ステップ)に対して、仕様より緩い条件下ながら初めて衝突発見に成功したと発表しました[1]。本発表のもとになっている論文は国際暗号学会(International Association for Cryptologic Research (IACR))のアーカイブサイト IACR ePrint Archive で公開されています[2]。

今回の発表された内容は、SHA-1の衝突発見に直接つながるものではありませんが、SHA-1の衝突発見に至るまでの節目となる出来事、マイルストーンの1つであり、近い将来にSHA-1の衝突が発見されるという予測を強く裏付けるものです。当委員会としては、従前通り、SHA-1に関する移行対策を実施して頂きたいと考えています。

当委員会(当時は暗号技術監視委員会)では、2005年にSHA-1に対する衝突発見アルゴリズムが論文発表された後、安全性評価を行った結果、近い将来この攻撃アルゴリズムが実際に実装可能になり、衝突発見困難性に対して脅威になるものと判断しました[3]。その後、情報セキュリティ政策会議から、2008年にSHA-1に関して移行指針[4]が発表されています。現在、CRYPTRECでは、SHA-1を「CRYPTREC暗号リスト」の「運用監視暗号リスト」[5]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、SHA-1の用途ごとの具体的な利用指針として、「CRYPTREC暗号技術ガイドライン(SHA-1)」[6]を公開しています。

引き続き、CRYPTRECでは、暗号技術などの監視・評価を行い、SHA-1の取り扱いなどについて変更が生じた場合は、CRYPTREC Web サイトなどを通じてお知らせします。

ご意見・コメントなどの問い合わせがございましたら、下記までお願いいたします。

CRYPTREC事務局
E-mail : info@cryptrec.go.jp

【参考文献】

[1] Press Release "Researchers urge: industry standard SHA-1 should be retracted sooner", CWI, Inria, NTU, October 8, 2015.
https://www.cwi.nl/news/2015/researchers-urge-industry-standard-sha-1-should-be-retracted-sooner

[2] Marc Stevens, Pierre Karpman, and Thomas Peyrin, "Freestart collision for full SHA-1". IACR ePrint Archive. https://eprint.iacr.org/2015/967

[3] CRYPTREC Report 2005「暗号技術監視委員会報告」(2006年3月)
http://www.cryptrec.go.jp/report/c05_wat_final.pdf

[4]「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」(平成20年4月22日 情報セキュリティ政策会議決定、平成24年10月26日 情報セキュリティ対策推進会議改定)：

※詳細は下記サイト参照
http://www.cryptrec.go.jp/topics/cryptrec_20151218_sha1_cryptanalysis.html

SHA-1 の安全性について

速報の概要

- SHA-1 の衝突発見に直接つながるものではない
- 一連の研究動向から、近い将来に SHA-1 の衝突が発見されるという注意喚起

H28 年度予定

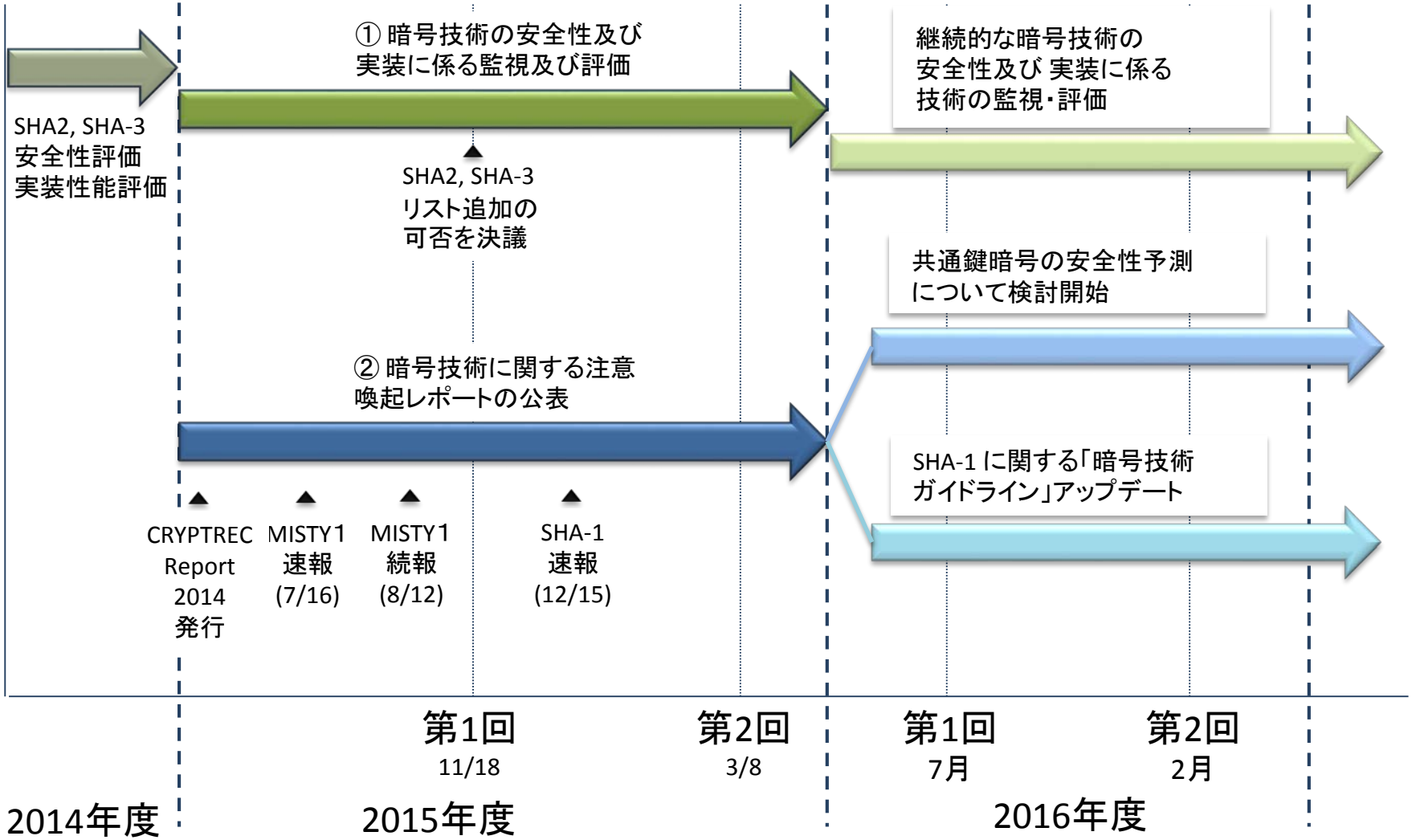
SHA-1 に関する「暗号技術ガイドライン」を最新動向に基づきアップデートを行う

2016年度暗号技術評価委員会活動予定

- 継続的な暗号技術の安全性及び 実装に係る技術の監視・評価の実施
- 共通鍵暗号の安全性予測について検討を開始
- SHA-1 に関する「暗号技術ガイドライン」を最新動向に基づきアップデートを行う

CRYPTREC
Cryptography Research and Evaluation Committees

2015年度実績と今後の予定



暗号技術評価委員会開催

2015年度暗号技術評価委員会活動

① 暗号技術の安全性及び実装に係る監視及び評価

② 暗号技術に関する注意喚起レポートの公表

③ 新世代暗号に係る調査

- 暗号技術調査ワーキンググループ(暗号解析評価)
- 暗号技術調査ワーキンググループ(軽量暗号)

暗号解析評価WG : 高木主査
軽量暗号WG : 本間主査

付録
（SHA-3およびSHA-2 の安全性・実装性能評価結果）

FIPS 180-4 で規定されている SHA-2

アルゴリズム	メッセージ長 (bits)	ブロック長 (bits)	ワード長 (bits)	出力長 (bits)
SHA -224	$< 2^{64}$	512	32	224
SHA -256	$< 2^{64}$	512	32	256
SHA -384	$< 2^{128}$	1024	64	384
SHA -512	$< 2^{128}$	1024	64	512
SHA -512/224	$< 2^{128}$	1024	64	224
SHA -512/256	$< 2^{128}$	1024	64	256

電子政府推奨暗号リストに含まれているアルゴリズム

ハッシュ関数 SHA-3 (および SHA-2) のセキュリティ強度 (p10 参考資料)

CRYPTREC Cryptography Research and Evaluation Committees

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
SHA-224	224	112	224	min(224, 256−*M*)*
SHA-512/224	224	112	224	224
SHA-512/256	256	128	256	256
SHA3-224	224	112	224	224
SHA3-256	256	128	256	256
SHA3-384	384	192	384	384
SHA3-512	512	256	512	512
SHAKE128	*d*	min(*d*/2,128)	≧min(*d*,128)	min(*d*,128)
SHAKE256	*d*	min(*d*/2,256)	≧min(*d*,256)	min(*d*,256)

* メッセージ長が2^Mブロックの時の第2原像攻撃に対する耐性。Merkle-Damgard構成であることからJouxのmulticollision攻撃が適用でき、2^{32}ブロック以上の長いメッセージの場合、全数探索より少ない計算量で第2原像が見つかる。

ハッシュ関数 SHA-3 (および SHA-2) の選出アルゴリズム (p10 参考資料)

CRYPTREC Cryptography Research and Evaluation Committees

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
SHA-512/256	256	128	256	256
SHA3-224	224	112	224	224
SHA3-256	256	128	256	256
SHA3-384	384	192	384	384
SHA3-512	512	256	512	512
SHAKE128	*d*	min(*d*/2,128)	≧min(*d*,128)	min(*d*,128)
SHAKE256	*d*	min(*d*/2,256)	≧min(*d*,256)	min(*d*,256)

256ビット以上のハッシュ関数を選択することが望ましい

* メッセージ長が2^Mブロックの時の第2原像攻撃に対する耐性。Merkle-Damgard構成であることからJouxのmulticollision攻撃が適用でき、2^{32}ブロック以上の長いメッセージの場合、全数探索より少ない計算量で第2原像が見つかる。

ハッシュ関数 SHA-3 の実装性能 (p10 参考資料)

- Xilinx 社の Virtex-5 を用いた高速ハードウェア実装では、回路規模が 1000～2000slice で 6～16Gbps
  - SHA-256 と比べ、回路規模は増加（約2～3 倍）するが、スループット性能は4 倍程度、レイテンシは約 1/2 の時間を実現

- ASIC 実装による性能評価では、FPGA よりも高いスループット性能を有する

- 軽量実装については、数100slice で実装可能

- ハードウェア実装及びソフトウェア実装におけるサイドチャネル耐性は、ブロック暗号 AES と比べて容易ではないと考える

ハッシュ関数 SHA-2 の実装性能 (p10 参考資料)

SHA-224

- SHA-256 とほぼ同等の性能であるが、
  最終データの転送に要する時間を短縮できるため、
  レイテンシの短縮が僅かながら達成できる
- ハッシュ値のメモリ容量を削減できるため、
  数多くのハッシュ値を保存するようなアプリケーション
  において、コスト削減が期待できる

SHA-512/256, SHA-512/224

- SHA-224 や SHA-256 と比べた場合、64bit CPU における
  ソフトウェア実装性能において一定の優位性を有する
  - 64bit 演算を高速で行う CPU の登場に因るところが大きく、
    今後の実装研究に大きな意味を持つ