CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術評価委員会活動報告

委員長　今井 秀樹

東京大学

CRYPTREC体制

暗号技術検討会

事務局：総務省、経済産業省

暗号技術評価委員会

事務局：NICT, IPA

「暗号技術の安全性評価及び実装評価を中心とした技術的な検討課題」を担当

暗号技術活用委員会

事務局：IPA, NICT

「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の活動

①暗号技術の安全性と実装に係る監視及び評価

②暗号技術の安全な利用方法に係る調査

③新世代暗号に係る調査

CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術評価委員会 委員

委員長	今井　秀樹	東京大学 名誉教授
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	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	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 マネージャー
委員	盛合　志帆	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 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	独立行政法人産業技術総合研究所 セキュアシステム研究部門 セキュアサービス研究グループ研究グループ長

各リストの位置づけ

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
電子政府推奨暗号リスト

CRYPTREC Cryptography Research and Evaluation Committees

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS
		RSASSA-PKCS1-v1_5
	守秘	RSA-OAEP
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号	3-key Triple DES
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード	CCM
		GCM
メッセージ認証コード		CMAC
		HMAC
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

CRYPTREC暗号リスト
推奨候補暗号リスト

CRYPTREC Cryptography Research and Evaluation Committees

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

CRYPTREC暗号リスト
運用監視暗号リスト

CRYPTREC
Cryptography Research and Evaluation Committees

技術分類		名称
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5
	鍵共有	該当なし
共通鍵暗号	64ビットブロック暗号	該当なし
	128ビットブロック暗号	該当なし
	ストリーム暗号	128-bit RC4
ハッシュ関数		RIPEMD-160
		SHA-1
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		CBC-MAC
エンティティ認証		該当なし

2014年度の活動

CRYPTREC
Cryptography Research and Evaluation Committees

①暗号技術の安全性及び実装に係る監視及び評価

- CRYPTREC暗号等の解析結果の監視
- ハッシュ関数（SHA-2 ファミリーおよび SHA-3）の安全性について外部評価の実施

②新世代暗号に係る調査

- 暗号解析評価WG、軽量暗号WG

③暗号技術の安全な利用方法に係る調査

- CRYPTREC暗号技術ガイドラインの更新

その他

- RC4 の注釈の変更
- ECDSA、ECDH の仕様書参照先変更の検討

2014年度の活動
①暗号技術の安全性及び実装に係る監視及び評価

CRYPTREC Cryptography Research and Evaluation Committees

外部評価(ハッシュ関数の安全性評価)

- SHA-512/256、SHA-512/224、SHA-224、SHA-3

	SHA-512/256 SHA-512/224 SHA-224	SHA-3 SHAKE128 SHAKE256
評価者	Donghoon Chang (Indraprastha Institute of Information Technology, Delhi, India)	
	Florian Mendel (Graz University of Technology, Austria)	Itai Dinur (École Normale Supérieure, France)

2014年度の活動
①暗号技術の安全性及び実装に係る監視及び評価

CRYPTREC Cryptography Research and Evaluation Committees

外部評価(ハッシュ関数の安全性評価)

- ハッシュ関数に求められる安全性要件
  - **Collision resistance**（衝突攻撃に対する耐性）

攻撃が成功すると ⇒ あるメッセージの署名が別のメッセージの署名にすり替えられてしまう

  - **Preimage resistance**（原像攻撃に対する耐性）

攻撃が成功すると ⇒ ハッシュ関数の任意の出力値から、この出力値を与える入力値を求めることができてしまう

  - **Second preimage resistance**（第2原像攻撃に対する耐性）

攻撃が成功すると ⇒ 任意のターゲットとなるメッセージの署名が別のメッセージの署名にすり替えられてしまう

2014年度の活動
①暗号技術の安全性及び実装に係る監視及び評価

CRYPTREC
Cryptography Research and Evaluation Committees

- 外部評価では、近年のハッシュ関数解析技術の進展により解析が進んでいることが示され、また新規の解析結果も報告された。外部評価レポートで報告された解析結果からは、対象のハッシュ関数の安全性には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。**

- 以上のことから、「**ハッシュ関数 SHA-512/256、SHA-512/224、SHA-224、SHA-3 の安全性には現時点では現実的な脅威につながる問題はない**」という評価結果とした。

2014年度の活動
②新世代暗号に係る調査

CRYPTREC
Cryptography Research and Evaluation Committees

- 暗号解析評価WG
  - 計算機能力評価WGの後継
    - 離散対数問題の困難性に関する調査
    - 格子問題等の困難性に関する調査

- 軽量暗号WG
  - 軽量暗号技術に関する現状調査
  - アプリケーションに関する調査
  - 実装評価の実施
  - 今後の活動方針に関する議論

各 WG からの詳細の報告はこの後の講演にて

2014年度の活動
③暗号技術の安全な利用方法に係る調査

CRYPTREC Cryptography Research and Evaluation Committees

- CRYPTREC暗号技術ガイドラインの更新
  - 2014年度は「CRYPTREC暗号技術ガイドライン（SSL/TLSにおける近年の攻撃への対応）」（2013年度発行）に POODLE 攻撃に対する解説を追加

[SSL/TLS の近年の攻撃動向]
- プロトコルの仕組みを利用した攻撃：BEAST、TIME、CRIME、Lucky Thirteen など
- プロトコル内で用いる暗号として RC4 を用いた場合の攻撃

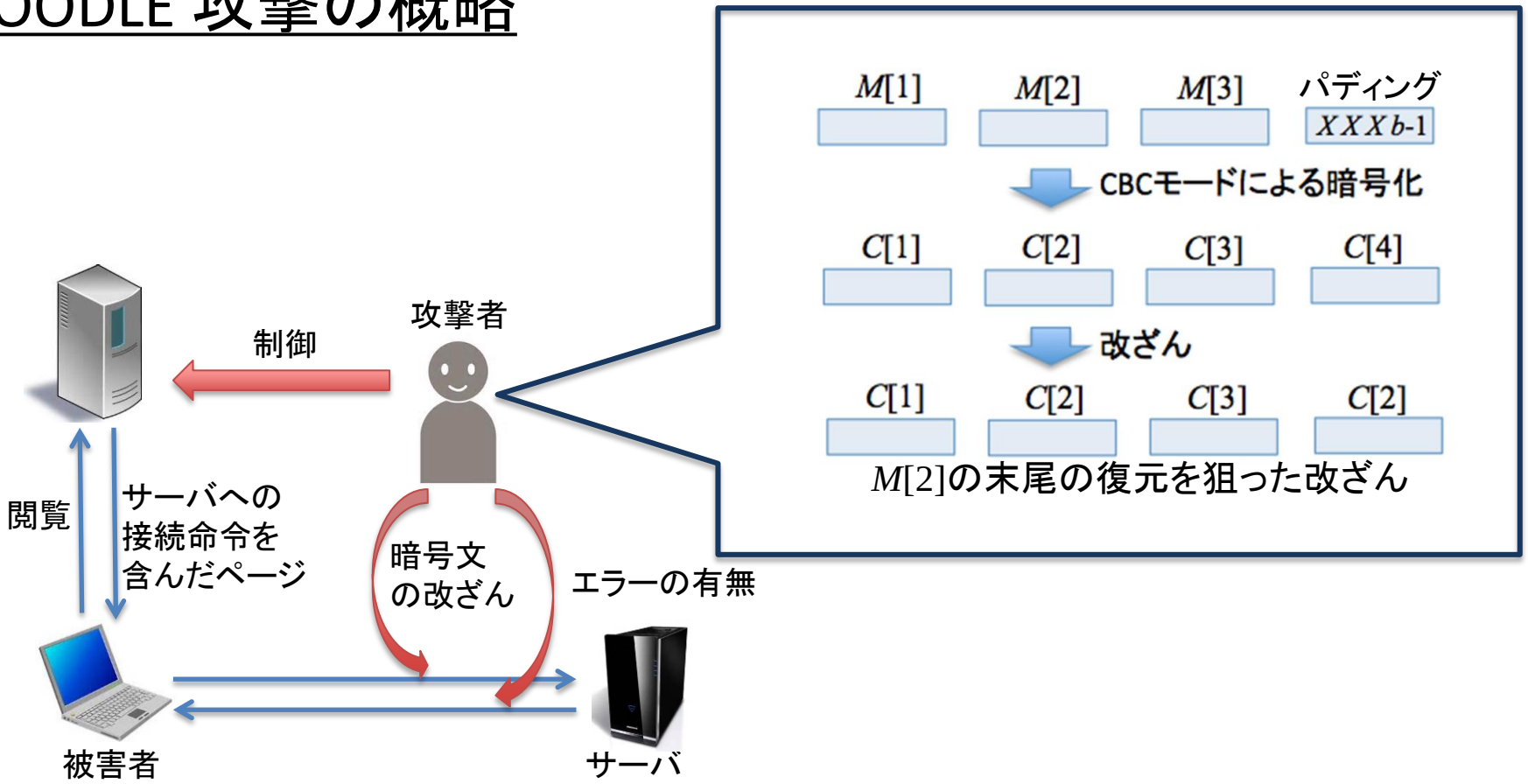
昨年、プロトコルの仕組みを利用した攻撃として新たに POODLE 攻撃が登場

POODLE (Padding Oracle On Downgraded Legacy Encryption)

2014年に発見された比較的新しい、SSL3.0におけるCBCモードに対する攻撃であり、Vaudenayにより 2002 年に提案されたパディングオラクル攻撃の実装の一例と見なすことができる

2014年度の活動
③暗号技術の安全な利用方法に係る調査

POODLE 攻撃の概略



2014年度の活動
③暗号技術の安全な利用方法に係る調査

CRYPTREC Cryptography Research and Evaluation Committees

その他、近年発表された攻撃：

Heartbleed

OpenSSL ライブラリの脆弱性を利用し、**SSL ハートビートの機能のレスポンスを利用してプログラムが扱うデータの情報漏えいを引き起こさせる。**

FREAK (Factoring RSA Export Keys)

中間者攻撃により、**輸出グレード(512ビット以下) のRSAを使って通信を行うように誘導される。**

⇒ 512ビットの RSA は現実的な時間で解読可能

このようにつぎつぎと問題が生じるため、
常に監視している必要がある。

2014年度の活動
RC 4 の注釈変更の検討

CRYPTREC
Cryptography Research and Evaluation Committees

- 128-bit key RC4(以下、RC4という。)は、現在「128-bit RC4は、SSL(TLS1.0以上)に限定して利用すること」という注釈が付与されている。

- 近年、RC4の SSL/TLS での利用における攻撃手法が進展してきたこと、SSL/TLS に対する新たな攻撃とその対応状況を鑑み、注釈の変更を検討した。

2014年度の活動
RC 4 の注釈変更の検討

CRYPTREC
Cryptography Research and Evaluation Committees

- 暗号技術活用委員会の協力も得て、検討を行った結果、早期にRC4からの移行が進むことが好ましく、「今後は極力利用すべきでない」という注釈変更の意図を明確化するために、以下のように RC4 の注釈を変更することとなった。

「互換性維持のために継続利用をこれまで容認してきたが、今後は極力利用すべきでない。SSL/TLSでの利用を含め、電子政府推奨暗号リストに記載された暗号技術への移行を速やかに検討すること。」

2014年度の活動
仕様書の参照先の変更

CRYPTREC
Cryptography Research and Evaluation Committees

- CRYPTREC暗号リストに掲載されている暗号技術ECDSA及びECDHの仕様書の参照先の変更について検討を行った。

- 評価の結果、SECG SEC 1 Ver 2.0には、「軽微な修正」の範囲を超える部分があることが認められた。

- 安全性・実装性のみならず、製品化・利用実績・知財権のほか、実装の適合性評価†にも影響が及ぶため、引き続き検討することとなった。

†暗号モジュール試験及び認証制度を指す

おわりに

- CRYPTRECは2000年に発足して以来、電子政府推奨暗号等の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討することでセキュアなIT社会の実現に貢献してきた。

電子政府推奨暗号リストの信頼性は
多くの暗号研究者によって支えられてきた

- 今後も引き続きCRYPTREC暗号リストの安全性の維持のため、皆様の協力が必要