CRYPTREC Report 2017

平成 30 年 3 月

国立研究開発法人情報通信研究機構
独立行政法人情報処理推進機構

CRYPTREC RP-2000-2017

「暗号技術評価委員会報告」

目次

はじめに

本報告書は、総務省及び経済産業省が主催する暗号技術検討会の下に設置され運営されている暗号技術評価委員会の 2017 年度活動報告である。

暗号技術評価委員会は、国立研究開発法人情報通信研究機構及び独立行政法人情報処理推進機構が共同で運営している。暗号技術評価委員会の 2017 年度の活動として、

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)新しい暗号技術に係る調査および評価

4)暗号技術の安全な利用方法に関する調査

を実施することを暗号技術検討会より承認を得て、活動を実施した。

1) については、電子政府推奨暗号リスト掲載の 64 ビットブロック暗号 3-key Triple DES に付与されている注釈の変更、および、3-key Triple DES を「電子政府推奨暗号リスト」から「運用監視暗号リスト」へ変更することを暗号技術検討会に提案した。また、認証暗号 ChaCha20-Poly1305 の安全性評価及び実装性能調査を実施し、ChaCha20-Poly1305 が、認証暗号として十分な安全性および実装性能を有していると判断し、暗号技術検討会に「推奨候補暗号リスト」への追加を提案した。

2) については、電子政府推奨暗号リスト掲載の DSA 及び DH の安全性にかかわる有限体上の離散対数問題について、注意喚起レポートを発行し、CRYPTREC ホームページで公開した。

3) については、暗号技術調査ワーキンググループ(暗号解析評価)を設置し、Post-Quantum Cryptography(耐量子計算機暗号)の技術動向調査を実施した。併せて、素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関する計算量評価の更新を行った。

4) については、SHA-1 の衝突発見を受け、「暗号技術ガイドライン(SHA-1)」の改定を行い、CRYPTREC ホームページで公開した。改定にあたり、ご協力いただきましたセコム株式会社(松本泰様、佐藤雅史様、島岡政基様)、JNSA 電子署名ワーキンググループ、及び東京工業大学田中圭介様に深く感謝の意を表する。

CRYPTREC は、客観的な評価による安全性及び実装性に優れると判断された暗号技術をリスト化する暗号技術評価プロジェクトとして 2000 年に発足して以来、18 年にわたりその活動は、安全・安心な ICT 社会の実現に貢献してきた。CRYPTREC は世界的にも広く知られ、その活動の一つ一つが CRYPTREC ブランドの信頼の醸成につながっていると考えている。今後も社会の情勢を踏まえ、未来の安心・安全な ICT 社会の実現につなげるべく、社会のニーズに対して、暗号技術の安全性という観点から必要とされる活動を展開していきたいと考えている。

暗号技術評価委員会の活動は暗号技術やその実装及び運用に携わる研究者及び技術者の献身的な協力により成り立っている。末筆ではあるが、本活動に様々な形でご協力頂いている関係者の皆様に深甚な謝意を表する次第である。

暗号技術評価委員会　委員長　太田 和夫

本報告書の利用にあたって

本報告書の想定読者は、一般的な情報セキュリティの基礎知識を有している方である。たとえば、電子政府において電子署名やGPKIシステム等暗号関連の電子政府関連システムに関係する業務についている方などを想定している。しかしながら、個別テーマの調査報告等については、ある程度の暗号技術の知識を備えていることが望まれる。

本報告書の第1章は暗号技術評価委員会の活動概要についての説明である。第2章は暗号技術評価委員会における監視活動に関する報告である。第3章は暗号技術評価委員会の下で活動している暗号技術調査ワーキンググループの活動報告である。

本報告書の内容は、我が国最高水準の暗号専門家で構成される「暗号技術評価委員会」及びそのもとに設置された「暗号技術調査ワーキンググループ」において審議された結果であるが、暗号技術の特性から、その内容とりわけ安全性に関する事項は将来にわたって保証されたものではなく、今後とも継続して評価・監視活動を実施していくことが必要なものである。

本報告書ならびにこれまでに発行されたCRYPTREC報告書、技術報告書、CRYPTREC暗号リスト記載の暗号技術の仕様書は、CRYPTREC事務局（総務省、経済産業省、国立研究開発法人情報通信研究機構、及び独立行政法人情報処理推進機構）が共同で運営する下記のWebサイトで参照することができる。

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

本報告書ならびに上記Webサイトから入手したCRYPTREC活動に関する情報の利用に起因して生じた不利益や問題について、本委員会及び事務局は一切責任をもっていない。

本報告書に対するご意見、お問い合わせは、CRYPTREC事務局までご連絡いただけると幸いである。

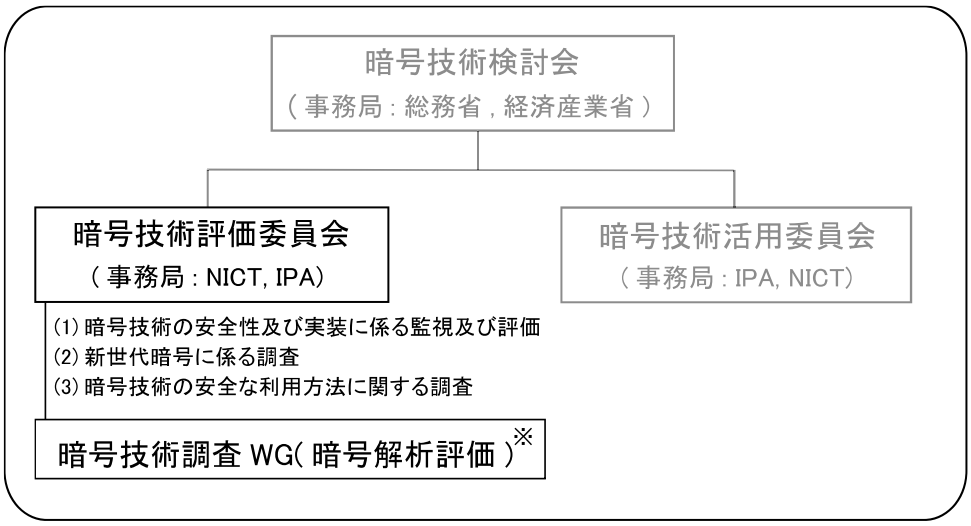
【問合せ先】　info @ cryptrec.go.jp

委員会構成

暗号技術評価委員会(以下、「評価委員会」という。)は、総務省と経済産業省が共同で主催する暗号技術検討会の下に設置され、国立研究開発法人情報通信研究機構(以下、「NICT」という。)と独立行政法人情報処理推進機構(以下、「IPA」という。)が共同で運営する。評価委員会は、CRYPTREC 暗号リスト(付録 1)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観点から、それらの安全性及び実装に係る監視及び評価を行う等、主として技術的活動を担い、暗号技術検討会に助言を行う。また、暗号技術の安全な利用方法に関する調査や新世代の暗号に関する調査も行う。

暗号技術調査ワーキンググループ(以下、「調査 WG」という。)は、評価委員会の下に設置され、NICT と IPA が共同で運営する。調査 WG は、評価委員会の指示のもと、評価委員会活動に必要な項目について調査・検討活動を担当する作業グループである。評価委員会の委員長は、実施する調査・検討項目に適する主査及びメンバーを選出し、調査・検討活動を指示する。主査は、その調査・検討結果を評価委員会に報告する。2017 年度において、評価委員会の指示に基づき実施される調査項目は、暗号技術調査ワーキンググループ(暗号解析評価)(以下、「暗号解析評価 WG」という。)にて検討される。

評価委員会と連携して活動する「暗号技術活用委員会」も、評価委員会と同様、暗号技術検討会の下に設置され、NICT と IPA が共同で運営している。



※ 今年度実施されている調査項目:

- 耐量子計算機暗号技術に関する調査
- 素因数分解問題及び楕円曲線上の離散対数問題の困難性に関する計算量の評価

図 0-1:CRYPTREC 体制図

委員名簿

暗号技術評価委員会

委員長	太田 和夫	電気通信大学 教授
委員	岩田 哲	名古屋大学 准教授
委員	上原 哲太郎	立命館大学 教授
委員	金子 敏信	東京理科大学 教授
委員	高木 剛	東京大学 教授
委員	手塚 悟	慶應義塾大学 特任教授
委員	本間 尚文	東北大学 教授
委員	松本 勉	横浜国立大学 教授
委員	松本 泰	セコム株式会社 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 研究室長
委員	山村 明弘	秋田大学 教授
委員	渡邊 創	国立研究開発法人産業技術総合研究所 研究企画室長

暗号技術調査ワーキンググループ(暗号解析評価)

主査	高木 剛	東京大学 教授
委員	青木 和麻呂	日本電信電話株式会社 グループリーダ
委員	草川 恵太	日本電信電話株式会社 研究主任
委員	國廣 昇	東京大学 准教授
委員	下山 武司	株式会社富士通研究所 主管研究員
委員	高島 克幸	三菱電機株式会社 主席技師長
委員	安田 貴徳	岡山理科大学 准教授
委員	安田 雅哉	九州大学 准教授

オブザーバー

内田 稔	内閣官房内閣サイバーセキュリティセンター
久保山 拓	内閣官房内閣サイバーセキュリティセンター
高木 浩光	内閣官房内閣サイバーセキュリティセンター
眞弓 隆浩	内閣官房内閣サイバーセキュリティセンター
岡田 崇志	個人情報保護委員会事務局
中嶋 昌幸	警察庁 情報通信局
廣田 亮	総務省 行政管理局[2017 年 7 月まで]
小高 久義	総務省 行政管理局
三輪 亮介	総務省 自治行政局 住民制度課
上東 孝旭	総務省 情報流通行政局
丸橋 弘人	総務省 情報流通行政局[2017 年 7 月まで]
守屋 潤一	総務省 情報流通行政局
今野 孝紀	総務省 情報流通行政局[2017 年 7 月まで]
本原 拓也	外務省 大臣官房
加藤 誠司	経済産業省 産業技術環境局[2017 年 6 月まで]
三島 崇	経済産業省 産業技術環境局[2017 年 7 月から]
稲垣 良一	経済産業省 商務情報政策局[2017 年 7 月から]
森川 淳	経済産業省 商務情報政策局
松本 裕悟	防衛省 整備計画局[2018 年 2 月まで]
今泉 隆文	防衛省 整備計画局
相原 大輔	警察大学校
滝澤 修	国立研究開発法人情報通信研究機構
花岡 悟一郎	国立研究開発法人産業技術総合研究所

事務局

国立研究開発法人情報通信研究機構 （宮崎哲弥、盛合志帆、大久保美也子、篠原直行、黒川貴司、金森祥子、野島良、吉田真紀、青野良範、笠井祥、大川晋司）
独立行政法人情報処理推進機構（江口純一、時田俊雄、小暮淳、神田雅透、稲垣詔喬[2017 年 4 月まで]、橋本徹[2017 年 5 月から]、兼城麻子）

第１章　活動の目的

1.1 電子政府システムの安全性確保

電子政府、電子自治体及び重要インフラにおける情報セキュリティ対策は根幹において暗号アルゴリズムの安全性に依存している。情報セキュリティ確保のためにはネットワークセキュリティ、通信プロトコルの安全性、機械装置の物理的な安全性、セキュリティポリシー構築、個人認証システムの脆弱性、運用管理方法の不備を利用するソーシャルエンジニアリングへの対応と幅広く対処する必要があるが、暗号技術は情報システム及び情報通信ネットワークにおける基盤技術であり、暗号アルゴリズムの安全性を確立することなしに情報セキュリティ対策は成り立たない。現在、様々な暗号技術が開発され、それを組み込んだ多くの製品・ソフトウェアかが市場に提供されているかが、暗号技術を電子政府システム等で利用していくためには、暗号技術の適正な評価が行われ、その情報が容易に入手できることが極めて重要となる。

CRYPTREC では、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」[1] 等に記載された暗号アルゴリズムを対象とする調査・検討を行う活動を行ってきた。たとえば、2005 年度に実施されたハッシュ関数の安全性評価に基づき、2006 年 6 月に SHA-1 の安全性に関する見解を、2006 年度に実施された素因数分解問題の困難性に関する評価に基づき、RSA1024 の安全性の評価結果をそれぞれ公表した。これらの見解に基づき、情報セキュリティ政策会議において「政府機関の情報システムにおいて使用される暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」[2] が 2008 年度に決定されるに至った。また、CRYPTREC 暗号リスト策定中に実施した安全性評価において、128-bit key RC4 の脆弱性を利用した攻撃が現実的になる場合が指摘されたことから、128-bit key RC4 は SHA-1 とともに CRYPTREC 暗号リストの運用監視暗号リストに記載されることになった。現在、暗号技術評価委員会では、暗号技術に関する安全性について重要な指摘があった場合、CRYPTREC の Web サイト上に注意喚起レポートを掲載する活動を実施している。たとえば、最近では、2017 年 2 月には SHA-1 の衝突が初めて計算されたことから、「SHA-1 の安全性低下について」[3]を Web 掲載した。

暗号技術に対する解析・攻撃技術の高度化が日夜進展している状況にあることから、今後とも、CRYPTREC によって発信される情報を踏まえて、関係各機関が連携して情報システム及び情報通信ネットワークをより安全なものにしていくための取り組みを実施していくことが非常に重要である。また、過去 18 年間に渡って実施してきた暗号技術の安全性及び信頼性確保のための活動は、最新の暗号研究に関する情報収集・分析に基づいており、引き続き、暗号技術に係る研究者等の多くの関係者の協力が必要不可欠である。

---

[1] http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2016.pdf

[2] http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf (2008 年 4 月 22 日決定情報セキュリティ政策会議決定)

[3] http://www.cryptrec.go.jp/topics/cryptrec_20170301_sha1_cryptanalysis.html

1.2 暗号技術評価委員会

電子政府システムにおいて利用可能な暗号アルゴリズムを評価・選択する活動が2000年度から2002年度まで暗号技術評価委員会において実施された。その結論を考慮して電子政府推奨暗号リスト[4]が総務省・経済産業省において決定された。

電子政府システムの安全性を確保するためには電子政府推奨暗号リストに掲載されている暗号の安全性を常に把握し、安全性を脅かす事態を予見することが重要課題となった。

そのため、2007年度に電子政府推奨暗号の安全性に関する継続的な評価、電子政府推奨暗号リストの改訂に関する調査・検討を行うことが重要であるとの認識の下に、暗号技術評価委員会が発展的に改組され、暗号技術検討会の下に暗号技術監視委員会が設置された。設置の目的は、電子政府推奨暗号の安全性を把握し、もし電子政府推奨暗号の安全性に問題点を有する疑いが生じた場合には緊急性に応じて必要な対応を行うこと、また、電子政府推奨暗号の監視活動のほかに、暗号理論の最新の研究動向を把握し、電子政府推奨暗号リストの改訂に技術面から支援を行うことである。

2008 年度において、暗号技術監視委員会では、「電子政府推奨暗号リストの改訂に関する骨子(案)」及び「電子政府推奨暗号リスト改訂のための暗号技術公募要項(2009 年度)(案)」を策定したが、2009 年度からは次期リスト策定のために新しい体制に移行し、名称を「暗号方式委員会」と変更した。電子政府推奨暗号リスト改訂のための暗号技術公募(2009 年度)を受けて、2010 年度からは応募された暗号技術などの安全性評価を開始し、2012 年度に「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」[5](付録 1)を策定した。その概要については、CRYPTREC Report 2012 を参照のこと。

2013 年度からは、名称を「暗号方式委員会」から「暗号技術評価委員会」と変更し、暗号技術の安全性に係る監視・評価及び実装に係る技術(暗号モジュールに対する攻撃とその対策も含む)の監視・評価を実施することになった。引き続き、暗号技術評価委員会では、その下に暗号技術調査ワーキンググループを設置し、暗号技術に関する具体的な検討を行っている。2013 年度から 2016 年度まで、暗号技術調査ワーキンググループ（軽量暗号）が設置され、活動の成果として、軽量暗号の利用促進をはかることを目的とする「CRYPTREC 暗号技術ガイドライン（軽量暗号)」[6]が作成された。また、2013 年度からは、暗号技術調査ワーキンググループ（暗号解析評価）が設置されている。詳細については、第 3 章を参照のこと。

1.3 CRYPTREC 暗号リスト

2000年度から2002年度のCRYPTRECプロジェクトの集大成として、暗号技術評価委員会で作成された「電子政府推奨暗号リスト（案)」は、2002年度に暗号技術検討会に提出され、

[4] http://www.cryptrec.go.jp/list_2003.html
[5] http://www.cryptrec.go.jp/list.html
[6] http://www.cryptrec.go.jp/report/cryptrec-gl-0001-2016-j.pdf

同検討会での審議ならびに（総務省・経済産業省による）パブリックコメント募集を経て、「電子政府推奨暗号リスト」として決定された。そして、「各府省の情報システム調達における暗号の利用方針（平成15年2月28日、行政情報システム関係課長連絡会議了承)」において、可能な限り、「電子政府推奨暗号リスト」に掲載された暗号の利用を推進するものとされた。

電子政府推奨暗号リストの技術的な裏付けについては、CRYPTREC Report 2002 暗号技術評価報告書（平成14年度版）に詳しく記載されている。CRYPTREC Report 2002 暗号技術評価報告書（平成14年度版）は、次のURLから入手できる。

http://www.cryptrec.go.jp/report.html

2009 年度には、2008 年度に検討した「電子政府推奨暗号リスト改訂のための暗号技術公募要項（2009 年度)」に基づき、電子政府推奨暗号リスト改訂のための暗号技術公募が行われた。2010 年度から 2012 年度にかけて、暗号方式委員会、暗号実装委員会及び暗号運用委員会にて評価が行われ、2012 年度に暗号技術検討会にて電子政府推奨暗号リストの改定が行われた。最終的に、総務省及び経済産業省がパブリックコメント[7]を行い、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト)」が決定された。
選定方法及びその結果については、CRYPTREC Report 2012(暗号技術評価委員会報告)に記載されている。

1.4 活動の方針

暗号技術評価委員会では、主に、暗号技術の安全性評価を中心とした技術的な検討、すなわち、

(a) 暗号技術の安全性及び実装に係る監視及び評価
(b) 新世代暗号に係る調査(軽量暗号、セキュリティパラメータ、ペアリング暗号、耐量子計算機暗号技術等)
(c) 暗号技術の安全な利用方法に関する調査(暗号技術ガイドラインの整備、学術的な安全性の調査・公表等)

を実施する。

監視に関する基本的な考え方は、CRYPTREC Report 2012 までに記載されていた電子政府推奨暗号リスト[8]掲載の暗号技術に対する考え方[9]と基本的に同じである。つまり、暗号技術の安全性及び実装に係る監視及び評価とは、研究集会、国際会議、研究論文誌、インターネット上の情報等を監視すること（情報収集）、CRYPTREC 暗号リストに掲載されている暗号技術の安全性に関する情報を分析し、それを暗号技術評価委員会に報告すること（情報分析)、安全性等において問題が認められた場合、暗号技術評価委員会において内容を審議し、評価結果を決定すること（審議及び決定)、の 3 つの段階からなる。また、仕様書の参照先

[7] http://www.cryptrec.go.jp/topics/cryptrec_201212_listpc.html
[8] 2003 年 2 月 20 日に策定されたものを指す。
[9] たとえば、暗号技術検討会 2008 年度報告書を参照のこと。
http://www.cryptrec.go.jp/report/c08_kentou_final.pdf

の変更を検討する際にも、監視に関する基本的な考え方を参考にしている。図 1-1 に電子政府推奨暗号の削除等の手順を示す。

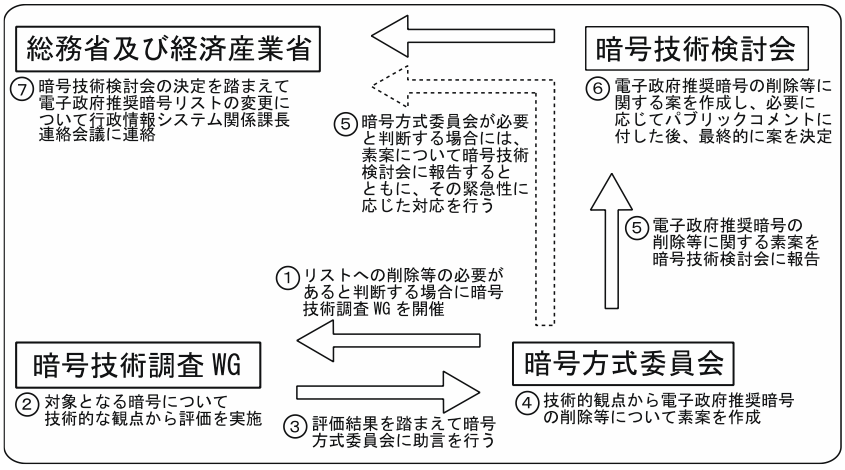


図1-1: 電子政府推奨暗号の削除等の手順[10]

(1) 実運用環境において安全性に問題が認められた電子政府推奨暗号は原則としてリストから削除する。
(2) 電子政府推奨暗号の仕様変更は認めない。
(3) 電子政府推奨暗号の仕様変更に到らないパラメータの修正等の簡易な修正を行うことにより当該暗号の安全性が維持される場合には、修正情報を周知して当該暗号をリストに残す。

また、暗号アルゴリズムの脆弱性に関する CRYPTREC からの情報発信については、下記に示すフローチャート(図 1-2)に基づいて取り扱うことが 2015 年度の暗号技術検討会にて承認されている。

[情報発信フローの概要]

（1） 暗号アルゴリズムの脆弱性情報を検知した後、CRYPTREC において参照している仕様に対する攻撃成功に関する情報か、もしくは攻撃成功までは到達していないが攻撃に必要となる計算量の著しい低下につながる結果であるか否かについて判断をし、以下のいずれに属する情報であるかを分類する。

A) 暗号アルゴリズムの完全な危殆化による緊急対応
B) 正確で信頼性の高い情報を発信することによる過剰反応防止
C) 長期的なシステムの安全性維持のための対策喚起
D) 対応不要

[10] 表中の「暗号方式委員会」は適宜、暗号技術評価委員会と読み替える。

（２）　上記の分類のうち、A)もしくは B)に分類される脆弱性情報については、速報を公開し、また、安全性評価を実施し、その評価結果を公開する。C)に分類される脆弱性情報については、必要に応じて C)に分類された情報であることの公表や安全性評価を実施する。ここで、速報とは、外部で公開されている情報に基づき記載するもので、CRYPTREC では自ら詳細評価は行っていないが、信頼に足る機関・組織等から得た情報に基づくものとする。また、安全性評価報告とは、CRYPTREC として安全性評価を実施しその評価結果をまとめたものとする。

（３）　取り扱う暗号アルゴリズムの範囲は、CRYPTREC 暗号リストに掲載されている暗号技術、および CRYPTREC 暗号リストに掲載されていないが、影響度が高いと暗号技術評価委員会で認められた暗号技術を対象とする。

（４）　速報および安全性評価結果は暗号技術評価委員会の審議に基づき公開される。また、これら脆弱性情報は、暗号技術評価委員会から暗号技術検討会に報告される。

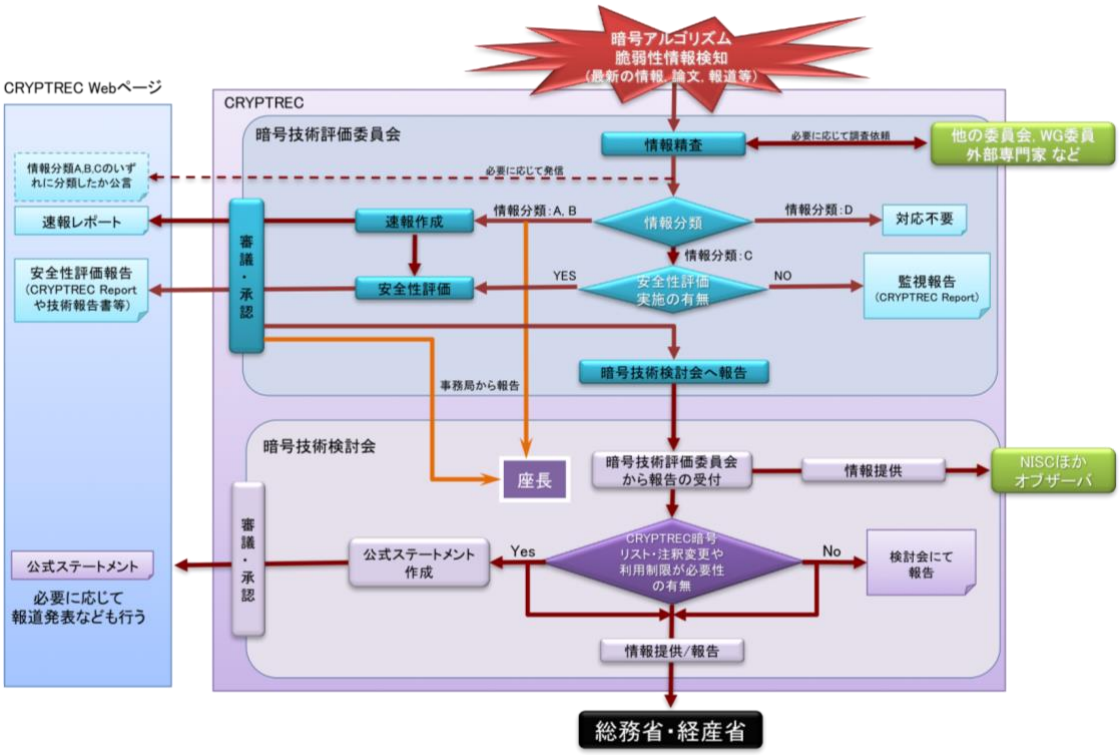


図1-2：暗号アルゴリズムの脆弱性に関する情報発信フロー

第２章　委員会の活動

2.1. 監視活動報告

電子政府推奨暗号の 3-key Triple DES に関して、米国 NIST が 2017 年 11 月に SP 800-67 を更新し[1]、同一の鍵を用いて暗号化できる最大ブロック数を 2^{32} ブロックから 2^{20} ブロックに下げたほか、今後、TLS や IPsec での利用を許容しない方針を打ち出したことから、CRYPTREC 暗号リストにおける今後の利用方針について審議をした。これについては、2.2. 節を参照のこと。

3-key Triple DES 以外の電子政府推奨暗号の安全性評価について 2017 年度の報告時点では収集した全ての情報が引き続き「情報収集」、「情報分析」フェーズに留まり、「審議及び決定」には至らず、電子政府推奨暗号の安全性に懸念を持たせるような事態は生じていないと判断した。以降、収集、分析した主たる情報について報告する。

2.1.1. 共通鍵暗号に関する安全性評価について

CRYPTREC 暗号リスト掲載の共通鍵暗号については、128 ビットブロック暗号 AES に対して Eurocrypt 2017 や Asiacrypt 2017 において新たな識別子（distinguisher）が発表された。また 128 ビットブロック暗号 CLEFIA についても Asiacrypt 2017 において新たな識別子が発表され Integral 攻撃による攻撃可能段数が 1 段進展した。以上のように 2017 年度は共通鍵暗号（特にブロック暗号）において着実な攻撃（安全性評価）の進展はあったものの、いずれもフルスペックまでの攻撃の報告はなかった。

一方、2016 年度の ACM CCS 2016 にて、64 ビットブロック暗号を、鍵を変えずに 2^{32} ブロック以上暗号化した場合の脅威（いわゆる Sweet32）の報告を受け、IETF 等の標準化機関や主要なブラウザで、SSL/TLS における 64 ビットブロック暗号の優先順位を下げる、或いは、同じ鍵で暗号化できるデータ量を制限するなどの対策が取られてきた流れの中で、米国 NIST が 2017 年 11 月に TDEA（Triple DES）に関する文書 SP 800-67 を Revision 2 に更新し、TDEA（Triple DES）で同一の鍵を用いて暗号化できる最大ブロック数を 2^{32} ブロックから 2^{20} ブロックに下げるという動きがあった。

2.1.2. 公開鍵暗号に関する安全性評価について

公開鍵暗号の安全性の根拠とする数学的問題に関しては、離散対数問題(DLP: Discrete Logarithm Problem)の解読法に引き続き進展が見られた。

Eurocrypt 2017 において Thorsten Kleinjung 氏らは 768 ビット素体上の DLP 解読実験に成功したと発表した。これまでの素体上の離散対数問題の記録（596 ビットの素体上）から大きく進展した結果であり、素因数分解問題と離散対数問題との解読記録のこれまでの差

[1] https://csrc.nist.gov/publications/detail/sp/800-67/rev-2/final

を大きく縮める結果でもある。計算時間はトータルで約 5,300 コア・年（Intel Xeon E5-2660 2.2GHz）であり、報告者らの大学のクラスタ環境で計算に 2015 年の 5 月から 12 月までをほぼ費やしたとのことである。本件に関し、暗号技術評価委員会は、RSA1024 に係る移行指針と同様に、DSA や DH を利用する場合には、鍵長において、2048 ビット以上の素数位数の有限体を用いることを推奨するという注意喚起を CRYPTREC ホームページ上で行った[2]。

同じく Eurocrypt 2017 において、Joshua Fried 氏らは、SNFS（Special NFS、特殊数体ふるい法）により、1,024 ビットの特殊な素体上での離散対数問題の計算に成功したと報告した。キロビットサイズの素体上の離散対数問題の計算としては世界初の結果である。計算時間はトータルで約 400 コア・年（Intel Xeon E5-2650 2.0GHz）であり、報告者らのクラスタ環境でオープンソース CADO-NFS で実装し、計算に 2 ヵ月程度費やしたとのことである。本計算で用いられた離散対数問題のパラメータ素数 p は DSA のパラメータ推奨に沿って、p-1 がハッシュ値長以下（本報告では 160 ビット）の素因数を持つが、SNFS で離散対数問題が計算可能となるように、約 25 年前に提案された Gordon の方法により、p にトラップドアが仕掛けられているが、今回のパラメータは p を見ただけではトラップドアが仕掛けられていることを見破るのは計算量的に困難なものとなっている。ドアが仕掛けられていることを見破るのは計算量的に困難なものとなっている。DSA や DH を利用する際には、上記のトラップドアを防ぐため、ランダムに生成されたことが検証可能な素数 p を用いるべきである。

2.1.3. ハッシュ関数に関する安全性評価について

CRYPTREC 暗号リスト掲載のハッシュ関数については、SHA-3 ファミリ（またその元となた Keccak）に対して攻撃（安全性評価）に進展が見られた。Eurocrypt 2017 においては衝突攻撃において Keccak-224 の攻撃可能段数の進展（4 段→5 段）、Keccak-256 の従来の攻撃可能段数（4 段）における計算量の削減、SHAKE-128 の 5 段に対する攻撃が初めて報告された。FSE 2018 では現像攻撃において、SHA3-256/SHAKE-256 の従来の攻撃可能段数（3 段）における計算量の削減が報告された。

また、同じく CRYPTREC 暗号リスト（運用監視暗号リスト）掲載のハッシュ関数である RIPEMD-160 に対しても攻撃（安全性評価）に進展が見られた。Eurocrypt 2017 においては、衝突攻撃において 30 段に RIPEMD-160 が攻撃可能であることが初めて報告された。また Semi-Free-start 衝突攻撃において従来の攻撃可能段数（36 段）における計算量の削減が報告された。また FSE 2018 では Semi-Free-start 衝突攻撃において攻撃可能段数の進展（30 段→46 段）が報告された。尚、RIPEMD-160 は仮想通貨で有名なビットコインで利用されているハッシュ関数の一つである。

以上のように 2017 年度はハッシュ関数において着実な攻撃（安全性評価）の進展はあったものの、いずれもフルスペックまでの攻撃の報告はなかった。

[2] http://www.cryptrec.go.jp/topics/cryptrec-er-0001-2017.html

2.1.4. その他の注視すべき技術動向

次世代の暗号技術に関して、量子計算機に対して耐性のある暗号技術標準化の動向が見られる。

NIST による量子計算機に耐性を持つ暗号（PQC：Post-Quantum Cryptography）公募が 2017 年 11 月 30 日に締め切られ、応募暗号の仕様が NIST ホームページ上に公開され、評価が開始された。NIST の PQC 標準化において、応募暗号の安全性・処理性能評価は、これまでの標準ブロック暗号 AES やハッシュ関数 SHA-3 のように、世界中の暗号研究者によりボランティアで行われることが見込まれる。Asiacrypt 2017 における NIST の招待講演では、NIST の PQC 標準化への応募総数は 82 件と発表された。その内訳件数を表 2-1 に示す。

2018 年 4 月 12 日～13 日に米国フロリダ州で第 1 回 PQC 標準化会議が開催され、NIST はこれから 5 年程度かけて、PQC 標準を制定していく予定である。

表 2-1: NIST PQC 標準化への応募暗号

	電子署名	鍵カプセル化／暗号化	合計
格子に基づく暗号技術	4	24	28
符号に基づく暗号技術	5	19	24
多変数多項式に基づく暗号技術	7	6	13
ハッシュ関数に基づく暗号技術	4	0	4
その他	3	10	13
合計	23	59	82

（出典）Dustin Moody（NIST）「The ship has sailed: The NIST Post-Quantum Crypto “competition”」[3]を元に編集

[3] https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/asiacrypt-2017-moody-pqc.pdf

2.2. 3-key Triple DES および 64 ビットブロック暗号の今後の利用について

ACM CCS 2016 にて、64 ビットブロック暗号を、同一の鍵を用いて 2^{32} ブロック以上暗号化した場合の脅威（いわゆる Sweet32）について発表[4,5]があったことを受け、IETF 等の標準化機関や主要なブラウザで、64 ビットブロック暗号の優先順位を下げたり、同じ鍵で暗号化できるデータ量を制限するなどの対策が取られている。また、米国 NIST は、2017 年 11 月に TDEA に関する文書 SP 800-67 を Revision 2 に更新し[6]、TDEA で同一の鍵を用いて暗号化できる最大ブロック数を 2^{32} ブロックから 2^{20} ブロックに下げたほか、今後、TLS や IPsec で TDEA の利用を許容しない(disallow)方針を打ち出した。

なお、64 ビットブロック暗号で同一の鍵を用いて暗号化する場合の最大ブロック数 2^{20} は、Sweet32[5] において HTTPS で secure cookie を導出する攻撃において最初の collision を見つけるのに必要なブロック数から導出されており、NIST SP 800-67 Revision 2[6] で規定されている数字である。また、64 ビットブロック暗号で同一の鍵を用いて CMAC でメッセージ認証コードを生成する場合の最大ブロック数 2^{21} は、同一の MAC が生成される（collision が起きる）確率が 100 万分の 1 以下となるよう導出された数字であり、NIST SP 800-38B[7]においても推奨されている。

これらの動向を受け、CRYPTREC 暗号リストにおける 64 ビットブロック暗号および 3-key Triple DES の今後の利用方針について、暗号技術評価委員会として検討を行った。

2.2.1. 64 ビットブロック暗号について

暗号通信を使わなくても 2^{20} ブロックで使うことが禁止されてしまうという問題はあるが、国際的な標準との整合性を取るため、CRYPTREC 暗号リストの 64 ビットブロック暗号に付与されている注釈について、暗号技術評価委員会では、以下の変更案を暗号技術検討会に提案するという結論になった。

【以前の注釈】 「より長いブロック長の暗号が利用できるのであれば、128 ビットブロック暗号を選択することが望ましい。」

[4] Karthikeyan Bhargavan, Gaëtan Leurent, “On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN”, ACM CCS 2016.
[5] Sweet32: Birthday attacks on 64-bit block ciphers in TLS and OpenVPN, https://sweet32.info/
[6] NIST Special Publication (SP) 800-67, Revision 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Nov 21, 2017.
[7] NIST Special Publication (SP) 800-38B, Recommendation for Block Cipher Modes of Operation: the CMAC Mode for Authentication, May, 2005.

【変更後の注釈】[8]
「CRYPTREC 暗号リストとして使う場合は、64 ビットブロック暗号で同一の鍵を用いて暗号化する場合、最大 2^{20} ブロックまで、同一の鍵を用いて CMAC でメッセージ認証コードを生成する場合、最大 2^{21} ブロックまでとする。」

2.2.2. 3-key Triple DES について

現在、電子政府推奨暗号リストにおいて、3-key Triple DES には下記のように注釈（注 3）が付与されている。

（注 3）3-key Triple DES は、以下の条件を考慮し、当面の利用を認める。
1）NIST SP 800-67 として規定されていること。
2）デファクトスタンダードとしての位置を保っていること。

NIST が 2017 年 11 月に公開した Draft NIST SP 800-52 Revision 2[9]において“The Triple Data Encryption Algorithm (TDEA), also known as 3DES is no longer approved for use with TLS”とし、また、Triple DES の sunset date に関するスケジュールを検討しており、当該注釈（注 3）は現実とそぐわなくなっている。

このような状況を踏まえ、CRYPTREC 暗号リストにおける 3-key Triple DES の扱いについて、暗号技術評価委員会から以下のような意見があった。

- 3-key Triple DES の利用状況を踏まえて運用監視暗号リストへの移行に伴う問題点を確認し、問題がなければ、運用監視暗号リストに移す。
- 運用監視暗号リストに移す際に、現在 3-key Triple DES についている注釈（注 3）は削除する。なお、運用監視暗号リストにおいても、64 ビットブロック暗号の安全な使い方に関する注釈はつける。
- 推奨候補暗号リストに掲載されている 3 つの 64 ビットブロック暗号については、引き続き検討を行い、結論を得るまでは現状維持とする。

暗号技術評価委員会では、運用監視暗号リストへの移行に問題がなければ、3-key Triple DES を運用監視暗号リストに移すことを暗号技術検討会に提案するという結論になった[10]。

[8]（事務局注）：第 1 回暗号技術検討会(2018 年 3 月 29 日開催)での審議の結果、「最大 2^{20} ブロックまで」「最大 2^{21} ブロックまで」がそれぞれ「2^{20} ブロックまで」「2^{21} ブロックまで」と修正された上で承認された。
[9] (DRAFT) NIST Special Publication 800-52 Revision 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Nov, 2017.
[10]（事務局注）：第 1 回暗号技術検討会(2018 年 3 月 29 日開催)での審議の結果、3-key Triple DES は電子政府推奨暗号リストから運用監視暗号リストへの降格が承認され、その注釈(注 3)は削除されることとなった。

2.2.3. MISTY1 について

2015 年に 64 ビットブロック暗号 MISTY1 のフルラウンド攻撃が発表されて以来、対応を検討してきた。現在知られているフルラウンド攻撃には 2^{64} ブロック分の平文・暗号文ペアが必要となっている。

今回、64 ビットブロック暗号に対して付与しようとしている新たな注釈は、MISTY1 についてもこの攻撃を回避する安全な使い方の指針となるため、暗号技術評価委員会では、MISTY1 個別の注釈を追加することは不要という結論になった。

2.3. 注意喚起レポートの発行

2.3.1. 768 ビット素数位数の有限体上の離散対数問題の状況と DSA, DH の今後のパラメータ選択について

位数が 768 ビット長の素数である有限体における離散対数の計算結果を示した論文が、国際暗号学会 (International Association for Cryptologic Research (IACR)) が主催する国際会議 Eurocrypt 2017 で発表され、768 ビットの素体上の離散対数の計算に要する計算コストが、2.2 GHz Xeon E5-2660 プロセッサ換算で、約 5300 コア・年に相当するものと見積もられた。768 ビットの RSA 合成数の素因数分解に要する計算コストは、CRYPTO2010 で発表された論文では、約 1700 コア・年と見積もられているので、これらの計算コストの違いはたかだか数倍程度であるため、暗号技術評価委員会では、RSA1024 に係る移行指針と同様に、今後とも DSA や DH を利用する場合には、鍵長において、2048 ビット以上の素数位数の有限体を用いることを推奨する旨の注意喚起[11]を行った。

2.4. 候補暗号リストへの新規暗号（事務局選出）の追加

2.4.1. ChaCha20-Poly1305 の CRYPTREC 暗号リストへの追加を視野に入れた評価について

ChaCha20-Poly1305 は、ユーザ数の多いブラウザに採用されるなど、実導入が進んでいるアルゴリズムである。2016 度の暗号技術検討会（2017 年 3 月 30 日）にて、CRYPTREC 暗号リストへの追加を視野に入れ、安全性評価・実装性能評価を実施することが承認され、2017 年度第 1 回暗号技術評価委員会（2017 年 7 月 21 日）の承認を受け、安全性評価および実装性能について外部評価を実施した。

(1) 安全性評価結果

ChaCha20-Poly1305 の構成を図 2-1 に示す。暗号化のためにストリーム暗号 ChaCha20 が使われ、認証のためにメッセージ認証コード (MAC) Poly1305 が使われている。

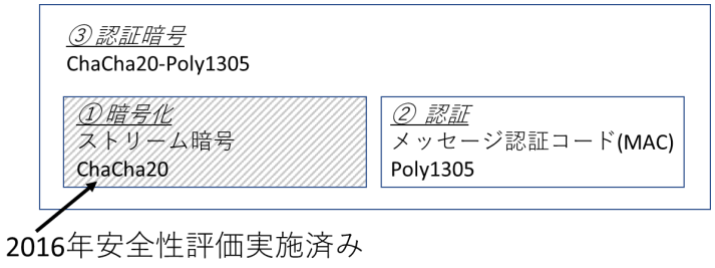


図 2-1 ChaCha20-Poly1305 の構成

[11] http://www.cryptrec.go.jp/topics/cryptrec-er-0001-2017.html

安全性については、以下の条件を満たす場合、認証暗号としての安全性を満たすことが証明されている[12]。

① 暗号化機能の安全性：ChaCha20 を擬似乱数生成器とみなすことができる。

② 認証機能の安全性：Poly1305 が安全なユニバーサルハッシュ関数である。

① 暗号化機能の安全性

2016 年度の評価結果[13]より、既知の様々な攻撃について鍵の総当たりよりも効率的な攻撃が見つからなかったことから、擬似乱数生成器とみなすことができるとの見解を得ている。

② 認証機能の安全性

今年度実施した評価レポートでは、以下の安全性評価について報告されている。

・証明可能安全性：Poly1305 は、ユニバーサルハッシュ関数とみなすことができる。

また、そのほかの安全性解析についても以下の通り報告されている。

表 2-2: Poly1305 の安全性解析結果の概要

攻撃の種類	解析結果
関連鍵攻撃	現実的な脅威とはならない
再偽造可能性	理想的な MAC と同等の安全性を有する
弱鍵	存在したとしても全体の直接的な安全性への影響はない
複数ユーザ安全性	ユーザ数の安全性に対する影響は小さい
ナンス再利用	ハッシュ鍵の導出を容易にする ゆえに、仕様書に沿い、ナンスの再利用は行ってはならない

以上の評価結果から、②の条件を満足し、Poly1305 は十分な安全性を満たすと考えられる。

③ 認証暗号としての安全性

今年度実施した評価レポートでは、以下の安全性評価について報告されている。

・証明可能安全性：①および②の安全性要件を満たし、ChaCha20-Poly1305 は、認証暗号としての安全性を有する。

[12] Gordon Procter. A Security Analysis of the Composition of ChaCha20 and Poly1305, Cryptology ePrint Archive: Report 2014/613, 2014. (https://eprint.iacr.org/2014/613).

[13] CRYPTREC 技術報告書 No.2601「Security Analysis of ChaCha20-Poly1305 AEAD」参照

また、以下の安全性解析についても報告されている。

表 2-3: ChaCha20-Poly1305 の安全性解析結果の概要

攻撃の種類	解析結果
関連鍵攻撃	ChaCha20 が①を満たす条件の下で安全性証明が可能である
弱鍵	存在しても現実的な脅威とはならない
複数ユーザ安全性	ユーザ数の安全性に対する影響は小さい
復号ミスユース	暗号化に関する安全性は満たさないが、認証に関する安全性は満たす
ナンス再利用	再利用されたナンスを伴う出力については偽造可能となる ゆえに、仕様書に沿い、ナンスの再利用は行ってはならない
再偽造可能性	ナンスを再利用しない限り理想的な認証暗号と同等の安全性をもつが、ナンスを再利用した場合、偽造可能となる ゆえに、仕様書に沿い、ナンスの再利用は行ってはならない

以上の評価結果から、ChaCha20-Poly1305 は、十分な安全性を満たすと考えられる。

(2) 実装性能評価結果

認証暗号として、AES-GCM は広く知られている一方、AES 計算のための拡張命令(ハードウェアによる AES アクセラレーション)が利用できない組み込みデバイスなどの CPU などで、計算コストが小さく、処理速度の速い認証暗号として ChaCha20-Poly1305 が注目されている。ChaCha20-Poly1305 は、AES-GCM と比べ、ソフトウェア実装に向いていると言われており、TLS 1.3 では実装することが必須のアルゴリズムとなっている。

評価レポートの結果から、ChaCha20-Poly1305 は、特に、組み込み機器や低電力アプリケーション向けの CPU で優位性があることが確認できた。一例として、世界中で広く利用されている OpenSSL を用いた実測による Linux 上での性能比較結果(暗号化処理速度)を図 2-2 に示す。AES-GCM と比較評価し、AES 計算のための拡張命令(ハードウェアによる AES アクセラレーション)を用いない環境で、ChaCha20-Poly1305 (鍵長 256 ビット)は約 2.86～4.46 倍の処理速度をもち、優位性があることがわかる。このように AES 計算のための拡張命令(ハードウェアによる AES アクセラレーション)を利用できない環境で、ChaCha20-Poly1305 は AES-GCM と比較し、実装性能が優れている。

なお、ハードウェア実装評価は実施していないが、主たる利用が TLS や組み込みデバイスなどのソフトウェアでの実装となることも考慮し、十分な実装性能を有すると考えられる。

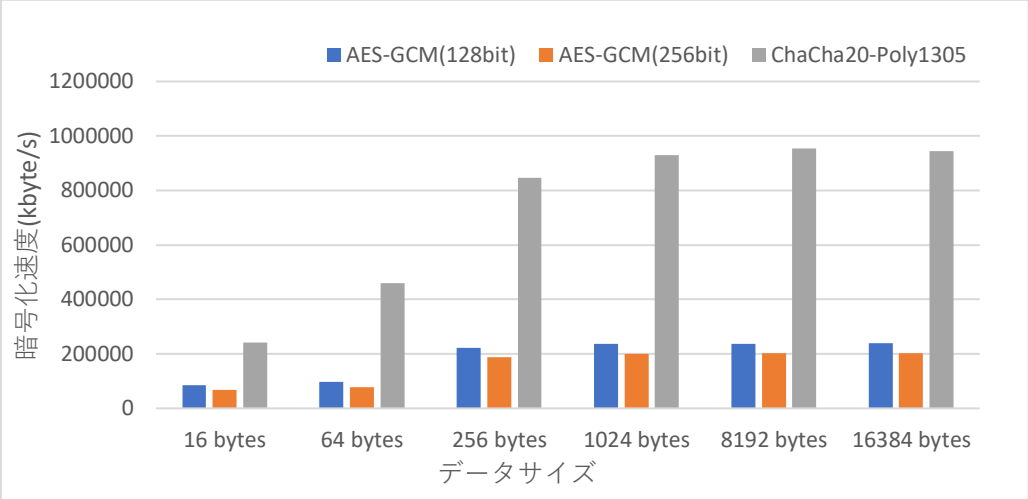


図 2-2：Linux における認証付き暗号の性能評価(2017 度実施した評価レポートより抜粋)

(3) 暗号技術評価委員会での審議結果

以上の調査および評価結果に基づき、暗号技術評価委員会では、実装性能について、CRYPTREC 暗号リストに掲載するために十分な実装性能を有していると判断し、CRYPTREC 暗号リストへの追加を暗号技術検討会へ提案することが決まった。また、CRYPTREC 暗号リストの技術分類(大分類)として認証暗号のカテゴリを新設し、そこに ChaCha20-Poly1305 を位置付ける案を暗号技術検討会に諮ることが決まった[14]。

[14] (事務局注)： 第 1 回暗号技術検討会(2018 年 3 月 29 日開催)での審議の結果、技術分類「認証暗号」の新設が承認され、技術分類「認証付き秘匿モード」に対して、「CRYPTREC 暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせても、「認証暗号」として使うことができる。」という注釈を付けることとなった。

2.5. 暗号技術の安全な利用方法に関する調査

2.5.1. 「暗号技術ガイドライン(SHA-1)」の改定について

一般に、暗号学的ハッシュ関数には、衝突発見困難性、第二原像計算困難性及び原像計算困難性の 3 つの安全性要件を満たすことが求められるが、2017 年に SHA-1 は衝突発見困難性を満たしていないことが発表された。SHA-1 は、暗号技術の補助関数としてさまざまな部分で利用されており、CRYPTREC 暗号リストの多くの暗号技術において採用されている。その中には、衝突発見が安全性に直接的に影響を与えるものと与えないものが存在している。

現状、実運用環境においては SHA-1 の継続利用を避けることが互換性維持の観点から現実的な選択肢ではない場面も想定されるため、CRYPTREC 暗号リストの電子政府推奨暗号リストにおいて補助関数として SHA-1 を用いる場合(ただし、擬似乱数生成系を除く)に、互換性維持の目的であれば継続利用が容認されるかどうかの指針を暗号技術評価委員会で決定した(表 2-4)。詳しくは、「CRYPTREC 暗号技術ガイドライン(SHA-1)改定版」[15]を参照のこと。

表2-4: CRYPTREC 暗号リストにおいてSHA-1 を補助関数として用いる
電子政府推奨暗号の継続利用の指針

<table>
<tr><th>技術分類</th><th>SHA-1 を補助関数
として用いる暗号名称</th><th>継続利用の指針</th></tr>
<tr><td rowspan="2">署名</td><td rowspan="2">DSA,
ECDSA,
RSASSA-PKCS1-v1_5,
RSA-PSS</td><td>署名生成については、
電子政府推奨暗号リストに記載された
ハッシュ関数への移行を推奨</td></tr>
<tr><td>署名検証については、
互換性維持目的※での継続利用は容認</td></tr>
<tr><td>守秘</td><td>RSA-OAEP</td><td rowspan="4">互換性維持目的での継続利用は容認</td></tr>
<tr><td>鍵共有</td><td>DH,
ECDH</td></tr>
<tr><td>メッセージ認証コード</td><td>HMAC</td></tr>
<tr><td>エンティティ認証</td><td>ISO/IEC 9798-3</td></tr>
</table>

※ 電子政府推奨暗号リストに記載されたハッシュ関数への移行が困難な場合や SHA-1 の継続利用を停止すると、より大きなセキュリティ上の懸念が生じうる場合を想定している。また、ここで述べる互換性維持には該当しないが、後述する長期署名における過去の SHA-1 による署名検証も容認される。

[15] http://www.cryptrec.go.jp/report/cryptrec-gl-2001-2013r1.pdf または、付録 6 を参照

2.6. 学会等参加状況

国内外の学術会議に参加し、暗号解読技術に関する情報収集を実施した。参加した国際会議は、表2-5 に示す通りである。

表 2-5: 国際会議への参加状況

学会名・会議名		開催国・都市	期間
Eurocrypt 2017	International Conference on the Theory and Applications of Cryptographic Techniques	フランス・パリ	2017年4月30日～2017年5月4日
PQCrypto 2017	Post-Quantum Cryptography	オランダ・ユトレヒト	2017年6月26日～2017年6月28日
ACNS 2017	International Conference on Applied Cryptography and Network Security	日本・金沢	2017年7月10日～2017年7月12日
Crypto 2017	International Cryptology Conference	アメリカ・サンタバーバラ	2017年8月20日～2017年8月24日
FDTC 2017	Workshop on Fault Diagnosis and Tolerance in Cryptography	台湾・台北	2017年9月25日
CHES 2017	Conference on Cryptographic Hardware and Embedded Systems	台湾・台北	2017年9月26 日～2017年9月28日
PROOFS 2017	Security Proofs for Embedded Systems	台湾・台北	2017年9月28日
ACM CCS 2017	ACM Conference on Computer and Communications Security	アメリカ・ダラス	2017 年 10 月 31 日～11 月 2 日
Asiacrypt 2017	International Conference on the Theory and Application of Cryptology and Information Security	中国・香港	2017 年 12 月 3 日～2017 年 12 月 7 日
FSE 2018	International Conference on Fast Software Encryption	ベルギー・ブルッヘ	2018年3月5 日～2018年3月7日

以下に、国際学会等に発表された論文を中心に、暗号解読技術の最新動向を示す。詳しくは、付録 7 を参照のこと。

2.6.1. 共通鍵暗号の解読技術

・A New Structual-Differential Property of 5-Round AES [Eurocrypt 2017]

Lorenzo Grassi, Christian Rechberger, Sondre Ronjom

米国標準ブロック暗号 AES(2000 年制定)の 5 段の識別子を示した。これまでは AES の識別子は 4 段のものは知られていたが 5 段のものは初めてであり、AES の解読可能な段数が進展した。ただし、128 ビット鍵の AES のフルスペックの段数は 10 段であり、今回の結果は AES の安全性に直ちに影響を与えるものではない。

・Automatic Search of Bit-Based Division Property for ARX Ciphers and Word-Based Division Property [Asiacrypt 2017]

Ling Sun, Wei Wang, Meiqin Wang

Division property を自動的に発見するツールを開発し、いくつかの暗号に適用し、これまでの記録を凌ぐ結果を得た。ARX 暗号に対しては、SAT 問題に基づき、ビットレベルの性質伝搬を追跡することにより、SHACAL-2 の 17 段識別(4 段増)および LEA の 8 段識別(1 段増)を構成した。ワードベースの division property に関しては、SMT 問題に基づくことにより、CLEFIA の 10 段識別(1 段増)を構成し、Whirlpool の 4/5 段識別のデータ計算量を改良し、Rijndael-192/256 の 6 段識別(2 段増)を示した。CLEFIA については、新しい識別により integral 攻撃を 1 段改良した。

・Yoyo Tricks with AES [Asiacrypt 2017]

Sondre Rønjom, Navid Ghaedi Bardeh, Tor Helleseth

SPN の新しい基本的性質を導入し、適応的選択暗号文/平文の設定において、3 段から 5 段の AES に対する鍵に依存しないヨーヨー識別を初めて構成した。これまでのすべての記録を更新し、必要なデータは各々3, 4, $2^{25.8}$ であり、差分を観測する以外には本質的に計算を必要としない。更に、6 段 AES に対する初めての鍵独立な識別を、平文および暗号文における不可能ゼロ差分を保つヨーヨー・ゲームに基づいて構成した。データ量は $2^{122.83}$ の平文/暗号文ペアを必要とし現実的ではないが、対応する差分を観測する以外は本質的な計算は必要としない。また、5 段 AES に対して、$2^{11.3}$ のデータおよび 2^{31} の計算量しか必要としない鍵回復攻撃を示した。

2.6.2. 公開鍵関数の解読技術

・Computation of a 768-Bit Prime Field Discrete Logarithm [Eurocrypt 2017]

Thorsten Kleinjung, Claus Diem, Arjen K. Lenstra, Christine Priplata, Colin Stahlke

NFS（数体ふるい法）により 768 ビットの素体上の離散対数問題の計算に成功したという報告であり、これまでの素体上の離散対数問題の記録（596 ビットの素体上）から大きく進展した。計算時間はトータルで約 5300 コア・年（Intel Xeon E5-2660 2.2GHz)。報告者ら

の大学のクラスタ環境で計算に 2015 年の 5 月から 12 月迄をほぼ費やしたとのこと。この研究成果は、素体上の離散対数問題の困難さに安全性の根拠を置く公開鍵暗号に対する既存の安全性評価結果に大きな進展と新たな知見を与えるものである。一方、CRYPTREC 暗号リスト掲載の公開鍵暗号で素体上の離散対数問題の困難さに安全性の根拠を置くものとして、署名の DSA と鍵共有の DH が該当するが、素数のサイズが 2048 ビット以上であれば本報告の結果は直ちにその安全性に影響を与えるものではない。

・A Kilobit Hidden SNFS Discrete Logarithm Computation [Eurocrypt 2017]

Joshua Fried, Pierrick Gaudry, Nadia Heninger, Emmanuel Thome

SNFS（特殊数体ふるい法）により、1024 ビットの特殊な素体上での離散対数問題の計算に成功したという報告で、キロビットサイズの素体上の離散対数問題の計算としては世界初。計算時間はトータルで約 400 コア・年（Intel Xeon E5-2650 2.0GHz)。報告者らのクラスタ環境でオープンソース CADO-NFS で実装し、計算に 2 ケ月ほど費やしたとのこと。素数 p は DSA のパラメータ推奨に沿って、p-1 がハッシュ値長以下（本報告では 160 ビット）の素因数を持つが、p に SNFS で離散対数問題が計算可能となるように、約 25 年前に提案された Gordon の方法により、p にトラップドアが仕掛けられている。提案当時は比較的小さな（トラップドアを持つ）パラメータしか生成できなかったが、その後の計算機の進歩により、今回のパラメータは十分な大きさを持ち、p を見ただけではトラップドアが仕掛けられていることを見破るのは計算量的に困難なものとなっている。署名の DSA、鍵共有の DH を用いる際には、上記のトラップドアを持たないパラメータを利用する必要があるが、上述のように p を見ただけではトラップドアが仕掛けられているか否かを見分けることは困難である。本トラップドアを防ぐには、ランダムに生成されたことが検証可能な素数 p を用いる必要がある。

・The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli [ACM CCS 2017]

Matus Nemec, Marek Sys and Petr Svenda, Dusan Klinec, Vashek Matyas

本論文は、Coppersmith の提案した攻撃手法を応用し、特に RSALib が提供する RSA モジュールに適用されていると思われる設定状況に対して、効果的な攻撃が行えることを示した。この論文の解析が成功した要因としては、ある特定の生成式に基づき鍵生成が行われていた(と想定される)こと、そのことにより式変形により、仮想的な等価式を用いて全数探索が可能であるほどの小さなパラメータを用いた解析が可能になってしまったことが考えられる。著者らは、公開情報のみを用いて、特に追加的な前提条件を設けることなく、Coppersmith の攻撃を適用することにより、探索・推定を可能とした。また、RSA モジュールが今回の解析が適用可能か否かをチェックできるツールをフリーで公開している。解析の対処策としては、別のライブラリを用いて生成した鍵のインポート，より影響の少ない

鍵長(例として 3072 ビットを挙げていた)への変更、リスクマネージメントの強化などを挙げている。

2.6.3. ハッシュ関数の解読技術

・Conditional Cube Attack on Reduced-Round Keccak Sponge Function [Eurocrypt 2017]

Senyang Huang, Xiaoyun Wang, Guangwu Xu, Meiqin Wang, Jingyuan Zhao

米国標準ハッシュ関数 SHA-3(2015 年制定)の元となったハッシュ関数 Keccak について条件付きキューブ攻撃を提案した。Keccak-MAC へのキーリカバリー攻撃で、Keccak-MAC-256/384/512 について 7/6/5 段の結果を初めて示し、Keccak-MAC-128 については計算量とデータ量を削減した。また、Keyak (Keccak sponge function ベースの AE) へのキーリカバリー攻撃で、Keyak-128 について 8 段の結果を初めて示し、7 段については計算量とデータ量を削減した。更に、Keccak sponge function への識別攻撃で、Keccak-384/512 について 7/6 段に結果を初めて示し、Keccak-224 については従来の攻撃可能段数 (7 段) で計算量とデータ量を削減した。ただし、(b=1600 の) Keccak/SHA-3 のフルスペックの段数は 24 段であり、Keccak/SHA-3 の安全性に直ちに影響を与えるものではない。

・New Collision Attacks on Round-Reduced Keccak [Eurocrypt 2017]

Kexin Qiao, Ling Song, Meicheng Liu, Jian Guo

米国標準ハッシュ関数 SHA-3(2015 年制定)の元となったハッシュ関数 Keccak に対する新たな衝突攻撃を提案した。Keccak-224 の攻撃可能段数を従来の 4 段から 5 段に伸ばした。また、Keccak-256 の従来の攻撃可能段数 (4 段) での解読計算量を削減した。また、SHA3 ファミリーの一つである SHAKE128 の 5 段に対する攻撃を初めて示した。ただし、(b=1600 の) Keccak/SHA-3 のフルスペックの段数は 24 段であり、Keccak/SHA-3 の安全性に直ちに影響を与えるものではない。

・Collisions and Semi-Free-Start Collisions for Round-Reduced RIPEMD-160 [Asiacrypt 2017]

FukangLiu, Florian Mendel, Gaoli Wang

RIPEMD-160 に対する衝突攻撃および semi-free-start 衝突攻撃が発表された。Asiacrypt 2013 において Mendel らが未解決問題としていた、RIPEMD-160 の段差分確率を理論的に計算する方法を示し、Mendel らの差分パスを自動的に発見する方法を改良し、30 段 RIPEMD-160 の衝突を 2^{67} の計算量で発見することができる。これは RIPEMD-160 の縮退版に対する初めての衝突攻撃である。更に、ASIACRYPT 2013 の RIPEMD-160 の最初の 36 段に対する semi-free-start 衝突攻撃を改良することにより、計算量を $2^{70.4}$ から $2^{55.1}$ に改良した。

・Cryptanalysis of 48-step RIPEMD-160 [FSE 2018]

Gaoli Wang, Yanzhao Shen, Fukang Liu

『運用監視暗号リスト』に掲載されているハッシュ関数「RIPEMD-160」の「Semi-free-start」衝突（＝攻撃者に有利な特別な条件下での衝突攻撃の一種）で、これまで42ステップまで攻撃可能であったものを、46ステップまで攻撃可能であることが示された。ただし、RIPEMD-160はフルスペックで80ステップあり、今回の発表はRIPEMD-160の安全性に対して直ちに影響のあるものではない。尚、「RIPEMD-160」は仮想通貨で有名なビットコインで利用されているハッシュ関数の一つである。

・Preimage Attacks on the Round-reduced Keccak with Cross-linear Structures [FSE 2018]

Ting Li, Yao Sun, Aaodong Liao, Dingkang Wang

『推奨候補暗号リスト』に掲載されている米国標準ハッシュ関数 SHA-3 ファミリーの「SHA3-256」、「SHAKE-256」への原像攻撃（＝与えられたハッシュ値を出力するメッセージを探索する攻撃）で、これまで3段では共に2^{190}程度の計算量で攻撃可能であったものを、計算量を削減し、2^{151}、2^{153}の計算量で攻撃可能であることが示された。ただし、SHA3-256/SHAKE-256のフルスペックは24段であるため、今回の発表はSHA3-256/SHAKE-256の安全性に対して直ちに影響のあるものではない。

2.7. 委員会開催記録

2017 年度、暗号技術評価委員会は、表 2-6 の通り 2 回開催された。各会合の開催日及び主な議題は以下の通りである。

表 2-6: 暗号技術評価委員会の開催

回	年月日	議題
第 1 回	2017 年 7 月 21 日	・委員会活動計画案の検討 ・ワーキンググループ活動計画案の検討 ・ChaCha20-Poly1305 に関する外部評価の検討 ・SHA-1 に関するガイドラインの改定案の検討 ・64 ビットブロック暗号の今後の利用に関する検討 ・768 ビット素数位数の有限体上の離散対数問題に関する注意喚起文案の検討 ・監視状況の報告
第 2 回	2018 年 2 月 28 日	・ワーキンググループ活動報告 ・3-key Triple DES 及び 64 ビットブロック暗号に関する注釈文案の検討 ・SHA-1 に関するガイドラインの改定案の検討 ・ChaCha20-Poly1305 に関する安全性評価・実装評価結果及びリストへの追加に関する検討 ・監視状況の報告 ・CRYPTREC Report 2017(暗号技術評価委員会報告)目次案の提示

2.8. 暗号技術調査ワーキンググループ開催記録

2017 年度、各暗号技術調査ワーキンググループ（WG）が活動した主要活動項目は、表 2-7 の通りである。表 2-8 の通り、WG は計 2 回開催された。各会合の開催日及び主な議題は以下の通りである。

表 2-7: 2017 年度の主要活動項目

ワーキンググループ名	主査	主要活動項目
暗号解析評価ワーキンググループ	高木 剛	近年、量子計算機が実用化されても安全性を保てると期待される暗号（耐量子計算機暗号:PQC）の調査・検討が各国で進められており、PQC の研究動向を把握する必要性が高まっている。暗号技術評価委員会活動計画における「新技術等に関する調査及び評価」の活動として、PQC の技術動向を調査する。また、素因数分解の困難性や楕円曲線上の離散対数問題の困難性に関しては、例年公表している予測図の更新を行う。

表 2-8: 暗号技術調査ワーキンググループ(暗号解析評価)の開催

回	年月日	議題
第 1 回	2017 年 7 月 27 日	・委員会活動計画の報告 ・ワーキンググループ活動計画案の検討 ・今年度の調査の進め方の検討
第 2 回	2018 年 2 月 21 日	・予測図の更新に関する検討 ・4 つ調査対象（格子に基づく暗号・多変数多項式に基づく暗号・符号に基づく暗号・同種写像に基づく暗号）に関する研究動向 ・ワーキンググループ活動報告案の了承

第３章　暗号技術調査ワーキンググループの活動

3.1. 暗号解析評価ワーキンググループ

3.1.1. 活動目的

(1)　耐量子計算機暗号の研究動向調査

近年、量子計算機が実用化されても安全性を保てると期待される暗号（耐量子計算機暗号：PQC）の調査・検討が各国で進められている。特に米国では NIST が PQC の公募を開始しており、欧州では ETSI が PQC の調査活動を行い、ISO/IEC でも標準化に向けた議論が始まっている。このように国内でも PQC の研究動向を把握する必要性がさらに高まっている。

2017 年度暗号技術評価委員会活動計画における「新技術等に関する調査及び評価」の活動として、PQC の技術動向を調査することが暗号技術検討会において承認された。暗号技術評価委員会では、暗号技術調査ワーキンググループ(暗号解析評価)を設置し、本調査を実施した。

- 耐量子計算機暗号（PQC）に関する近年の研究動向を調査し、報告書を作成する。（完成予定は 2018 年度末。）
- PQC の代表的な候補である、4 つの分類（格子に基づく暗号技術、符号に基づく暗号技術、多変数多項式に基づく暗号技術、同種写像に基づく暗号技術）を調査対象とする。
- 上記の各分類において、該当する方式及び文献について三つの機能（暗号化、鍵交換、署名）の観点による整理等を実施する。

(2) 予想図の更新

素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関して CRYPTREC が例年公表している予測図の更新を行った。

- 素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関する計算量の評価に大幅な変更がないかどうかの確認を行った。
- スーパーコンピュータのベンチマーク結果の 1 位から 500 位を 1993 年から半年毎に集計している Web サイト TOP500[1]における、2017 年 6 月・11 月のベンチマーク結果の追加を行った。

[1] https://www.top500.org/

3.1.2. 委員構成(敬称略、五十音順)

主査：　高木　剛　　東京大学
委員：　青木　和麻呂　日本電信電話株式会社
委員：　草川　恵太　　日本電信電話株式会社
委員：　國廣　昇　　東京大学
委員：　下山　武司　　株式会社富士通研究所
委員：　高島　克幸　　三菱電機株式会社
委員：　安田　貴徳　　岡山理科大学
委員：　安田　雅哉　　九州大学

3.1.3. 活動概要

(1) 耐量子計算機暗号の研究動向調査

- 調査対象とする 4 つの分類項目(下記の①から④)について担当者を決定した。

表 3-1: 担当委員の一覧

	とりまとめ委員	執筆者
導入	高木主査・事務局	高木主査・事務局
①格子に基づく暗号技術	下山委員	下山委員、安田(雅)委員、青野(事務局)
②多変数多項式に基づく暗号技術	安田(貴)委員	安田(貴)委員
③符号に基づく暗号技術	草川委員	草川委員
④同種写像に基づく暗号技術	高島委員	高島委員

- 上記の分類において、NIST の公募に対して提案された暗号技術の概要を調査した。
- NIST における PQC の公募では、締め切り(2017 年 11 月 30 日)までに、82 件の方式が提案され、そのうち 69 件が書類選考を通過している。

表 3-2: 米国 NIST 主催 PQC 標準化の書類選考後の提案数(仮分類)※

分類	署名	暗号化／鍵交換
格子基づく暗号技術	5	21
多変数多項式に基づく暗号技術	9	3
符号基づく暗号技術	3	17
同種写像に基づく暗号技術	0	1
上記以外のもの	5	7

※NIST から正式な発表はなく、WG で検討された仮分類である
†署名・暗号化両方に提案されている 2 件を含む

(2) 予測図の更新

- 2017 年度は、「素因数分解問題の困難性」及び「楕円曲線上の離散対数問題の困難性」に関するグラフの更新を行った。

3.1.4. 成果概要

(1) 耐量子計算機暗号の研究動向調査

- スケジュールの修正について

2018 年度は WG を 3 回開催する予定である。

2017 年度第 2 回 WG（2018 年 2 月） ： 執筆方針案への意見の収集

2018 年度第 1 回 WG（2018 年 6 月） ： 執筆方針の決定

2018 年度第 2 回 WG（2018 年 10 月）： 報告書の中間報告

2018 年度第 3 回 WG（2019 年 2 月） ： 報告書完成

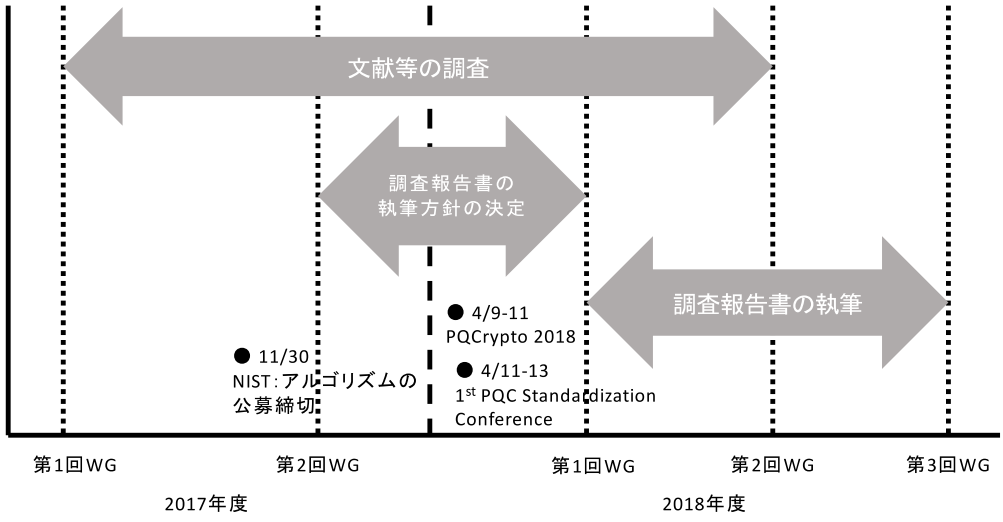


図 3-1: WG のスケジュール

- 執筆方針について

本 WG では執筆方針を決定する上で重要な項目等を集めることを目的とし、執筆方針の決定自体は、主査・とりまとめ委員・事務局によるメール等での協議を経て、2018 年度の第 1 回 WG で正式に決定するものとしたい。また、執筆方針を決定する上で重要な項目等の候補を以下に列挙する：

- 暗号化、署名、鍵交換のいずれに該当するか？
- アルゴリズム
- 暗号パラメータの値

- セキュリティレベルおよびその根拠
- 攻撃手法とその計算量
- 実行する演算（鍵生成/暗号化/復号/符号化/検証 等）に必要な計算時間、及び全ての入力・出力（鍵、暗号文、署名など）のサイズ

(2) 予測図の更新

- 素因数分解問題の困難性および楕円曲線上の離散対数問題の困難性に関する計算量評価に大幅な進展はなかったため、2017 年 6 月・11 月のベンチマーク結果を追加して予測図の更新を行った(図 3-2 及び 3-3)。
- 2018 年度に、一般数体篩法における篩処理の計算量について再評価を行う予定である。

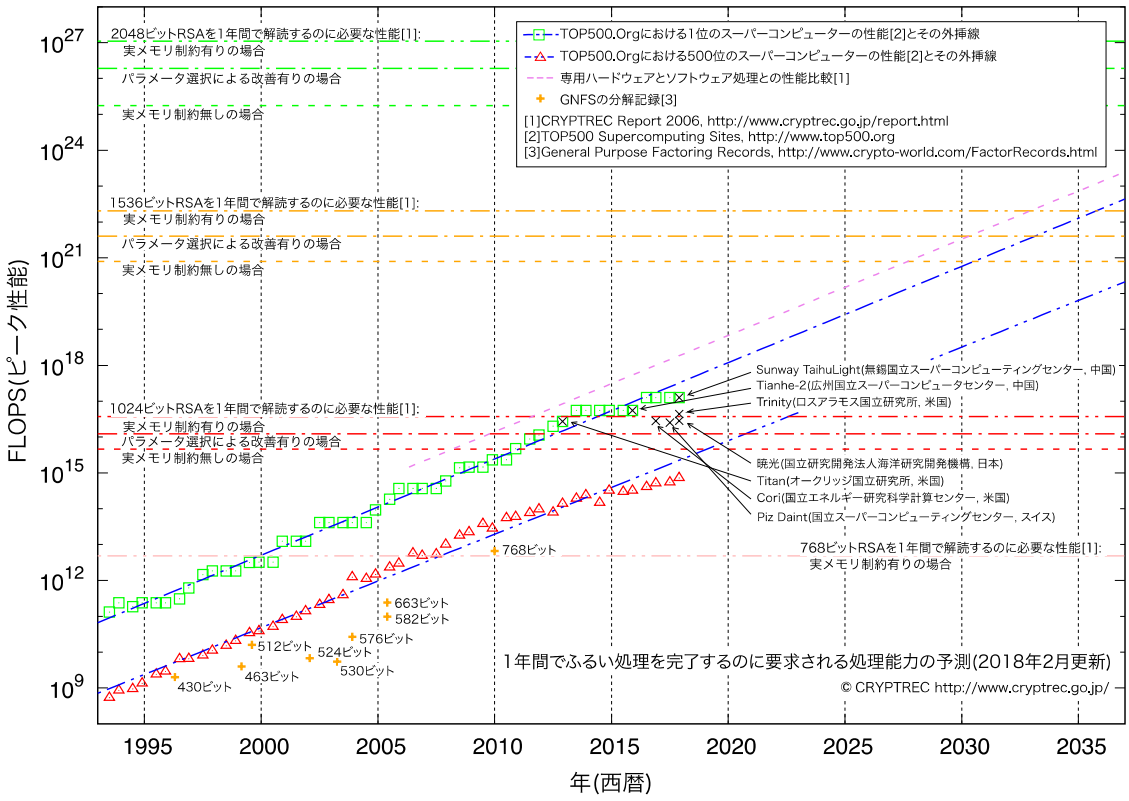


図 3-2: 素因数分解の困難性に関する計算量評価

(1 年間でふるい処理を完了するのに要求される処理能力の予測、2018 年 2 月更新)

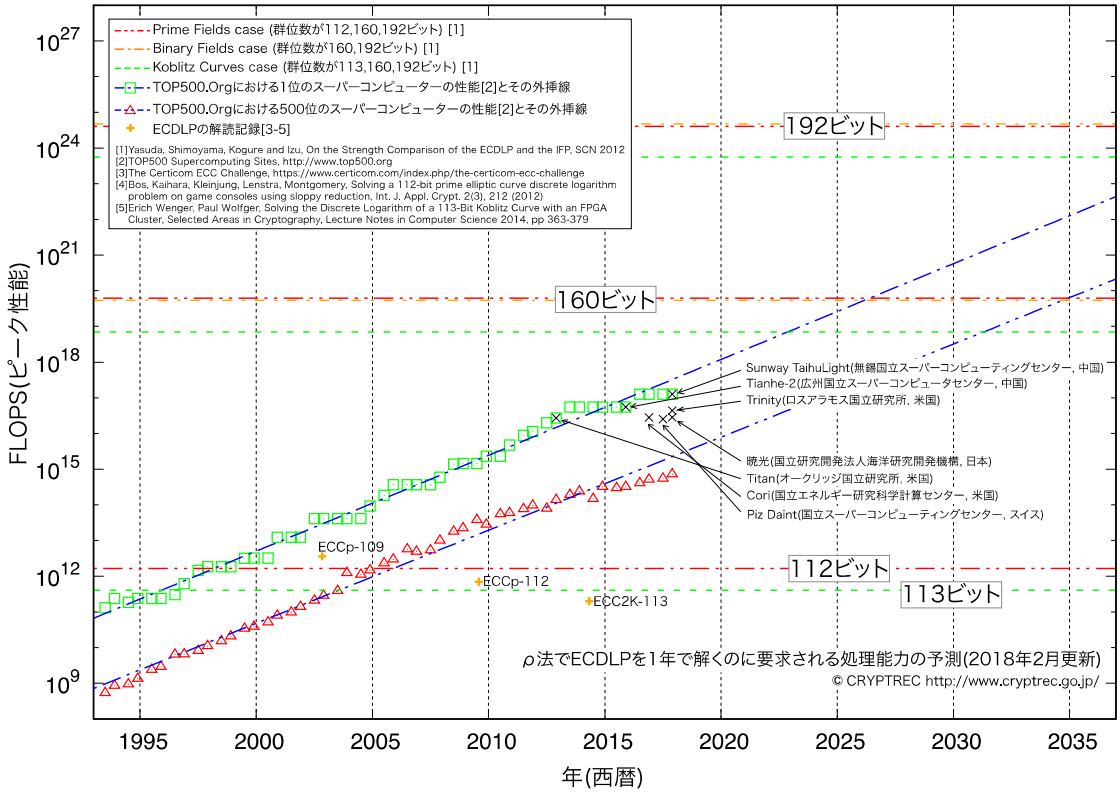


図 3-3：楕円曲線上の離散対数計算の困難性に関する計算量評価

（ρ 法で ECDLP を 1 年で解くのに要求される処理能力の予測、2018 年 2 月更新）

電子政府における調達のために参照すべき暗号のリスト
（CRYPTREC暗号リスト）

平成２５年３月１日
総　　務　　省
経　済　産　業　省

電子政府推奨暗号リスト

暗号技術検討会[1]及び関連委員会（以下、「CRYPTREC」という。）により安全性及び実装性能が確認された暗号技術[2]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。

技術分類		暗号技術
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS(注1)
		RSASSA-PKCS1-v1_5(注1)
	守秘	RSA-OAEP(注1)
	鍵共有	DH
		ECDH
共通鍵暗号	64 ビットブロック暗号(注2)	該当なし
	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(注13)	CCM
		GCM(注4)
メッセージ認証コード		CMAC
		HMAC
認証暗号		該当なし
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

[1] 総務省政策統括官（情報セキュリティ担当）及び経済産業省商務情報政策局長が有識者の参集を求め、暗号技術の普及による情報セキュリティ対策の推進を図る観点から、専門家による意見等を聴取することにより、総務省及び経済産業省における施策の検討に資することを目的として開催。

[2] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

（注1） 「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 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成25年 3 月 1 日 現在）

（注2） CRYPTREC暗号リストにおいて、64 ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注4） 初期化ベクトル長は 96 ビットを推奨する。

（注13） CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

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[3]のリスト。

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	該当なし
	鍵共有	PSEC-KEM(注5)
共通鍵暗号	64 ビットブロック暗号(注6)	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(注7)
ハッシュ関数		SHA-512/256
		SHA3-256
		SHA3-384
		SHA3-512
		SHAKE128(注12)
		SHAKE256(注12)
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(注14)	該当なし
メッセージ認証コード		PC-MAC-AES
認証暗号		ChaCha20-Poly1305
エンティティ認証		ISO/IEC 9798-4

（注5） KEM (Key Encapsulating Mechanism) - DEM (Data Encapsulating Mechanism) 構成における利用を前提とする。

（注6） CRYPTREC暗号リストにおいて、64 ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注7） 平文サイズは 64 ビットの倍数に限る。

（注12） ハッシュ長は 256 ビット以上とすること。

（注14） CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

[3] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

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とCRYPTRECにより確認された暗号技術[4]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。

技術分類		暗号技術
公開鍵暗号	署名	該当なし
	守秘	RSAES-PKCS1-v1_5(注8)(注9)
	鍵共有	該当なし
共通鍵暗号	64 ビットブロック暗号(注15)	3-key Triple DES
	128 ビットブロック暗号	該当なし
	ストリーム暗号	128-bit RC4(注10)
ハッシュ関数		RIPEMD-160
		SHA-1(注8)
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(注16)	該当なし
メッセージ認証コード		CBC-MAC(注11)
認証暗号		該当なし
エンティティ認証		該当なし

（注8） 「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 情報セキュリティ政策会議決定、平成24年10月情報セキュリティ対策推進会議改定）を踏まえて利用すること。
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
（平成25年 3 月 1 日 現在）

（注9） SSL 3.0 / TLS 1.0, 1.1, 1.2 で利用実績があることから当面の利用を認める。

（注10） 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。

（注11） 安全性の観点から、メッセージ長を固定して利用すべきである。

（注15） CRYPTREC暗号リストにおいて、64 ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。

（注16） CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。

[4] 暗号利用モード、メッセージ認証コード、エンティティ認証は、他の技術分類の暗号技術と組み合わせて利用することとされているが、その場合、CRYPTREC暗号リストに掲載されたいずれかの暗号技術と組み合わせること。

変更履歴情報

変更日付	変更箇所	変更前の記述	変更後の記述
平成27年 3月27日	（注１０）	128-bit RC4 は、 SSL(TLS1.0 以上)に限定して利用すること。	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。
平成28年 3月29日	推奨候補 暗号リスト （技術分類： ハッシュ関数）	該当なし	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256(注12)
	（注１２）	[新規追加]	ハッシュ長は 256 ビット以上とすること。
平成29年 3月30日	推奨候補 暗号リスト （技術分類： ハッシュ関数）	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE256(注12)	SHA-512/256 SHA3-256 SHA3-384 SHA3-512 SHAKE128(注12) SHAKE256(注12)
平成30年 3月29日	（注２） （注６）	より長いブロック長の暗号が利用できるのであれば、128 ビットブロック暗号を選択することが望ましい。	CRYPTREC暗号リストにおいて、64 ビットブロック暗号により、同一の鍵を用いて暗号化する場合、2^{20}ブロックまで、同一の鍵を用いてCMACでメッセージ認証コードを生成する場合、2^{21}ブロックまでとする。
	（注１５）	[新規追加]	
	電子政府推奨 暗号リスト （技術分類： 共通鍵暗号）	3-key Triple DES(注3)	該当なし
	（注３）	3-key Triple DES は、以下の条件を考慮し、当面の利用を認める。 １）NIST SP 800-67 とし	[削除]

		て規定されていること。 ２）デファクトスタンダードとしての位置を保っていること。	
	運用監視暗号リスト（技術分類：共通鍵暗号）	該当なし	3-key Triple DES（注１５）
	電子政府推奨暗号リスト	［技術分類の新設］	技術分類：認証暗号 暗号技術：該当なし
	推奨候補暗号リスト		技術分類：認証暗号 暗号技術： ChaCha20-Poly1305
	運用監視暗号リスト		技術分類：認証暗号 暗号技術：該当なし
	（注１３） （注１４） （注１６）	［新規追加］	CRYPTREC暗号リスト掲載のブロック暗号を、認証付き秘匿モードと組み合わせて、「認証暗号」として使うことができる。
	電子政府推奨暗号リスト（見出し）	名称	暗号技術
	推奨候補暗号リスト（見出し）		
	運用監視暗号リスト（見出し）		

付録２

CRYPTREC 暗号リスト掲載暗号の問い合わせ先一覧

電子政府推奨暗号リスト

1. 公開鍵暗号

暗号名	DSA
関連情報	仕様
・ NIST Federal Information Processing Standards Publication 186-4 (July 2013), Digital Signature Standard (DSS) で規定されたもの。 ・ 参照 URL http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf	

暗号名	ECDSA (Elliptic Curve Digital Signature Algorithm)
関連情報 1	公開ホームページ
和文： http://www.fujitsu.com/jp/group/labs/resources/tech/external-activities/crypto/ 英文： http://www.fujitsu.com/jp/group/labs/en/resources/tech/external-activities/crypto/ ・ 参照 URL SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0) http://www.secg.org/SEC1-Ver-1.0.pdf	
問い合わせ先 1	
富士通株式会社 電子政府推奨暗号 問い合わせ窓口 E-MAIL：fj-soft-crypto-ml@dl.jp.fujitsu.com	
関連情報 2	仕様
・ ANS X9.62-2005, Public Key Cryptography for The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA) で規定されたもの。 ・ 参照 URL http://www.x9.org/	

暗号名	RSA Public-Key Cryptosystem with Probabilistic Signature Scheme (RSA-PSS)
関連情報	仕様　公開ホームページ
	・ PKCS#1 RSA Cryptography Standard (Ver.2.2) ・ 参照 URL http://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf 和文：なし

暗号名	RSASSA-PKCS1-v1_5
関連情報	仕様　公開ホームページ
	・ PKCS#1 RSA Cryptography Standard (Ver.2.2) ・ 参照 URL http://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf 和文：なし

暗号名	RSA Public-Key Cryptosystem with Optimal Asymmetric Encryption Padding (RSA-OAEP)
関連情報	仕様　公開ホームページ
	・ PKCS#1 RSA Cryptography Standard (Ver.2.2) ・ 参照 URL http://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf 和文：なし

暗号名	DH
関連情報 1	仕様
	・ ANSI X9.42-2003, Public Key Cryptography for The Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography で規定されたもの。 ・ 参照 URL http://www.x9.org/
関連情報 2	仕様
	・ NIST Special Publication 800-56A Revision 2 (May 2013), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography において、FCC DH プリミティブとして規定されたもの。 ・ 参照 URL http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf

暗号名	ECDH (Elliptic Curve Diffie-Hellman Scheme)
関連情報 1	公開ホームページ
和文： http://www.fujitsu.com/jp/group/labs/resources/tech/external-activities/crypto/ 英文： http://www.fujitsu.com/jp/group/labs/en/resources/tech/external-activities/crypto/ ・ 参照 URL SEC 1: Elliptic Curve Cryptography (September 20, 2000 Version 1.0) http://www.secg.org/SEC1-Ver-1.0.pdf	
問い合わせ先 1	
富士通株式会社 電子政府推奨暗号 問い合わせ窓口 E-MAIL：fj-soft-crypto-ml@dl.jp.fujitsu.com	
関連情報 2	仕様
・ NIST Special Publication SP 800-56A Revision 2(May 2013), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography において、C(2e,0s,ECC CDH)として規定されたもの。 ・ 参照 URL http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf	

2. 共通鍵暗号

暗号名	AES
関連情報	仕様
・ NIST FIPS PUB 197, Specification for the ADVANCED ENCRYPTION STANDARD (AES), November 26, 2001 ・ 参照 URL http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf	

暗号名	Camellia
関連情報	公開ホームページ
和文：http://info.isl.ntt.co.jp/crypt/camellia/index.html 英文：http://info.isl.ntt.co.jp/crypt/eng/camellia/index.html	
問い合わせ先	〒180-8585 東京都武蔵野市緑町 3-9-11
日本電信電話株式会社　NTT セキュアプラットフォーム研究所 Camellia 問い合わせ窓口　担当 TEL:0422-59-6582, FAX:0422-59-4015 E-MAIL: camellia-ml@hco.ntt.co.jp	

暗号名	KCipher-2
関連情報	公開ホームページ 和文：http://www.kddi-research.jp/products/kcipher2.html 英文：http://www.kddi-research.jp/english/products/kcipher2.html
問い合わせ先	〒356-8502 埼玉県ふじみ野市大原 2-1-15 株式会社 KDDI 総合研究所　情報セキュリティグループ グループリーダー　清本 晋作 TEL:049-278-7638, FAX:049-278-7510 E-MAIL: kiyomoto@kddi-research.jp

3. ハッシュ関数

暗号名	SHA-256, SHA-384, SHA-512
関連情報	仕様 ・ NIST FIPS PUB 180-4, Secure Hash Standard (SHS) ・ 参照 URL http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

4. 暗号利用モード(秘匿モード)

暗号名	CBC, CFB, CTR, OFB
関連情報	仕様 ・ NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques ・ 参照 URL http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

5. 暗号利用モード(認証付き秘匿モード)

暗号名	CCM
関連情報	仕様
	・ NIST SP 800-38C, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004 ・ 参照 URL http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf

暗号名	GCM
関連情報	仕様
	・ NIST SP 800-38D, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, November 2007 ・ 参照 URL http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

6. メッセージ認証コード

暗号名	CMAC
関連情報	仕様
	・ NIST FIPS SP 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005 (Updated Oct. 2016) ・ 参照 URL http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38b.pdf

暗号名	HMAC
関連情報	仕様
	・ NIST FIPS PUB 198-1, The Keyed-Hash Message Authentication Code (HMAC), July 2008 ・ 参照 URL http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.198-1.pdf

7. エンティティ認証

暗号名	ISO/IEC 9798-2
関連情報	仕様
	・ ISO/IEC 9798-2:2008, Information technology - Security techniques - Entity Authentication - Part 2: Mechanisms using symmetric encipherment algorithms, 2008. 及び ISO/IEC 9798-2:2008/Cor.1:2010, Information technology - Security techniques - Entity Authentication - Part 2: Mechanisms using symmetric encipherment algorithms. Technical Corrigendum 1, 2010 で規定されたもの。なお、同規格書は日本規格協会(http://www.jsa.or.jp/)から入手可能である。

暗号名	ISO/IEC 9798-3
関連情報	仕様
	・ ISO/IEC 9798-3:1998, Information technology - Security techniques - Entity Authentication - Part 3: Mechanisms using digital signature techniques, 1998. 及び ISO/IEC 9798-3:1998/Amd.1:2010, Information technology - Security techniques - Entity Authentication - Part 3: Mechanisms using digital signature techniques. Amendment 1, 2010 で規定されたもの。なお、同規格書は日本規格協会(http://www.jsa.or.jp/)から入手可能である。

推奨候補暗号リスト

1. 公開鍵暗号

暗号名	PSEC-KEM Key agreement
関連情報	公開ホームページ
	和文　http://info.isl.ntt.co.jp/crypt/psec/index.html 英文　http://info.isl.ntt.co.jp/crypt/eng/psec/index.html
問い合わせ先	〒180-8585 東京都武蔵野市緑町 3-9-11
	日本電信電話株式会社　NTT セキュアプラットフォーム研究所 PSEC-KEM 問い合わせ窓口　担当 TEL: 0422-59-3462　　FAX: 0422-59-4015 E-MAIL: publickey-ml@hco.ntt.co.jp

2. 共通鍵暗号

暗号名	CIPHERUNICORN-E
関連情報	公開ホームページ
	和文：https://jpn.nec.com/secureware/sdk/cipherunicorn-e.html 英文：https://jpn.nec.com/secureware/sdk/cipherunicorn-e-en.html
問い合わせ先	〒211-8666 神奈川県川崎市中原区下沼部 1753
	日本電気株式会社　セキュリティ・ネットワーク事業部 E-MAIL: info@security.jp.nec.com

暗号名	Hierocrypt-L1
関連情報	公開ホームページ
	和文：http://www.toshiba.co.jp/rdc/security/hierocrypt/ 英文：http://www.toshiba.co.jp/rdc/security/hierocrypt/index.htm
問い合わせ先	〒212-8582 神奈川県川崎市幸区小向東芝町 1
	株式会社東芝 研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー 電子政府推奨暗号 問い合わせ窓口 E-MAIL: rdc-crypt-info@ml.toshiba.co.jp

暗号名	MISTY1
関連情報	公開ホームページ http://www.mitsubishielectric.co.jp/corporate/randd/information_technology/security/code/misty01_b.html
問い合わせ先	〒247-8520 神奈川県鎌倉市上町屋 325 番地 三菱電機株式会社 インフォメーションシステム統括事業部 トータルソリューションシステム第二部 IoT 技術課　坂上 勉 TEL：0467-41-3516 E-MAIL：Sakagami.Tsutomu@bp.MitsubishiElectric.co.jp

暗号名	CIPHERUNICORN-A
関連情報	公開ホームページ 和文：https://jpn.nec.com/secureware/sdk/cipherunicorn-a.html 英文：https://jpn.nec.com/secureware/sdk/cipherunicorn-a-en.html
問い合わせ先	〒211-8666 神奈川県川崎市中原区下沼部 1753 日本電気株式会社　セキュリティ・ネットワーク事業部 E-MAIL:　info@security.jp.nec.com

暗号名	CLEFIA
関連情報	公開ホームページ 和文：https://www.sony.co.jp/Products/cryptography/clefia/ 英文：https://www.sony.net/Products/cryptography/clefia/
問い合わせ先	ソニー株式会社 CLEFIA 問い合わせ窓口 E-MAIL: clefia-q@jp.sony.com

暗号名	Hierocrypt-3
関連情報	公開ホームページ 和文：http://www.toshiba.co.jp/rdc/security/hierocrypt/ 英文：http://www.toshiba.co.jp/rdc/security/hierocrypt/index.htm
問い合わせ先	〒212-8582 神奈川県川崎市幸区小向東芝町 1 株式会社東芝 研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー 電子政府推奨暗号 問い合わせ窓口 E-MAIL: rdc-crypt-info@ml.toshiba.co.jp

暗号名	SC2000
関連情報	公開ホームページ
和文： http://www.fujitsu.com/jp/group/labs/resources/tech/external-activities/crypto/ 英文： http://www.fujitsu.com/jp/group/labs/en/resources/tech/external-activities/crypto/	
問い合わせ先	富士通株式会社 電子政府推奨暗号 問い合わせ窓口
E-MAIL： fj-soft-crypto-ml@dl.jp.fujitsu.com	

暗号名	MUGI
関連情報	公開ホームページ
和文：http://www.hitachi.co.jp/rd/yrl/crypto/mugi/ 英文：http://www.hitachi.com/rd/yrl/crypto/mugi/	
問い合わせ先	〒140-8572 東京都品川区南大井 6-27-18
株式会社日立製作所 セキュリティ事業統括本部 セキュリティ先端技術本部 HIRT センタ 主任技師 栗田 博司 TEL：044-555-0894(ダイヤルイン), FAX ： 03-5471-4677 E-MAIL： hiroshi.kurita.wp@hitachi.com	

暗号名	Enocoro-128v2
関連情報	公開ホームページ
和文:http://www.hitachi.co.jp/rd/yrl/crypto/enocoro/ 英文:http://www.hitachi.com/rd/yrl/crypto/enocoro/index.html	
問い合わせ先	〒244-0817 神奈川県横浜市戸塚区吉田町 292
株式会社日立製作所　研究開発グループ　システムイノベーションセンタ セキュリティ研究部　主任研究員　渡辺 大 TEL：050-3135-2017, FAX：050-3135-3392 E-MAIL: dai.watanabe.td@hitachi.com	

暗号名	MULTI-S01
関連情報	公開ホームページ 和文：http://www.hitachi.co.jp/rd/yrl/crypto/s01/ 英文：http://www.hitachi.com/rd/yrl/crypto/s01/
問い合わせ先	〒140-8572 東京都品川区南大井 6-27-18 株式会社日立製作所 セキュリティ事業統括本部 セキュリティ先端技術本部 HIRT センタ 主任技師 栗田 博司 TEL：044-555-0894(ダイヤルイン), FAX ： 03-5471-4677 E-MAIL：hiroshi.kurita.wp@hitachi.com

3. ハッシュ関数

暗号名	SHA-512/256
関連情報	仕様 ・ NIST FIPS PUB 180-4, Secure Hash Standard (SHS) ・ 参照 URL http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

暗号名	SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256
関連情報	仕様 ・ NIST FIPS PUB 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions ・ 参照 URL http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf

4. メッセージ認証コード

暗号名	PC-MAC-AES
関連情報	
参照 URL: http://jpn.nec.com/rd/crl/code/research/pcmacaes.html	
問い合わせ先	〒211-8666 神奈川県川崎市中原区下沼部 1753 日本電気株式会社　セキュリティ研究所　主任研究員 峯松 一彦 TEL：044-431-7686, FAX：044-431-7644 E-MAIL: k-minematsu@ah.jp.nec.com

5. 認証暗号

暗号名	ChaCha20-Poly1305
関連情報	仕様 ・ Internet Research Task Force (IRTF), Request for Comments (RFC) 7539, ChaCha20 and Poly1305 for IETF Protocols, May 2015 で規定されたもの。 ・ 参照 URL https://tools.ietf.org/html/rfc7539

6. エンティティ認証

暗号名	ISO/IEC 9798-4
関連情報	仕様 ・ ISO/IEC 9798-4:1999, Information technology - Security techniques - Entity Authentication - Part 4: Mechanisms using a cryptographic check function, 1999. 及び ISO/IEC 9798-4:1999/Cor.1:2009, Information technology - Security techniques - Entity Authentication - Part 3: Mechanisms using a cryptographic check function. Technical Corrigendum 1, 2009 で規定されたもの。なお、同規格書は日本規格協会(http://www.jsa.or.jp/)から入手可能である。

運用監視暗号リスト

1. 公開鍵暗号

暗号名	RSAES-PKCS1-v1_5
関連情報	仕様

- PKCS#1 RSA Cryptography Standard (Ver.2.2)
- 参照 URL

http://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf

和文：なし

2. 共通鍵暗号

暗号名	Triple DES
関連情報	仕様

- NIST SP 800-67 Revision 2, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, November 2017
- 参照 URL

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-67r2.pdf

暗号名	RC4
関連情報	仕様

- RC4 は EMC Corporation 社のトレードマークである。
- 仕様 RC4 のアルゴリズムについては、RSA Laboratories が発行した CryptoBytes 誌 (Volume5, No.2, Summer/Fall 2002) に掲載された次の論文に記載されているもの。
  Fluhrer, Scott, Itsik Mantin, and Adi Shamir, "Attacks On RC4 and WEP", CryptoBytes, Volume 5, No.2, Summer/Fall 2002
- 参照 URL

http://www.cryptrec.go.jp/cryptrec_13_spec_cypherlist_files/PDF/cryptobytes_v5n2.pdf

3. ハッシュ関数

暗号名	RIPEMD-160
関連情報	仕様
・ 参照 URL http://www.esat.kuleuven.ac.be/~bosselae/ripemd160.html	

暗号名	SHA-1
関連情報	仕様
・ NIST FIPS PUB 180-4, Secure Hash Standard (SHS) ・ 参照 URL http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf	

4. メッセージ認証コード

暗号名	CBC-MAC
関連情報	仕様
・ ISO/IEC 9797-1:1999, Information technology - Security techniques - Message Authentication Codes(MACs) - Part 1: Mechanisms using a block cipher, 1999 で規定されたもの。なお、同規格書は日本規格協会(http://www.jsa.or.jp/)から入手可能である。	

付録３

768 ビット素数位数の有限体上の離散対数問題の状況と DSA, DH の今後のパラメータ選択について

平成 29 年 8 月 30 日
暗号技術評価委員会

有限体上の離散対数問題は、現在、CRYPTREC 暗号リストの電子政府推奨暗号リストに掲載されている DSA 及び DH や、インターネットで使われているセキュア通信プロトコル TLS における鍵共有方式など、多くの暗号技術の安全性の根拠として利用されています。

暗号技術評価委員会は、RSA1024 に係る移行指針と同様に、DSA や DH を利用する場合には、鍵長において、2048 ビット以上の素数位数の有限体を用いることを推奨します。

有限体上の離散対数問題[1]は、現在、CRYPTREC 暗号リストの電子政府推奨暗号リスト[2]に掲載されている DSA 及び DH や、インターネットで使われているセキュア通信プロトコル TLS[3]における鍵共有方式など、多くの暗号技術の安全性の根拠として利用されています。

CRYPTREC では、以前より、(素数位数の)有限体上の離散対数問題における安全なパラメータサイズは、RSA 合成数の素因数分解問題における安全なパラメータサイズと同等であると判断しています[4]。

今般、位数が 768 ビット長の素数である有限体(以下、768 ビットの素体という)における離散対数の計算結果を示した論文[5]が、国際暗号学会 (International Association for Cryptologic Research (IACR)) が主催する国際会議 EUROCRYPT 2017[6]で発表されました。この論文では、768 ビットの素体上の離散対数の計算に要する計算コストが、2.2 GHz Xeon E5-2660 プロセッサ換算で、約 5300 コア・年に相当するものと見積もられています。

768 ビットの RSA 合成数の素因数分解に要する計算コストは、CRYPTO2010 で発表された論文[7]では、約 1700 コア・年と見積もられているので、これらの計算コストの違いはたかだか数倍程度となります。これは上記の判断の妥当性の根拠の一つとみなせます。

このため、暗号技術評価委員会では、RSA1024 に係る移行指針[2, 8]と同様に、今後とも DSA や DH を利用する場合には、鍵長において、2048 ビット以上の素数位数の有限体を用いることを推奨します。

暗号技術評価委員会では、今後も引続き状況の監視・調査を行い、CRYPTREC Web サイトなどを通じてお知らせしてまいります。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 at cryptrec.go.jp

【本レポートは、暗号アルゴリズムの脆弱性に関する情報発信フロー(暗号技術検討会 2015 年度報告書[9]の 3.2.3.(2))における「C:長期的なシステムの安全性維持のための対策喚起」として発表しています。】

[1] 有限体の元である g と y が $y = g^x$ を満たすとき x を求める問題を有限体上の離散対数問題といいます。現在までのところ、大きな位数(元の総数)である有限体上の離散対数を計算することは、一般的に難しいこととされています。

[2] 電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト)
http://www.cryptrec.go.jp/images/cryptrec-ls-0001-2016.pdf

[3] T. Dierks et al., "The Transport Layer Security (TLS) Protocol Version 1.2", RFC5246,
https://tools.ietf.org/html/rfc5246

[4] CRYPTREC Report 2006,
http://www.cryptrec.go.jp/report/c06_wat_final.pdf

[5] T. Kleinjung et al., "Computation of a 768-bit prime field discrete logarithm",
https://eprint.iacr.org/2017/067

[6] https://eurocrypt2017.di.ens.fr/

[7] T. Kleinjung et al., "Factorization of a 768-bit RSA modulus",
https://eprint.iacr.org/2010/006

[8] 「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 日改定 情報セキュリティ対策推進会議決定)
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf

[9] 暗号技術検討会 2015 年度報告書
http://www.cryptrec.go.jp/report/c15_kentou_final.pdf

付録４

ChaCha20-Poly1305 および Poly1305 の安全性調査・評価(概要版)

岩田　哲

名古屋大学大学院工学研究科

2017 年 10 月

エグゼクティブサマリー

メッセージ認証コード Poly1305 [Ber05b] および認証暗号化方式 ChaCha20-Poly1305 [NL15] の安全性調査・評価を行った．

Poly1305 について，次の結果を得た．

- Bernstein による安全性証明 [Ber05b, Ber05a] に問題点は見受けられない．Poly1305 は証明可能安全性を有する MAC である．
- 関連鍵攻撃が可能である．しかし人工的な攻撃であり，現実的な脅威とはならないと考えられる．
- 複数ユーザ安全性について，ユーザ数への依存が限定的な安全性バウンドを導出できる．一般に，証明可能安全性の観点からはユーザ数が増加すると敵の攻撃確率の上界がそれに伴い増加するが，Poly1305 ではこの増加が限定的である．

また文献調査により，次のことを確認した．

- 弱鍵が存在する．
- 再偽造可能性の意味で耐性がある．
- ナンスを再利用すると多項式ハッシュ関数の鍵を導出でき，偽造攻撃ができる．

また，ChaCha20-Poly1305 について次の結果を得た．

- Procter による [Pro14] の証明には一か所軽微な誤りがあるが簡単に修正可能であり，ChaCha20-Poly1305 は証明可能安全性を有する認証暗号化方式である．
- ChaCha20 ブロック関数が関連鍵攻撃に対して安全であるという仮定のもと，ChaCha20-Poly1305 は関連鍵攻撃に対する安全性を有する．
- 再偽造可能性の意味で耐性がある．
- ナンスを再利用すると偽造攻撃ができる．
- 弱鍵が存在する．
- 復号ミスユース耐性について，暗号化の意味での安全性は失われるが，認証の意味での安全性は保たれる．
- 複数ユーザ安全性について，ユーザ数に依存した自明な安全性バウンドを導出できる．また，ユーザ数への依存が限定的な安全性バウンドを導出できると予想される．

Poly1305 と ChaCha20-Poly1305 両方について，ナンスの再利用による安全性への影響は大きく，実装の際にはこれが起こらないよう注意が必要である．弱鍵の影響はどちらも少ないと考えられ，また Poly1305 の関連鍵攻撃が現実的に問題となることはないと考えられる．その他，懸念事項は見受けられない．

なお本報告書は Poly1305 と ChaCha20-Poly1305 のメッセージ認証コードと認証暗号化方式としての理論的な安全性調査・評価を行ったものであり，サイドチャネル攻撃等の実装に関する解析，あるい TLS のプロトコルとしての安全性解析等は扱っていない．

付録５

ChaCha20-Poly1305 の実装性能調査
(概要版)

株式会社レピダム

2017 年 10 月

第1章　エグゼクティブサマリー

本調査では、認証暗号 (Authentication Encryption: AE または Authenticated Encryption with Associated Data: AEAD) の一種である ChaCha20-Poly1305 について、実際に利用する観点で、標準化状況や OSS コミュニティでの採用状況を踏まえて、実装性能評価を実施した。

ChaCha20-Poly1305 は特に IETF (Internet Engineering Task Force) で積極的に標準化が進められており、今後も幅広いプロトコルへの適用が予想される。また各種 OSS での採用も広まっており、ChaCha20-Poly1305 の利用環境は整いつつあると言える。

ChaCha20-Poly1305 の実装性能を評価した論文はまだ少ない。ベンチマークとしてソフトウェア実装やハードウェア実装が公開されており、ベンチマーク結果において今後組み込み環境において ChaCha20-Poly1305 の性能が向上することが示唆されている。

世界中で広く利用されている OpenSSL を用いて ChaCha20-Poly1305 と他の認証暗号との性能比較を行った。AES-NI を有効にした Intel Core i7 において、ChaCha20-Poly1305 のスループットは、鍵長以下のデータサイズでは AES-NI 無効時より小さく、鍵長を超えるデータサイズでは大きくなることがわかった。また AES-NI を有効にした Intel Xeon においては、ChaCha20-Poly1305 のスループットはデータサイズによらずほとんど変わらないことがわかった。AES-NI 有効時および AES-NI 無効時において AES-GCM と ChaCha20-Poly1305 のスループットを比較すると、AES-NI 無効時に ChaCha20-Poly1305 の実行速度が AES-GCM を上回ることがわかった。

表 5.7: Linux における認証暗号の性能比較結果（AES-NI 有効時）

データサイズ	AES-GCM 128bit	AES-CCM 128bit	AES-GCM 256bit	AES-CCM 256bit	ChaCha20 -Poly1305
16 bytes	510175.13	608111.52	428784.76	535849.70	241889.67
64 bytes	1188073.26	2438522.67	1131148.69	2213954.71	471620.46
256 bytes	2373195.95	9757960.96	2004236.03	8849291.52	916063.15
1024 bytes	3767685.80	39013930.33	2931220.82	35412411.05	1716506.28
8192 bytes	4724222.63	310425097.56	3431729.83	266724133.55	1825169.41
16384 bytes	4795012.44	623660083.88	3480622.42	566605561.86	1851042.47

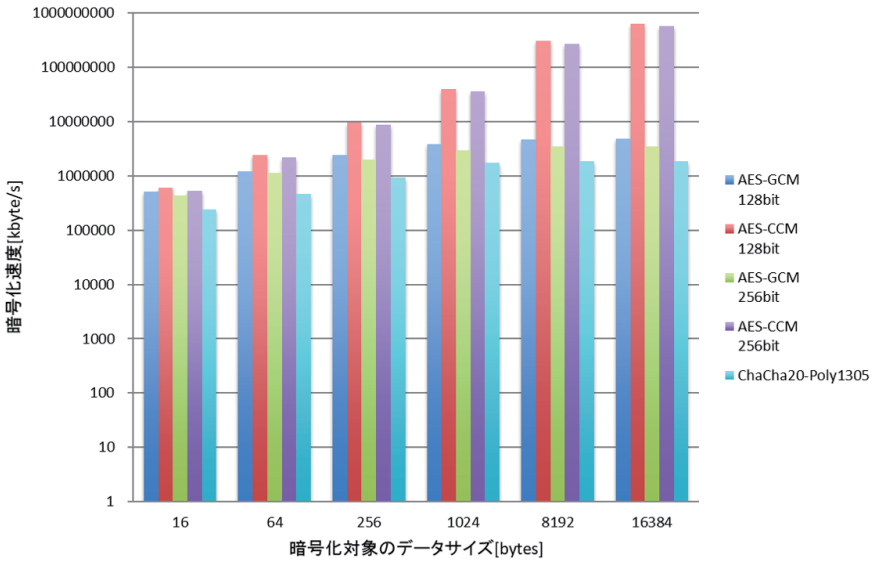


図 5.9: AES-NI 有効時の性能比較結果 (Linux)

表 5.15: Linux における認証暗号の性能比較結果（AES-NI 無効時）

データサイズ	AES-GCM 128bit	AES-CCM 128bit	AES-GCM 256bit	AES-CCM 256bit	ChaCha20 -Poly1305
16 bytes	84327.32	221654.70	68747.66	173721.25	241264.39
64 bytes	98523.65	887972.20	76813.31	697759.83	460033.79
256 bytes	221492.39	3554475.52	187173.03	2798027.18	845216.94
1024 bytes	235878.06	14200349.01	200182.44	11171555.33	929916.93
8192 bytes	237016.41	113009104.21	203634.01	88966176.77	953292.12
16384 bytes	239697.92	227576113.83	203696.81	178625265.66	944701.44

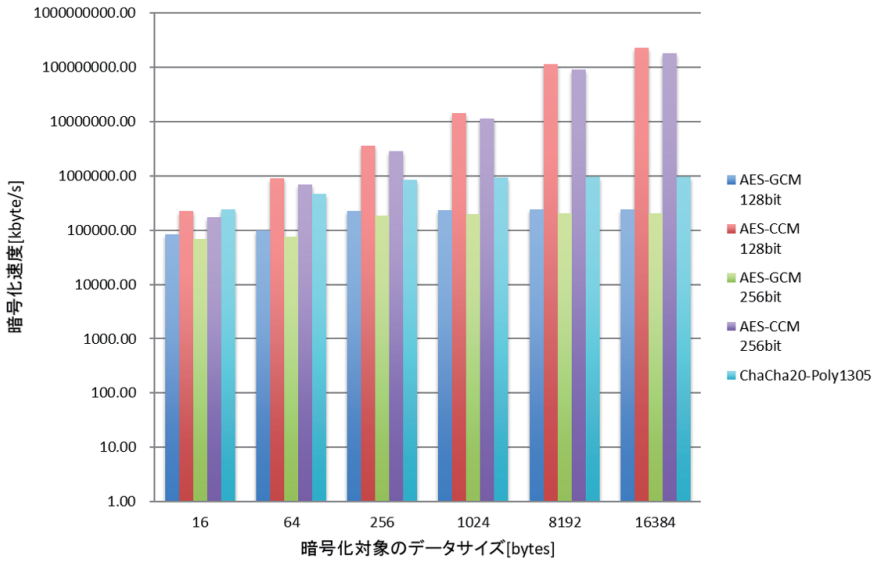


図 5.17: AES-NI 無効時の性能比較結果 (Linux)

付録６

CRYPTREC 暗号技術ガイドライン (SHA-1)
改定版

2018 年 4 月

国立研究開発法人情報通信研究機構
独立行政法人情報処理推進機構

目次

1. 本書の位置付け

1.1. 本書の目的

本書は、電子政府のシステム調達者及び電子政府システムを構築する開発者に向けて、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」(2013 年 3 月 1 日) [C13a]の「運用監視暗号リスト」[1]に記載されているハッシュ関数 SHA-1 を継続して利用する際に参考となる指針を示すものである。そのために、運用監視暗号リストに記載されている SHA-1 を補助関数として用いる暗号技術が、互換性維持の目的であれば継続利用が容認されるかどうかを示す。

2 章において、SHA-1 を用いる補助関数のタイプ別に各々の暗号技術の継続利用の指針について示し、3 章において SHA-1 を用いる補助関数のタイプと継続利用に関する詳細について示す。4 章において SHA-1 の危殆化に関する背景及びそれらに関連する参考情報について示す。

1.2. 本書の適用範囲

本書で取り扱う暗号技術は、1.2.1 節及び 1.2.2 節の範囲とする。

1.2.1. CRYPTREC 暗号リスト

本書で取り扱う暗号技術は、「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」(2013 年 3 月 1 日) [C13a]の「電子政府推奨暗号」[2]に記載されている暗号技術のうち、SHA-1 を利用する場合のあるものを対象とする(表 1)。

1.2.2. CRYPTREC 暗号の仕様書

本書で取り扱う暗号技術は、「CRYPTREC 暗号の仕様書」[C17b](2018 年 1 月現在)で指定されている仕様書を対象とする(表 1)。

---

[1] 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。

[2] 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が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。

表 1: 本書で対象となる暗号技術の範囲と仕様書

技術分類		暗号名称	仕様書
公開鍵暗号	署名	DSA	NIST FIPS PUB 186-4
		ECDSA	SEC 1: Elliptic Curve Cryptography (September 20, 2000, Version 1.0) または ANS X9.62-2005
		RSASSA-PKCS1-v1_5	Public-Key Cryptography Standards (PKCS)#1 v2.2
		RSA-PSS	Public-Key Cryptography Standards (PKCS)#1 v2.2
	守秘	RSA-OAEP	Public-Key Cryptography Standards (PKCS)#1 v2.2
	鍵共有	DH	ANS X9.42-2003 または NIST SP 800-56A Revision2 (May 2013)において FFC DH プリミティブとして規定されたもの
		ECDH	SEC 1: Elliptic Curve Cryptography (September 20, 2000, Version 1.0) または NIST SP 800-56A Revision2 (May 2013)において C(2e,0s,ECC CDH) として規定されたもの
メッセージ認証コード		HMAC	NIST FIPS PUB 198-1
エンティティ認証		ISO/IEC 9798-3	ISO/IEC 9798-3:1998, ISO/IEC 9798-3:1998/Amd 1:2010, ISO/IEC 9798-3:1998/Cor 1:2009, ISO/IEC 9798-3:1998/Cor 2:2012

1.3. 注意事項

本書の内容は、2018 年 1 月時点の情報に基づき記載されている。今後、CRYPTREC 暗号リストの改定や攻撃方法の進展状況等によって、本書に掲載される内容が現実にそぐわないケースが発生する可能性がある。

CRYPTREC では、SHA-1 の安全性に関する見解などを公表してきたが、内閣サイバーセキュリティセンター (National center of Incident readiness and Strategy for Cybersecurity、以下 NISC という。) や米国の国立標準技術研究所 (National Institute of Standards and Technology、以下 NIST という。) が示してきたような SHA-1 に関する利用期限については公表していない。

1.4. 謝辞

本書を作成するにあたり、セコム株式会社 IS 研究所の松本 泰 様、佐藤 雅史 様、島岡 政基 様、及び、NPO 日本ネットワークセキュリティ協会(JNSA) 電子署名 WG のメンバーの方々から有益なご意見・コメントいただいた。ここに謝意を表する。

2. CRYPTREC 暗号リストにおいて SHA-1 を補助関数として用いる電子政府推奨暗号の継続利用の指針

ハッシュ関数 SHA-1 は NIST が 1995 年に策定した、ハッシュ長が 160 ビットの暗号学的ハッシュ関数である [NT15b]。一般に、暗号学的ハッシュ関数には、衝突発見困難性[3]、第二原像計算困難性[4]及び原像計算困難性[5]の 3 つの安全性要件を満たすことが求められる。ところが、2017 年に SHA-1 は衝突発見困難性を満たしていないことが発表された[S17a,S17b]。

SHA-1 は、暗号技術の補助関数としてさまざまな部分で利用されており、CRYPTREC 暗号リストの多くの暗号技術において採用されている。その中には、衝突発見が安全性に直接的に影響を与えるものと与えないものが存在している。現状、実運用環境においては SHA-1 の継続利用を避けることが互換性維持の観点から現実的な選択肢ではない場面も想定されるため、CRYPTREC 暗号リストの電子政府推奨暗号リストにおいて補助関数として SHA-1 を用いる場合(ただし、擬似乱数生成系を除く[6])に、互換性維持の目的であれば継続利用が容認されるかどうかを示す(表 2)。

表 2: CRYPTREC 暗号リストにおいて SHA-1 を補助関数として用いる電子政府推奨暗号の継続利用の指針

技術分類	SHA-1 を補助関数として用いる暗号名称	継続利用の指針
署名	DSA, ECDSA, RSASSA-PKCS1-v1_5, RSA-PSS	署名生成については、 電子政府推奨暗号リストに記載されたハッシュ関数への移行を推奨 署名検証については、 互換性維持目的※での継続利用は容認
守秘	RSA-OAEP	互換性維持目的での継続利用は容認
鍵共有	DH, ECDH	
メッセージ認証コード	HMAC	
エンティティ認証	ISO/IEC 9798-3	

※ 電子政府推奨暗号リストに記載されたハッシュ関数への移行が困難な場合や SHA-1 の継続利用を停止すると、より大きなセキュリティ上の懸念が生じうる場合を想定している。また、ここで述べる互換性維持には該当しないが、後述する長期署名における過去の SHA-1 による署名検証も容認される。

[3] ハッシュ関数 Hash が衝突発見困難性を有するとは、$X_1 \neq X_2$ かつ Hash (X_1) = Hash (X_2) となる X_1, X_2 を見つけることが困難であることをいう。

[4] ハッシュ関数 Hash が第二原像計算困難性を有するとは、X_1 に対して、$X_1 \neq X_2$ かつ Hash (X_1) = Hash (X_2) となる X_2 を見つけることが困難であることをいう。

[5] ハッシュ関数 Hash が原像計算困難性を有するとは、Y に対して、Hash (X) = Y となる X を見つけることが困難であることをいう。

[6] 擬似乱数生成系は、その利用特性上、インタオペラビリティを確保する必要性がないため、暗号学的に安全な擬似乱数生成アルゴリズムであれば、どれを利用しても基本的に問題が生じない。

3. SHA-1 を用いる補助関数と継続利用の詳細

3.1. SHA-1 を用いる補助関数のタイプ

表 2 の指針の理由を示すため、本書で対象となる暗号技術の範囲における SHA-1 を用いる補助関数を分類する(表 3)。各補助関数のタイプについては、後述する。

表 3: 本書で対象となる暗号技術と補助関数のタイプ

技術分類	SHA-1 を補助関数として用いる暗号名称	補助関数のタイプ
署名	DSA, ECDSA, RSASSA-PKCS1-v1_5	・メッセージのハッシュ値
	RSA-PSS	・メッセージのハッシュ値 ・ハッシュ値の連結(MGF)
守秘	RSA-OAEP	・ハッシュ値の連結(MGF)
鍵共有	DH, ECDH	・ハッシュ値の連結(KDF)
メッセージ認証コード	HMAC	・ハッシュ関数のカスケーディング
エンティティ認証	ISO/IEC 9798-3	・上記の署名と同じ

3.1.1. メッセージのハッシュ値

本書で対象となる署名では、ハッシュ関数 Hash に関して、署名生成および署名検証対象のメッセージ M を入力として、その出力値(ハッシュ値) H = Hash(M) の計算を行う。

3.1.2. ハッシュ値の連結

3.1.2.1. マスク生成関数(Mask Generation Function, MGF)

本書で対象となる署名または守秘の中では、ハッシュ関数 Hash に関して、Data を入力として、h を空文字から始めて、Counter を 1 つずつ増やしながら、

h = h || Hash(Data || Counter)　(||は文字列の連結)

のように、ハッシュ値を連結していくことで、指定された長さの出力値 h の計算を行う。

3.1.2.2. 鍵導出関数(Key Derivation Function, KDF)

(a) 本書で対象となる鍵共有の中では、ハッシュ関数 Hash に関して、共有鍵 Z を入力として、h を空文字から始めて、Counter を 1 つずつ増やしながら、

$$h := \mathrm{Hash}(Z \,||\, \mathrm{OtherInfo}) \,||\, h, \text{ または}$$

$$h := \mathrm{Hash}(\mathrm{Counter} \,||\, Z \,||\, \mathrm{OtherInfo}) \,||\, h$$

のように[7]、出力値を次々に連結していくことで、指定された長さの出力値 h の計算を行うことがある。なお、OtherInfo とは、鍵共有が使われる状況に応じて決定される固有のデータを指す。

(b) 本書で対象となる鍵共有の中では、メッセージ認証コード HMAC [NT08]に関して、共有鍵 Z を入力として、h を空文字から始めて、Counter を 1 つずつ増やしながら、

$$h := \mathrm{HMAC}(\mathrm{Counter} \,||\, Z \,||\, \mathrm{OtherInfo}) \,||\, h$$

のように、出力値を次々に連結していくことで、指定された長さの出力値 h の計算を行う。なお、OtherInfo とは、鍵共有が使われる状況に応じて決定される固有のデータを指す。

3.1.3. ハッシュ関数のカスケーディング

本書で対象となるメッセージ認証コード HMAC [NT08]では、ハッシュ関数 Hash に関して、鍵 K 及びメッセージ M を入力として、

$$\mathrm{HMAC}(K, M) := \mathrm{Hash}(K_2 \,||\, \mathrm{Hash}(K_1 \,||\, M))$$

ただし、$K_1 := K \oplus \mathrm{ipad}$, $K_2 := K \oplus \mathrm{opad}$ である

(ipad と opad はある固定値で、⊕は排他的論理和).

のように、ハッシュ関数 Hash をカスケーディング(関数の合成)してハッシュ値の計算を行う。

[7] 各仕様によって、共有鍵 Z や Counter などの位置が前後する場合がある。

3.2. SHA-1 の継続利用について

3.2.1. 署名

署名には、署名が付与された文書やデータに改ざんが施されていないことを確認する改ざん防止の機能と、文書やデータに付与された署名が署名を付与した本人であることを確認するなりすましを防止する機能がある。ここでは、主に、署名生成から時間が経過した後に署名検証が求められる用途を想定し、指針を示す。このような用途の例としては電子契約等で用いる否認[8]防止目的の署名、コード署名、タイムスタンプ局が発行するタイムスタンプトークンの署名などが考えられる。

(1) 署名生成

署名対象となるハッシュ値が同じである相異なる 2 つの文書やデータの作成が現実的となれば、一方の文書(データ)に署名したあと、他方に差し替えられる(署名者が意図しなかった方の文書やデータに署名したかのように見せかけられる)リスクが高まるため、署名の作成において SHA-1 の継続利用は不適当である。署名を新規作成する場合には、より安全性の高いハッシュ関数(たとえば、ハッシュ関数 SHA-256 など)の利用に切り替えることが推奨される。

(2) 署名検証

電子政府システムやアプリケーションに依存するが、e-文書法など、法律的な要請を考慮して、当面の間、署名検証を必要とする場合もある。過去に SHA-1 を用いて生成された署名であっても、以下に述べる長期署名やその他の手段によって、作成された当時の署名の有効性が維持されていると判断される場合には、署名の検証において SHA-1 の継続利用は容認される。

有効性を維持する方法の一つとして、署名やタイムスタンプの有効期間を超えた後でも、それらの有効性を確認可能な長期署名フォーマット(CMS、XML 及び PDF に対応)が標準化されているので［I12a, I12b, I17, J08a, J08b］、長期保存が必要な場合は、これらを利用して署名検証を維持・継続できる。

[8] 電子契約等を取り交した後になって、その者がその事実や内容を否定すること。

3.2.2. 守秘

RSA-OAEP [R12]は、3.1.2.1.節で述べたように、マスク生成関数の補助関数としてハッシュ関数を使用している。RSA-OAEP の安全性に関しては、用いられているハッシュ関数に衝突耐性が保証されていなかったとしても安全性が保たれるという理論的な研究がなされている [KA10]。安全性について特段の問題点は指摘されていないため、守秘において SHA-1 の継続利用は互換性維持目的であれば容認される。

3.2.3. 鍵共有

過去の評価結果[C00,C01,C02]では、基本的な鍵共有の使用に際しては、受動的攻撃(鍵共有のために通信されるデータに攻撃者が影響を与えることがない場合)に対しては問題点は指摘されていないが、能動的攻撃(鍵共有のために通信されるデータに攻撃者が影響を与える可能性がある場合)に対して、最低限、以下の 3 点に注意を払う必要がある、とされている。

・公開鍵とエンティティとの結び付きを保証する手段を確保する。
・(更新を前提とする)セッション鍵共有方式として使用する場合には、交換する公開鍵は一時的なものとする。
・共有される鍵が乱数と見分けがつかなくするためには鍵導出関数を使用する。

共有される鍵を乱数と見分けがつかなくするために使用される鍵導出関数(Key Derivation Function, KDF)は、3.1.2.2.節で述べたように、補助関数のタイプ別では、ハッシュ値の連結ベースのものと、ハッシュ関数のカスケーディングベースのものの 2 つの構成方法がある。安全性について特段の問題点は指摘されていないため、鍵共有において SHA-1 の継続利用は互換性維持目的であれば容認される。

3.2.4. メッセージ認証コード

HMAC [NT08]は、3.1.3.節で述べたように、ハッシュ関数のカスケーディングベースで構成されている。HMAC の安全性に関しては、用いられているハッシュ関数に衝突耐性が保証されていなかったとしても安全性が保たれるという理論的な研究がなされている [B15, G14]。安全性について特段の問題点は指摘されていないため、メッセージ認証コードにおいて SHA-1 の継続利用は互換性維持目的であれば容認される。

3.2.5. エンティティ認証

エンティティ認証とは、認証される者が実際にその者であることを確認する機能である。ここでは、エンティティ認証を実現する仕組みとして署名を用いるものを想定している。3.2.1 節の署名とは異なり、チャレンジ-レスポンスのように、署名対象のデータ[9]と署名のデータを短時間で使い捨てるように利用される。衝突を計算する十分な時間が現時点では確保できないと考えられるため、短時間に認証が完了するのであれば、エンティティ認証に用いられる署名において SHA-1 の継続利用は互換性維持目的であれば容認される。

[9] ISO/IEC 9798-3 では、シークエンス番号、タイムスタンプ、ID 番号や乱数等からなるデータの組み合わせが規定されている。

4. SHA-1 の危殆化に関する背景と参考情報

4.1. CRYPTREC 及び NISC における対応

SHA-1 は、2002 年度に策定した「電子政府における調達のために参照すべき暗号のリスト（電子政府推奨暗号リスト）」(2003 年 2 月 20 日)に、注釈(注 6)[10]を付けて掲載された。暗号技術監視委員会(当時)は、2005 年に SHA-1 に対する衝突探索アルゴリズムに関する論文 [W05]が発表された際に、その詳細を検討し [C06]、「SHA-1 の安全性に関する見解」の案 [C05]を作成した。その後、この見解案は 2006 年 6 月 28 日に正式に承認され、暗号技術検討会事務局へ提出された [C07]。

その後、電子政府システムにおいて移行についての検討が進められ [ME10,ME11,MI09]、内閣官房情報セキュリティセンター(当時)は、2008 年 4 月に「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」 [NC08b]を公表した。なお、この指針は 2012 年 10 月に改定版 [NC12b]が公表されている。いままでに、政府認証基盤(GPKI)や地方公共団体組織認証基盤(LGPKI)などにおいて、システムの移行が進んでいる [L14,MI14]。

2012 年度に改定された CRYPTREC 暗号リストにおいては、運用監視暗号リストに、注釈(注 8)[11]を付けて記載された。

2015 年 10 月 8 日に、オランダの国立情報工学・数学研究所(CWI)、フランスの国立情報学自動制御研究所(INRIA)及びシンガポールの南洋理工大学(NTU)の共同研究チームは、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衝突発見に成功したと発表した [S15]。暗号技術評価委員会では、CRYPTREC の Web ページにおいてこの件に関する注意喚起を行い [C15a]、暗号技術検討会に報告した [C15b]。

2017 年 2 月 23 日に、CWI 及び Google の共同研究チームは、SHA-1 のフルラウンドに対する衝突発見に成功したと発表した [S17a]。発表された論文 [S17b]によれば、衝突発見に要する計算量は、6500 CPU コア・年 + 100 GPU・年であり、768 ビット(10 進 232 桁)の合成数の素因数分解に要した計算量 [KL10]や 768 ビットの離散対数の計算 [KL17]よりも数倍ほど大きな量であった。暗号技術評価委員会では、CRYPTREC の Web ページにおいてこの件に関する注意喚起を行った [C17a]。

---

[10] 『新たな電子政府用システムを構築する場合、より長いハッシュ値のものが使用できるのであれば、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。ただし、公開鍵暗号での仕様上、利用すべきハッシュ関数が指定されている場合には、この限りではない。』

[11] 『「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 情報セキュリティ政策会議決定、平成 24 年 10 月情報セキュリティ対策推進会議改定)を踏まえて利用すること。 http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf (平成 25 年 3 月 1 日現在)』

現在までに、SHA-1 の第二原像計算困難性及び原像計算困難性については実運用環境に影響を及ぼすほどの問題は見つかっていない。

CRYPTREC では、表 3 のように、SHA-1 の安全性に関する意見などを公表してきたが、NIST が示してきたような SHA-1 に関する利用期限については公表していない。

表 3: SHA-1 の衝突に係る主な年表

時期	出来事
1995 年 4 月	FIPS PUB 180-1 策定 (NIST)
2003 年 2 月	電子政府推奨暗号リスト策定 (CRYPTREC)
2004 年 8 月	SHA-1 への攻撃に対する短い声明 (NIST) [NT04]
2005 年 8 月	衝突探索アルゴリズムの論文発表 (Wang ら)
2006 年 4 月	SHA-1 への攻撃に対する声明 (NIST) [NT06]
2006 年 6 月	SHA-1 の安全性に関する見解 (CRYPTREC)
2008 年 4 月	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 に係る移行指針の策定 (NISC)
2011 年 1 月	SP 800-131A 策定(2015 年 10 月に Revision 1 に改定) (NIST)
2013 年 3 月	CRYPTREC 暗号リスト策定 (CRYPTREC)
2015 年 10 月	SHA-1 のフリースタート衝突の発見 (Stevens ら)
2017 年 2 月	SHA-1 の衝突発見(Stevens ら)

4.2. NISTにおける対応

(1) ハッシュ関数

NIST SP 800-57 Part 1 Revision 1では、SHA-1については、表4の通り記載されている。

表4: NISTにおけるハッシュ関数の安全性強度と利用範囲の状況（[NT16]から抜粋）

Security Strength	**Digital Signatures and hash-only applications**	**HMAC, Key Derivation Functions, Random Number Generation**
≤80	SHA-1	
112	SHA-224, SHA-512/224, SHA3-224	
128	SHA-256, SHA-512/256, SHA3-256	SHA-1
192	SHA-384, SHA3-384	SHA-224, SHA-512/224
≥256	SHA-512, SHA3-512	SHA-256, SHA-512/256, SHA-384, SHA-512, SHA3-512

また、NIST SP 800-131A Revision 1では、SHA-1については、表5の通り記載されている。

表5: NISTにおけるSHA-1の承認状況（[NT15c]から抜粋）

Hash Function	**Use**	
SHA-1	Digital signature generation	Disallowed, except where specifically allowed by NIST protocol-specific guidance.
	Digital signature verification	Legacy-use
	Non-digital signature applications	Acceptable

SHA-1 for digital signature generation:
SHA-1 may only be used for digital signature generation where specifically allowed by NIST protocol-specific guidance. For all other applications, SHA-1 **shall not** be used for digital signature generation.

SHA-1 for digital signature verification:
For digital signature verification, SHA-1 is allowed for **legacy-use**.

SHA-1 for non-digital signature applications:
For all other hash function applications, the use of SHA-1 is **acceptable**. The other applications include HMAC, Key Derivation Functions (KDFs), Random Bit Generation, and hash-only applications (e.g., hashing passwords and using SHA-1 to compute a checksum, such as the approved integrity technique specified in Section 4.6.1 of [FIPS 140]).

(2) 擬似乱数生成系

NIST SP 800-131A Revision 1では、FIPS 186-2 や ANS X9.62-1998で指定されている擬似乱数生成系については、表6 の通り記載されている。NISTの基準ではSHA-1 のHASH_DRBG及びHMAC_DRBG での利用が許容されているが、それ以外での利用は現在では承認されていない。

表 6: NIST における乱数生成器の承認状況 ([NT15c]から抜粋)

Description	Use
HASH_DRBG, HMAC_DRBG and CTR_DRBG	Acceptable
DUAL_EC_DRBG	Disallowed
RNGs in FIPS 186-2, ANS X9.31 and ANS X9.62-1998	Deprecated through 2015 Disallowed after 2015
Acceptable is used to mean that the algorithm and key length is safe to use; no security risk is currently known. **Deprecated** means that the use of the algorithm and key length is allowed, but the user must accept some risk. The term is used when discussing the key lengths or algorithms that may be used to apply cryptographic protection to data (e.g., encrypting or generating a digital signature).	

なお、現在、NIST SP 800-90C [NT16b]はドラフト版になっている。NICT SP 800-90B [NY16a]は最終版が 2018 年 1 月に公開されている。

(3) 鍵導出関数

NIST SP 800-131A Revision 1では、鍵導出関数について、表7 の通り記載されている。

表 7: NIST における鍵導出関数の承認状況 ([NT15c]から抜粋)

Algorithm	Use	
HMAC-based KDF	Acceptable	
CMAC-based KDF	Two-key TDEA-based KDF	Deprecated through 2015 Disallowed after 2015
	AES and Three-key TDEA	Acceptable
HMAC-based KDF (HMAC is the Keyed-Hash Message Authentication Code [FIPS 198-1]): The use of HMAC-based KDFs is **acceptable** using an **approved** hash function, including SHA-1. See Section 10 for discussions of the key lengths used with HMAC CMAC-based KDF: The use of two-key TDEA as the block cipher algorithm in a CMAC-based KDF is **deprecated** through December 31, 2015. Two-key TDEA **shall not** be used to derive keying material after December 31, 2015. The use of AES and three-key TDEA as the block cipher algorithm in a CMAC-based KDF is **acceptable**.		

5. 参考文献

[B15] M. Bellare, New Proofs for NMAC and HMAC: Security Without Collision-Resistance, Journal of Cryptology 28(4): 844-878 (2015). https://eprint.iacr.org/2006/043

[C00] CRYPTREC Report 2000, 2001年3月 http://www.cryptrec.go.jp/report/c12_sch_web.pdf

[C01] CRYPTREC Report 2001, 2002年3月 http://www.cryptrec.go.jp/report/c12_sch_web.pdf

[C02] CRYPTREC Report 2002, 2003年3月 http://www.cryptrec.go.jp/report/c12_sch_web.pdf

[C03a] 総務省・経済産業省, 電子政府における調達のために参照すべき暗号のリスト(電子政府暗号リスト), 2003年2月20日 http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_fy2005.pdf

[C05] CRYPTREC Report 2005 (第2版), 2006年5月17日 http://www.cryptrec.go.jp/report/c05_wat_final.pdf

[C06] ハッシュ関数(SHA-1)の安全性評価および攻撃手法整理, CRYPTREC技術報告書501番, 2006年3月, http://www.cryptrec.go.jp/estimation/rep_ID0501.pdf

[C07] 暗号技術検討会報告書(2006年度), 2007年3月 http://www.cryptrec.go.jp/report/c06_kentou_final.pdf

[C08a] CRYPTREC Report 2007, 2008年3月 http://www.cryptrec.go.jp/report/c07_wat_final.pdf

[C08b] 2007年度電子政府推奨暗号の利用方法に関するガイドブック, 2008年3月 http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf

[C10] 2009年度版リストガイド, 2010年3月 http://www.cryptrec.go.jp/report/c09_guide_final.pdf

[C13a] 総務省・経済産業省, 電子政府における調達のために参照すべき暗号のリスト(CRYPTREC暗号リスト), 2013年3月1日 http://cryptrec.go.jp/images/cryptrec_ciphers_list_2016.pdf

[C13b] CRYPTREC Report 2012, 2013年3月 http://www.cryptrec.go.jp/report/c12_sch_web.pdf

[C15a] SHA-1の安全性について, 平成27年12月18日 http://www.cryptrec.go.jp/topics/cryptrec_20151218_sha1_cryptanalysis.html

[C15b] 暗号技術検討会報告書(2015年度), 2016年3月 http://www.cryptrec.go.jp/report/c15_kentou_final.pdf

[C17a] SHA-1の安全性低下について, 平成29年3月1日 http://www.cryptrec.go.jp/topics/cryptrec_20170301_sha1_cryptanalysis.html

[C17b] CRYPTREC暗号の仕様書, 2017年6月 http://www.cryptrec.go.jp/method.html

[G14] P. Gaži, K. Pietrzak, and M. Rybár: The Exact PRF-Security of NMAC and HMAC, CRYPTO 2014, Lecture Notes in Computer Science vol. 8616, pp.113-130, 2014. https://eprint.iacr.org/2014/578.pdf

[I98] ISO/IEC 9798-3:1998, Information technology - Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques
[I12a] ISO 14533-1:2012, Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)
[I12b] ISO 14533-2:2012, Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)
[I17] ISO 14533-3:2017, Processes, data elements and documents in commerce, industry and administration - Long term signature profiles - Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)
[IK03] Tetsu Iwata and Kaoru Kurosawa: OMAC: One-Key CBC MAC. Fast Software Encryption 2013: 129-153.
https://eprint.iacr.org/2002/180.pdf
[J08a] JIS X 5092:2008, CMS 利用電子署名(CAdES)の長期署名プロファイル
Long term signature profiles for CMS advanced electronic signatures (CAdES)
[J08b] JIS X 5093:2008, XML 署名利用電子署名(XAdES)の長期署名プロファイル
Long term signature profiles for XML advanced electronic signatures (XAdES)
[J14] 独立行政法人情報処理推進機構, 承認されたセキュリティ機能に関する仕様(平成 26 年 4 月 1 日),
https://www.ipa.go.jp/security/jcmvp/documents/asf01.pdf
[K10] Hugo Krawczyk: Cryptographic Extraction and Key Derivation: The HKDF Scheme. CRYPTO 2010, Lecture Notes in Computer Science vol. 6223, pp. 631-648, 2010.
https://eprint.iacr.org/2010/264.pdf
[KA10] Akinori Kawachi, Akira Numayama, Keisuke Tanaka, Keita Xagawa: Security of Encryption Schemes in Weakened Random Oracle Models. Public Key Cryptography 2010: 403-419.
https://www.iacr.org/archive/pkc2010/60560406/60560406.pdf
[KL10] T. Kleinjung, K. Aoki, J. Franke, A. K. Lenstra, E. Thomé, J. W. Bos, P. Gaudry, A. Kruppa, P. L. Montgomery, D. A. Osvik, H. te Riele, A. Timofeev, and P. Zimmermann: Factorization of a 768-bit RSA modulus. CRYPTO 2010, Lecture Notes in Computer Science vol. 6223, pp. 333-350. 2010. https://eprint.iacr.org/2010/006.pdf
[KL17] T. Kleinjung, C. Diem, A. K. Lenstra1, C. Priplata, and C. Stahlke, Computation of a 768-bit prime field discrete logarithm
https://eprint.iacr.org/2017/067.pdf
[L09] G. Leurent, P. Q. Nguyen: How Risky Is the Random-Oracle Model?, CRYPTO 2009, Lecture Notes in Computer Science vol. 5677, pp. 445-464. 2009.
https://iacr.org/archive/crypto2009/56770440/56770440.pdf
[L14] 地方公共団体情報システム機構, LGPKI の移行方針について, 2014 年 12 月 19 日更新, http://www.lgpki.jp/unei/LGPKI_ikouhoushin_20141219.pdf
[ME10] 「電子署名法における暗号アルゴリズム移行研究会」報告書(2010 年 3 月)
http://www.meti.go.jp/policy/netsecurity/docs/esig/h21_esign-crypto-report.pdf

[ME11] 「電子署名法における暗号アルゴリズム移行研究会」報告書(2011 年 3 月)
http://www.meti.go.jp/policy/netsecurity/docs/esig/h22esig-alg-report.pdf
[MI09] 「公的個人認証サービスにおける暗号方式等の移行に関する検討会報告書」,
平成 21 年 1 月,
http://www.soumu.go.jp/main_sosiki/kenkyu/kouteki_kojin/pdf/090126_houkoku.pdf
[MI14] 総務省 行政管理局 政府認証基盤, 暗号アルゴリズムの移行について,
https://www.gpki.go.jp/documents/angouikou.html
[NC08a] 内閣官房情報セキュリティセンター (NISC), 情報セキュリティ政策会議 第 17 回会合 資料 3-1, 政府機関における安全な暗号利用の促進, 移行指針(案)に基づく暗号方式の移行完了までのスケジュール, 2008 年 2 月 4 日
http://www.nisc.go.jp/conference/seisaku/dai16/pdf/16siryou0301.pdf
[NC08b] 内閣官房情報セキュリティセンター (NISC), 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, 2008 年 4 月 22 日, 情報セキュリティ政策会議決定
http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf
[NC12a] 内閣官房情報セキュリティセンター (NISC), 情報セキュリティ政策会議 第 31 回会合 資料 3-1, 政府機関の暗号アルゴリズムに係る移行指針の改定概要, (参考) 政府機関における暗号移行スケジュール, 平成 24 年 11 月 1 日
http://www.nisc.go.jp/conference/seisaku/dai31/pdf/31shiryou0301.pdf
[NC12b] 内閣官房情報セキュリティセンター (NISC), 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, 2012 年 10 月 26 日改定, 情報セキュリティ対策推進会議決定
http://www.nisc.go.jp/active/general/pdf/angou_ikoushishin.pdf
[NT04] NIST Brief Comments on Recent Cryptanalytic Attacks, 2004 年 8 月,
https://csrc.nist.gov/News/2004/NIST-Brief-Comments-on-Recent-Cryptanalytic-Attack
[NT06] NIST Comments on Cryptanalytic Attacks on SHA-1, 2006 年 4 月,
https://csrc.nist.gov/News/2006/NIST-Comments-on-Cryptanalytic-Attacks-on-SHA-1
[NT08] NIST FIPS PUB 198-1, 2008 年 7 月
http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
[NT09] NIST Special Publication 800-108, 2009 年 10 月
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-108.pdf
[NT11] NIST Special Publication 800-135 Revision 1, 2011 年 12 月
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-135r1.pdf
[NT13] NIST Special Publication 800-56A Revision 2, 2013 年 5 月
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Ar2.pdf
[NT15a] NIST, Special Publication 800-90A Revision 1, 2015 年 6 月
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf
[NT15b] NIST FIPS PUB 180-4, 2015 年 8 月
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf

[NT15c] NIST Special Publication 800-131A Revision 1, 2015年11月
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf
[NT16] NIST, NIST Special Publication 800-57 Part 1 Revision 4, 2016年1月
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
[NT16a] NIST, NIST Special Publication 800-90B, 2018年1月
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90B.pdf
[NT16b] NIST, (Second DRAFT) NIST Special Publication 800-90C
http://csrc.nist.gov/publications/drafts/800-90/sp800_90c_second_draft.pdf
[N08] Akira Numayama, Toshiyuki Isshiki, Keisuke Tanaka: Security of Digital Signature Schemes in Weakened Random Oracle Models. Public Key Cryptography 2008: 268-287.
https://www.iacr.org/archive/pkc2008/49390269/49390269.pdf

[R12] RSA Laboratories, PKCS #1 v2.2: RSA Cryptography Standard, 2012年10月
https://www.emc.com/collateral/white-papers/h11300-pkcs-1v2-2-rsa-cryptography-standard-wp.pdf
[S15] 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
[S17a] Announcing the first SHA1 collision
https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html, February 23, 2017.
[S17b] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, Y. Markov, The first collision for full SHA-1,
CRYPTO 2017, Lecture Notes in Computer Science vol. 10401, pp. 570-596, 2017.
https://shattered.io/static/shattered.pdf, February 23, 2017.
[W05] X. Wang, Y. Lisa Yin, and H. Yu, Finding Collisions in the Full SHA-1, CRYPTO 2005, Lecture Notes in Computer Science vol. 3621, pp. 17-36, 2005.
https://www.iacr.org/archive/crypto2005/36210017/36210017.pdf

以上

CRYPTREC 暗号技術ガイドライン(SHA-1), CRYPTREC GL-2001-2013R1

発行日　2018 年 4 月 12 日　改定版 (CRYPTREC Report 2017 付録 6 版)
発行者

・〒184-8795
東京都小金井市貫井北町四丁目 2 番 1 号
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）
NATIONAL INSTITUTE OF
INFORMATION AND COMMUNICATIONS TECHNOLOGY
4-2-1 NUKUI-KITAMACHI,KOGANEI
TOKYO,184-8795 JAPAN

・〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
独立行政法人情報処理推進機構
（技術本部 セキュリティセンター 暗号グループ）
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
2-28-8 HONKOMAGOME,BUNKYO-KU
TOKYO,113-6591 JAPAN

付録 7

学会等での主要攻撃論文発表等一覧

目次

1. 具体的な暗号の攻撃に関する発表

表 1 に具体的な暗号の攻撃に関する発表のリストをカテゴリー別に示す。★は電子政府推奨暗号の安全性に直接関わる技術動向、☆はその他の注視すべき技術動向である。

表 1 具体的な暗号の攻撃に関する発表

公開鍵暗号		頁
★	Computation of a 768-Bit Prime Field Discrete Logarithm [Eurocrypt 2017]	91
☆	A Kilobit Hidden SNFS Discrete Logarithm Computation [Eurocrypt 2017]	91
	A Reaction Attack on the QC-LDPC McEliece Cryptosystem [PQCrypto2017]	–
	An Updated Security Analysis of PFLASH [PQCrypto 2017]	–
☆	A Low-resource Quantum Factoring Algorithm [PQCrypto 2017]	93
☆	Quantum Algorithms for Computing Short Discrete Logarithms and Factoring RSA Integers [PQCrypto 2017]	93
	Cryptanalysis of RLWE-Based One-Pass Authenticated Key Exchange [PQCrypto 2017]	–
	A Hybrid Lattice Basis Reduction and Quantum Search Attack on LWE [PQCrypto 2017]	–
	Improved Attacks for Characteristic-2 Parameters of the Cubic ABC Simple Matrix Encryption Scheme [PQCrypto 2017]	–
	Key Recovery Attack for All Parameters of HFE- [PQCrypto 2017]	–
	Practical Key Recovery Attack for ZHFE [PQCrypto 2017]	–
	LPN Decoded [CRYPTO 2017]	
★	The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli [ACM CCS 2017]	97
	Revisiting the Expected Cost of Solving uSVP and Applications to LWE [Asiacrypt 2017]	–
	Coded-BKW with Sieving [Asiacrypt 2017]	–
	Grover Meets Simon - Quantumly Attacking the FX-construction [Asiacrypt 2017]	–
	Quantum Multicollision-Finding Algorithm [Asiacrypt 2017]	–
	An Efficient Quantum Collision Search Algorithm and Implications on Symmetric Cryptography [Asiacrypt 2017]	–
	Quantum Resource Estimates for Computing Elliptic Curve Discrete Logarithms [Asiacrypt 2017]	–
ブロック暗号		頁
★	A New Structual-Differential Property of 5-Round AES [Eurocrypt 2017]	92
☆	New Impossible Differential Search Tool from Design and Cryptanalysis Aspects Revealing Structural Properties of Several Ciphers [Eurocrypt 2017]	93

2. Eurocrypt 2017 の発表

2.1. Eurocrypt 2017 の発表（1 日目）

Computation of a 768-Bit Prime Field Discrete Logarithm [Eurocrypt 2017]

Thorsten Kleinjung, Claus Diem, Arjen K. Lenstra, Christine Priplata, Colin Stahlke

NFS（数体ふるい法）により768ビットの素体上の離散対数問題の計算に成功したという報告であり、これまでの素体上の離散対数問題の記録（596 ビットの素体上）から大きく進展した。計算時間はトータルで約 5300 コア・年（Intel Xeon E5-2660 2.2GHz）。報告者らの大学のクラスタ環境で計算に 2015 年の 5 月から 12 月迄をほぼ費やしたとのこと。この研究成果は、素体上の離散対数問題の困難さに安全性の根拠を置く公開鍵暗号に対する既存の安全性評価結果に大きな進展と新たな知見を与えるものである。一方、CRYPTREC 暗号リスト掲載の公開鍵暗号で素体上の離散対数問題の困難さに安全性の根拠を置くものとして、署名の DSA と鍵共有の DH が該当するが、素数のサイズが 2048 ビット以上であれば本報告の結果は直ちにその安全性に影響を与えるものではない。

A Kilobit Hidden SNFS Discrete Logarithm Computation [Eurocrypt 2017]

Joshua Fried, Pierrick Gaudry, Nadia Heninger, Emmanuel Thome

SNFS（特殊数体ふるい法）により、1024 ビットの特殊な素体上での離散対数問題の計算に成功したという報告で、キロビットサイズの素体上の離散対数問題の計算としては世界初。計算時間はトータルで約 400 コア・年（Intel Xeon E5-2650 2.0GHz）。報告者らのクラスタ環境でオープンソース CADO-NFS で実装し、計算に 2 ケ月ほど費やしたとのこと。素数pは DSA のパラメータ推奨に沿って、p-1 がハッシュ値長以下（本報告では 160 ビット）の素因数を持つが、p に SNFS で離散対数問題が計算可能となるように、約 25 年前に提案された Gordon の方法により、p にトラップドアが仕掛けられている。提案当時は比較的小さな（トラップドアを持つ）パラメータしか生成できなかったが、その後の計算機の進歩により、今回のパラメータは十分な大きさを持ち、p を見ただけではトラップドアが仕掛けられていることを見破るのは計算量的に困難なものとなっている。署名の DSA、鍵共有の DH を用いる際には、上記のトラップドアを持たないパラメータを利用する必要があるが、上述のようにpを見ただけではトラップドアが仕掛けられているか否かを見分けることは困難である。本トラップドアを防ぐには、ランダムに生成されたことが検証可能な素数 p を用いる必要がある。

2.2. Eurocrypt 2017 の発表(2 日目)

Conditional Cube Attack on Reduced-Round Keccak Sponge Function [Eurocrypt 2017]

Senyang Huang, Xiaoyun Wang, Guangwu Xu, Meiqin Wang, Jingyuan Zhao

米国標準ハッシュ関数 SHA-3(2015 年制定)の元となったハッシュ関数 Keccak について条件付きキューブ攻撃を提案した。Keccak-MAC へのキーリカバリー攻撃で Keccak-MAC-256/384/512 について 7/6/5 段の結果を初めて示し、Keccak-MAC-128 については計算量とデータ量を削減した。また、Keyak(Keccak sponge function ベースの AE)へのキーリカバリー攻撃で、Keyak-128 について 8 段の結果を初めて示し、7 段については計算量とデータ量を削減した。更に、Keccak sponge function への識別攻撃で、Keccak-384/512 について 7/6 段に結果を初めて示し、Keccak-224 については従来の攻撃可能段数(7 段)での計算量とデータ量を削減した。ただし、(b=1600 の)Keccak/SHA-3 のフルスペックの段数は 24 段であり、Keccak/SHA-3 の安全性に直ちに影響を与えるものではない。

New Collision Attacks on Round-Reduced Keccak [Eurocrypt 2017]

Kexin Qiao, Ling Song, Meicheng Liu, Jian Guo

米国標準ハッシュ関数 SHA-3(2015 年制定)の元となったハッシュ関数 Keccak に対する新たな衝突攻撃を提案した。Keccak-224 の攻撃可能段数を従来の 4 段から 5 段に伸ばした。また、Keccak-256 の従来の攻撃可能段数(4 段)での解読計算量を削減した。また、SHA3 ファミリーの一つである SHAKE128 の 5 段に対する攻撃を初めて示した。ただし、(b=1600 の) Keccak/SHA-3 のフルスペックの段数は 24 段であり、Keccak/SHA-3 の安全性に直ちに影響を与えるものではない。

2.3. Eurocrypt 2017 の発表(3 日目)

A New Structual-Differential Property of 5-Round AES [Eurpcrypt 2017]

Lorenzo Grassi, Christian Rechberger and Sondre Ronjom

米国標準ブロック暗号 AES(2000 年制定)の 5 段の識別子 を示した。これまでは AES の識別子は 4 段のものは知られていたが 5 段のものは初めてであり、AES の解読可能な段数が進展した。ただし、128 ビット鍵の AES のフルスペックの段数は 10 段であり、今回の結果は AES の安全性に直ちに影響を与えるものではない。

2.4. Eurocrypt 2017 の発表（4 日目）

New Impossible Differential Search Tool from Design and Cryptanalysis Aspects Revealing Structural Properties of Several Ciphers [Eurocrypt 2017]

Yu Sasaki, Yosuke Todo

ブロック暗号の設計と解析の両面で役立つ不能差分を探索する新しいツールを提案し、Midori128、LILLIPUT、Minalpher の不能差分の段数を伸ばし、ARIA、MIBS の段数は従来と同じで新たな不能差分を示した。新しいツールは MILP（Mixed Integer Linear Programing：混合整数線形計画法）を用いてこれまでの差分探索ツールを変更することで実現される。Cui らにより同様の研究が ePrint に投稿されているが、基本アイデアは同じであるものの本研究では不能差分攻撃により特化しており、8ビット S-box の暗号に対して新しい結果を提示している。

3. PQCrypto 2017 の発表

3.1. PQCrypto 2017 の発表（2 日目）

A Low-resource Quantum Factoring Algorithm [PQCrypto 2017]

Daniel J. Bernstein, Jean-François Biasse, Michele Mosca

標準的なヒューリスティックを仮定すると、たった $(\log N)^{\frac{2}{3}+o(1)}$ 量子ビットしか用いずに時間 $L^{q+o(1)}$ 内に整数を素因数分解するアルゴリズムを示す。ただし、$L = \mathrm{e}^{(\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}}$ であり、$q = \sqrt[3]{8/3} \approx 1.387$ である。量子以前では既知の最も小さい漸近計算量は $L^{p+o(1)}$（ただし $\mathrm{p} > 1.9$）である。新アルゴリズムの時間計算量は、漸近的には Shor のアルゴリズムより悪いが、必要な量子ビット数は漸近的には少なくてすむため、より早い時期に物理的な実装が可能かもしれない。

Quantum Algorithms for Computing Short Discrete Logarithms and Factoring RSA Integers [PQCrypto 2017]

Martin Ekerå, Johan Håstad

対数が小さい場合に離散対数を計算する Ekerå の量子アルゴリズムを一般化することにより、アルゴリズムを繰り返す回数と、アルゴリズムの計算量と量子計算機の制約との間の様々なトレードオフを可能とした。更に RSA 合成数の素因数分解問題やサイド情報を利用して巡回群位数を求める問題等、他の重要な問題を離散対数問題に帰着する応用を示す。これにより、量子計算機の制約が緩和されるという意味において、Shor のアルゴリズムより単純な素因数分解アルゴリズムを構成することができる。n ビット整数を素因数分解する場合、Shor のアルゴリズムでは指数は 2n ビットとなるが、本アルゴリズムでは n/2 ビットより少し大きいくらいである。

4. ACNS 2017 の発表

4.1. ACNS 2017 の発表(2 日目)

A Practical Chosen Message Power Analysis Approach Against Ciphers with the Key Whitening Layers [ACNS 2017]

Chenyang Tu, Lingchen Zhang, Zeyi Liu, Neng Gao, Yuan Ma

Feistel-SP 構造を持ち key whitening 処理を含んでいるブロック暗号の、Loop Architecture を用いた実装に対するサイドチャネル攻撃の方法を提案している。Loop Architecture 実装では、key whitening 処理は単独で実行されないため、key whitening 処理の消費電力は全体の消費電力から検出することが難しく、whitening key をラウンド鍵やその他の中間値から分離することが難しいことから、電力解析を困難にしている。この論文では Chosen Message DPA によって攻撃する方法を提案している。key whitening を含むアルゴリズムには CLEFIA, Camellia, DESL, PRINCE が挙げられるが、この論文では CLEFIA, Camellia の Loop Architecture 実装に対する攻撃を実際に成功させ、key whitening は DPA に関してはセキュリティを向上させないと結論付けている。

5. Crypto 2017 の発表

5.1. Crypto 2017 の発表(1 日目)

Non-Full Sbox Linearization: Applications to Collision Attacks on Round-Reduced Keccak [CRYPTO 2017]

Ling Song, Guohong Liao, Jian Guo

Keccak の縮退版に対する衝突攻撃が示された。シンガポール南洋理工大学と中国華南師範大学のチームが、これまでの記録を 1 段しのぐ、5 段 Keccak-224 と 6 段 Keccak 衝突チャレンジの衝突攻撃に成功した。これらの結果は、Keccak の置換における非線型層の代数的性質を注意深く調べ、線型化を適用することにより得られた。まだ大分マージンはあるが、今後の攻撃の進展には注意が必要である。

5.2. Crypto 2017 の発表(2 日目)

The First Collision for Full SHA-1 [CRYPTO 2017]

Marc Stevens, Elie Bursztein, Pierre Karpman, Ange Albertini, Yarik Markov

オランダ国立情報工学・数学研究所(CWI: Centrum Wiskunde & Informatica)および Google 研究

所のチームが、SHA-1 の衝突を、1995 年の SHA-1 標準制定以来初めて発見した。Eurocrypt 2013 の Stevens による理論的攻撃に基づいており、理論的な計算量は 2^{61} 回の SHA-1 呼び出しと見積もられているが、今回の実際の計算量は $2^{63.1}$ 回の SHA-1 呼び出しであり、約 6500CPU 年と 100GPU 年かかった。本結果に関する CRYPTREC の見解については、CRYPTREC ホームページ上に公開済であり、より安全なハッシュ関数への移行を推奨している。

6. FDTC 2017 の発表

A Practical Fault Attack on ARX-like Ciphers with a Case Study on ChaCha20 [FDTC2017]

S.V. Dilip Kumar, Sikhar Patranabis, Jakub Breier, Debdeep Mukhopadhyay, Shivam Bhasin, Anupam Chattopadhyay, Anubhab Baksi

インド/シンガポールの研究チームが、Android 端末に標準搭載の Web ブラウザ Google Chrome で HTTPS 通信に標準採用された共通鍵暗号(ストリーム暗号)ChaCha20 に対してフォールト攻撃(レーザー攻撃)を初めて成功させた。提案攻撃手法は ChaCha20 と同種の構造(ARX 構造)を持つストリーム暗号に適用可能で、8 ビットマイクロコントローラ上で実証実験を行っている。これにより ChaCha20 の実装でフォールト攻撃へ耐性を持たせるには適切な対策を講じる必要があることが初めて示された。

7. CHES 2017 の発表

7.1. CHES 2017 の発表(1 日目)

How Improved Blind Side-Chanel Analysis by Exploitation of Joint Distributions of Leakages [CHES2017]

Christophe Clavier, Leo Reymaud

本論文では、Linge らによるリーク情報の結合分布を利用するブラインド攻撃(リーク情報のみを用いた攻撃)を再考している。Linge の距離ベースの分布の比較より、最尤(ML)アプローチの方が効率的であること、その攻撃が一次ブールマスキングによって保護された実装に容易に適用できることを、様々なアプリケーション(AES ベースのセッション鍵導出関数、3-DES を用いた MAC、等)で、シミュレーション及び実際のデバイス上での実験で実証し、また対策方法も提案している。

How SGX Amplifies the Power of Cache Attacks [CHES2017]

Ahmad Moghimi, Gorka Irazoqui, Thomas Eisenbarth

インテルの SGX(ソフトウェア保護拡張)はプロセッサ内で信頼できる実行環境を構築することが

狙いであるが、サイドチャネル攻撃を考慮していないため、CacheZoom と名付けた著者らの攻撃ツールによって、SGX エンクレーブ（飛び領土）の全てのメモリアクセスを仮想的に追跡できるとのこと。コンセプト証明のため、AES の実装に対してキャッシュ攻撃による鍵回復をデモンストレーションし、これまでの攻撃では数百回の測定を必要とするのに対し、わずか 10 回の測定で T-table ベース実装の AES から鍵回復に成功している。

7.2. CHES 2017 の発表（3 日目）

A Systematic Approach to the Side-Channel Analysis of ECC Implementations with Worst-Case Horizontal Attacks [CHES2017]

Romain Poussier, Yuanyuan Zhou, Francois-Xavier Standaert

ベルギー/オランダの研究チームが、楕円曲線暗号の主要処理である「楕円曲線上のスカラー倍演算」の強力な実装攻撃で知られる HDPA（Horizontal Differential Power Attack）に対するシステマティックな強度評価手法を提案し、それを実現するツールを開発した。提案高度評価手法／ツールにより、評価者の立場からは安全性の上界を、設計者の立場からは対策技術の効果をシステマティックに評価可能となる（補：CRYPTREC 暗号リストに掲載の暗号技術の中では、ECDSA(署名),ECDH（鍵共有）に適用可能)。

Sliding Right into Disaster : Left-to-Right Sliding Windows Leak [CHES2017]

Daniel J.Bernstein, Joachim Breitner, Daniel Genkin, Leon Groot Bruinderink, Nadia Heninger, Tanja Lange, Christine van Vredendaal, Yuval Yarom

本論文ではGnuPGにて用いられるコードに基づいた汎用的な暗号ライブラリLibgcryptで実装された RSA-1024 の完全な攻撃をデモンストレーション（実証）している。Libgcrypt は冪剰余演算に left-to-right 方法のスライディングウィンドウ（SW）方式を使用している。本論文の攻撃は、left-to-right の SW 方式の自乗と乗算では、right-to-left よりも冪指数に関するより多くの情報を著しくリークすることを利用し、部分鍵再構成の Heninger-Shacham のアルゴリズムを拡張することで RSA-1024 の効率的な完全鍵回復を実現している。

8. PROOFS 2017 の発表

Symbolic Approach for Side-Channel Resistance Analysis of Masked Assembly Codes [PROOFS2017]

Ines Ben El Ouahma, Quentin Meunier, Karine Heydemann, Emmanuelle Encrenaz

本論文ではマスキングされたプログラムのサイドチャネルロバスト性を検証するための記号的手法を提案している。ソフトウェアでは、通常、ソースコードレベルでマスキングされるが、コンパイルと最適化が影響を与える可能性があるため、分析はアセンブリレベルで行う。提案手法では、定義さ

れた分布推論規則を用いて中間計算値が秘密変数と統計的に独立であることを検証する。マスキングされた AES の第一ラウンドで検証し、安全なソースコードがアセンブリ実装されると安全ではなくなることがあることを示している。

9. ACM CCS 2017 の発表

9.1. ACM CCS 2017 の発表(2 日目)

Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2 [ACM CCS 2017]

Mathy Vanhoef, Frank Piessens

本論文は、2017 年 10 月 16 日に Wi-Fi のハンドシェイクプロトコル WPA/WPA2 に対して発表された攻撃 KRACKs (key reinstallation attacks) に関する論文である。本攻撃はハンドシェイクプロトコルのメッセージ再送を悪用しクライアントに鍵を再利用させる。ハンドシェイクプロトコルの仕様上の問題が原因のため、特定の実装や製品に関わらず影響がある。著者は、攻撃手順を示し、具体的な暗号スイート/仕様/実装に対する影響を確認し、本攻撃に関する注意(対策等)を述べている。

9.2. ACM CCS 2017 の発表(3 日目)

The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli [ACM CCS 2017]

Matus Nemec, Marek Sys and Petr Svenda, Dusan Klinec, Vashek Matyas

本論文は、Coppersmith の提案した攻撃手法を応用し、特に RSALib が提供する RSA モジュールに適用されていると思われる設定状況に対して、効果的な攻撃が行えることを示した。この論文の解析が成功した要因としては、ある特定の生成式に基づき鍵生成が行われていた(と想定される)こと、そのことにより式変形により、仮想的な等価式を用いて全数探索が可能であるほどの小さなパラメータを用いた解析が可能になってしまったことが考えられる。著者らは、公開情報のみを用いて、特に追加的な前提条件を設けることなく、Coppersmith の攻撃を適用することにより、探索・推定を可能とした。また、RSA モジュールが今回の解析が適用可能か否かをチェックできるツールをフリーで公開している。解析の対処策としては、別のライブラリを用いて生成した鍵のインポート，より影響の少ない鍵長(例として 3072 ビットを挙げていた)への変更、リスクマネージメントの強化などを挙げている。

10. Asiacrypt 2017 の発表

10.1. Asiacrypt 2017 の発表(1 日目)

The ship has sailed: the NIST Post-Quantum Cryptography "Competition" [ASIACRYPT 2017, Invited Lecture]

Dustin Moody

米国 NIST(National Institute of Standards and Technology: 国立標準技術研究所)による量子計算機に耐性を持つ暗号(PQC: Post Quantum Cryptography)公募が 11 月 30 日に締め切られ、その内訳が下記の通り発表された。

	電子署名	鍵カプセル化/暗号化	合計
格子ベース	4	24	28
符号ベース	5	19	24
多変数多項式ベース	7	6	13
ハッシュベース	4	0	4
その他	3	10	13
合計	23	59	82

既に NIST ホームページ上に仕様書が公開され、評価が始まっており、2018 年 4 月 12 日～13 日にアメリカ・フロリダ州で第一回 PQC 標準化会議が開催される。

Automatic Search of Bit-Based Division Property for ARX Ciphers and Word-Based Division Property [Asiacrypt 2017]

Ling Sun, Wei Wang, Meiqin Wang

Division property を自動的に発見するツールを開発し、いくつかの暗号に適用し、これまでの記録を凌ぐ結果を得た。ARX 暗号に対しては、SAT 問題に基づき、ビットレベルの性質伝搬を追跡することにより、SHACAL-2 の 17 段識別(4 段増)および LEA の 8 段識別(1 段増)を構成した。ワードベースの division property に関しては、SMT 問題に基づくことにより、CLEFIA の 10 段識別(1 段増)を構成し、Whirlpool の 4/5 段識別のデータ計算量を改良し、Rijndael-192/256 の 6 段識別(2 段増)を示した。CLEFIA については、新しい識別により integral 攻撃を 1 段改良した。

Yoyo Tricks with AES [Asiacrypt 2017]

Sondre Rønjom, Navid Ghaedi Bardeh, Tor Helleseth

SPN の新しい基本的性質を導入し、適応的選択暗号文/平文の設定において、3 段から 5 段の AES に対する鍵に依存しないヨーヨー識別を初めて構成した。これまでのすべての記録を更新し、必要なデータは各々3, 4, $2^{25.8}$ であり、差分を観測する以外には本質的に計算を必要としない。更

に、6 段 AES に対する初めての鍵独立な識別を、平文および暗号文における不可能ゼロ差分を保つヨーヨー・ゲームに基づいて構成した。データ量は $2^{122.83}$ の平文/暗号文ペアを必要とし現実的ではないが、対応する差分を観測する以外は本質的な計算は必要としない。また、5 段 AES に対して、$2^{11.3}$ のデータおよび 2^{31} の計算量しか必要としない鍵回復攻撃を示した。

Collisions and Semi-Free-Start Collisions for Round-Reduced RIPEMD-160 [Asiacrypt 2017]

FukangLiu, Florian Mendel, Gaoli Wang

RIPEMD-160 に対する衝突攻撃および semi-free-start 衝突攻撃が発表された。Asiacrypt 2013 において Mendel らが未解決問題としていた、RIPEMD-160 の段差分確率を理論的に計算する方法を示し、Mendel らの差分パスを自動的に発見する方法を改良し、30 段 RIPEMD-160 の衝突を 2^{67} の計算量で発見することができる。これは RIPEMD-160 の縮退版に対する初めての衝突攻撃である。更に、ASIACRYPT 2013 の RIPEMD-160 の最初の 36 段に対する semi-free-start 衝突攻撃を改良することにより、計算量を $2^{70.4}$ から $2^{55.1}$ に改良した。

11. FSE 2018 の発表

11.1. FSE 2018 の発表（1 日目）

Rotational-XOR Cryptanalysis of Reduced-round SPECK [FSE 2018]

Yunwen Liu, Glenn De Witte, Adrian Ranea, Friedrich Wiemer

CRYPTREC が 2017 年度に発行した『CRYPREC 暗号技術ガイドライン（軽量暗号）』で評価対象となっている米国 NSA が設計した軽量暗号「SPECK」について、SPECK32/64（ブロック長 32、鍵長 64 の SPECK）で特定の弱い鍵に対する 9 段の差分特性より高い確率を持つ 10/11/12 段の RX（Rotational-XOR）特性による識別子（Distinguisher）が示された。また SPECK48（ブロック長 48、鍵長 72or96 の SPECK）では 15 段の識別子が示された。ただし、SPECK32/64 のフルスペックは 22 段（SPECK48 は 22/23 段）であるため今回の発表は SPECK32/64（SPECK48）の安全性に対して直ちに影響のあるものではない。

A Security Analysis of Deoxys and Its Internal Tweakable Block Ciphers [FSE 2018]

Carlos Cid, Tao Huang, Thomas Peyrin, Yu Sasaki, Ling Song

認証暗号の国際コンペである『CAESAR』の第 3 次審査を通過した認証暗号 Deoxys とその内部で利用されている Tweakable ブロック暗号の Deoxys-BC-256、Deoxys-BC-384 について新たな安全性解析結果を示している。矩形攻撃（Rectangle attack）により、Deoxys-BC-256/Deoxys-BC-384 がフルラウンド 14 段/16 段のうち 10/13 段まで攻撃可能であること、また、認証暗

号 Deoxys-I-128-128/Dexys-II-128-128 がフルラウンド 14 段のうち 9 段まで、認証暗号 Deoxys-I-256-128/Deoxys-II-256-128 がフルラウンド 16 段のうち 12 段まで、攻撃可能であることが示された。尚、FSE 2018 開催中の Rump session において認証暗号コンペ CAESAR における第4次選考結果(ファイナリスト)が公式にアナウンスされ、Deoxys はファイナリストの一つとなった。

Understanding RUP Integrity of COLM [FSE 2018]

Nilanjan Datta, Atul Luykx, Bart Mennink, Mridul Nandi

認証暗号の国際コンペである『CAESAR』の第3次審査を通過した認証暗号 COLM について新たな安全性解析結果を示している。RUP(release of unverified plaintext)条件での安全性を定義し、COLM が持つ二重の暗号化層の中間に位置する線形混合関数を、単純な排他的論理和に置き換えた場合と、任意の線形混合関数に一般化した場合(COLM タイプ構造と呼称)に対しての攻撃(偽造)を示している。またその結果から、実際の COLM 及び COLM タイプ構造で RUP-secure とするための方策を 2 つ提示している。尚、FSE 2018 開催中の Rump session において認証暗号コンペ CAESAR における第 4 次選考結果(ファイナリスト)が公式にアナウンスされ、COLM はファイナリストの一つとなった。

11.2. FSE 2018 の発表(2 日目)

Cryptanalysis of 48-step RIPEMD-160 [FSE 2018]

Gaoli Wang, Yanzhao Shen, Fukang Liu

『運用監視暗号リスト』に掲載されているハッシュ関数「RIPEMD-160」の「Semi-free-start」衝突(=攻撃者に有利な特別な条件下での衝突攻撃の一種)で、これまで 42 ステップまで攻撃可能であったものを、46 ステップまで攻撃可能であることが示された。ただし、RIPEMD-160 はフルスペックで 80 ステップあり、今回の発表は RIPEMD-160 の安全性に対して直ちに影響のあるものではない。尚、RIPEMD-160 は仮想通貨で有名なビットコインで利用されているハッシュ関数の一つである。

Preimage Attacks on the Round-reduced Keccak with Cross-linear Structures [FSE 2018]

Ting Li, Yao Sun, Aaodong Liao, Dingkang Wang

『推奨候補暗号リスト』に掲載されている米国標準ハッシュ関数 SHA-3 ファミリーの「SHA3-256」、「SHAKE-256」への原像攻撃(=与えられたハッシュ値を出力するメッセージを探索する攻撃)で、これまで 3 段では共に 2^{190} 程度の計算量で攻撃可能であったものを、計算量を削減し、2^{151}、2^{153} の計算量で攻撃可能であることが示された。ただし、SHA3-256/SHAKE-256 のフルスペックは 24 段であるため、今回の発表は SHA3-256/SHAKE-256 の安全性に対して直ちに影響のあるものではない。

11.3. FSE 2018 の発表（3 日目）

Human-readable Proof of the Related-Key Security of AES-128 [FSE 2018]

Khoongming Khoo,Eugene Lee, Thomas Peyrin, Siang Meng Sim

『電子政府推奨暗号リスト』に掲載されている米国標準のブロック暗号「AES」について、これまでは計算機探索により証明されていた関連鍵攻撃における差分パスの最小のアクティブ S-BOX 数について、AES-128（128 ビット鍵 AES）の関連鍵攻撃モデルにおいて初めて計算機探索以外による証明がなされた。これにより AES-128 の鍵関連攻撃に対する安全性が証明された。

CRYPTREC Report 2017
暗号技術評価委員会報告 CRYPTREC RP-2000-2017

発行日　2018年 6月30日　第1版
発行者
・〒184-8795
東京都小金井市貫井北町四丁目2番1号
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）
NATIONAL INSTITUTE OF
INFORMATION AND COMMUNICATIONS TECHNOLOGY
4-2-1 NUKUI-KITAMACHI,KOGANEI
TOKYO,184-8795 JAPAN

・〒113-6591
東京都文京区本駒込二丁目28番8号
独立行政法人情報処理推進機構
（技術本部 セキュリティセンター 暗号グループ）
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
2-28-8 HONKOMAGOME,BUNKYO-KU
TOKYO,113-6591 JAPAN