CRYPTREC Report 2010

平成 23 年 3 月

独立行政法人情報通信研究機構
独立行政法人情報処理推進機構

「暗号方式委員会報告」

目次

はじめに

本報告書は、総務省及び経済産業省が主催している暗号技術検討会の下に設置されている暗号方式委員会の 2010 年度活動報告である。

電子政府(e-Government)での利用に資する暗号技術のリストアップを目的として、暗号技術監視委員会の前身とも言える暗号技術評価委員会では、2000 年度から 2002 年度の 3 年間をかけて、暗号技術評価活動(暗号アルゴリズムの安全性評価)を推進してきた。その結果、2003 年 2 月に、暗号技術検討会を主催する総務省、経済産業省が電子政府推奨暗号リストを公表する運びとなり、暗号技術評価活動も一区切りを迎えた。2003 年度からは、電子政府推奨暗号の安全性の監視等を行う「暗号技術監視委員会」と電子政府推奨暗号を実装する暗号モジュールの評価基準・試験基準の作成等を行う「暗号モジュール委員会」の 2 委員会の体制になった。

2009 年度からは、それぞれ「暗号方式委員会」及び「暗号実装委員会」に名称を変更した上で、新たに「暗号運用委員会」を設置して、電子政府推奨暗号の適切な運用についてシステム設計者・運用者の観点から調査・検討を行うための活動を開始した。

暗号方式委員会は、旧暗号技術監視委員会と同じく、独立行政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おり、技術面を中心とした活動を担当している。一方、ユーザの立場でかつ政策的な判断を加えて結論を出しているのが暗号技術検討会であり、相互に協調して電子政府の安全性及び信頼性を確保する活動を推進している。

2010 年度は、「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）」に応募された 6 件の暗号技術に関して、安全性評価を行った。2011 年 3 月には、「CRYPTREC シンポジウム 2011」を開催し、応募された暗号技術の安全性評価に関する事務局見解が発表され、委員及びシンポジウム参加者からの質疑応答を受けた。その結果、6 件中、4 件の暗号技術に関しては、第 2 次評価を継続することとなった。2011 年度の暗号方式委員会では、公募された暗号技術と既存の電子政府推奨暗号リスト掲載暗号の比較評価（第 2 次評価）をはじめとして、電子政府推奨暗号リストの改訂に関する事項を審議していく予定である。暗号技術調査ワーキンググループ(WG)では、昨年度に引き続き、リストガイド WG を開催し、暗号鍵管理に関する調査を行った。

電子政府推奨暗号の監視は、暗号が使われ続ける限り継続していかねばならない活動である。また、この活動は、暗号実装委員会及び暗号運用委員会との連携を保ちつつ、暗号技術やその実装及び運用に係る研究者及び技術者等の多くの関係者の協力を得て成り立っているものであることを改めて強調しておきたい。

末筆ではあるが、本活動に様々な形でご協力下さった関係者の皆様に深甚な謝意を表する次第である。

暗号方式委員会　委員長　今井 秀樹

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章は暗号方式委員会及び監視活動等について説明してある。第2章は電子政府推奨暗号リスト改訂に係る暗号技術評価に関する報告である。第3章は今年度の監視活動、調査等の活動概要の報告である。第4章は暗号方式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「暗号方式委員会」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、電子政府推奨暗号の仕様書は、CRYPTREC事務局（総務省、経済産業省、独立行政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。

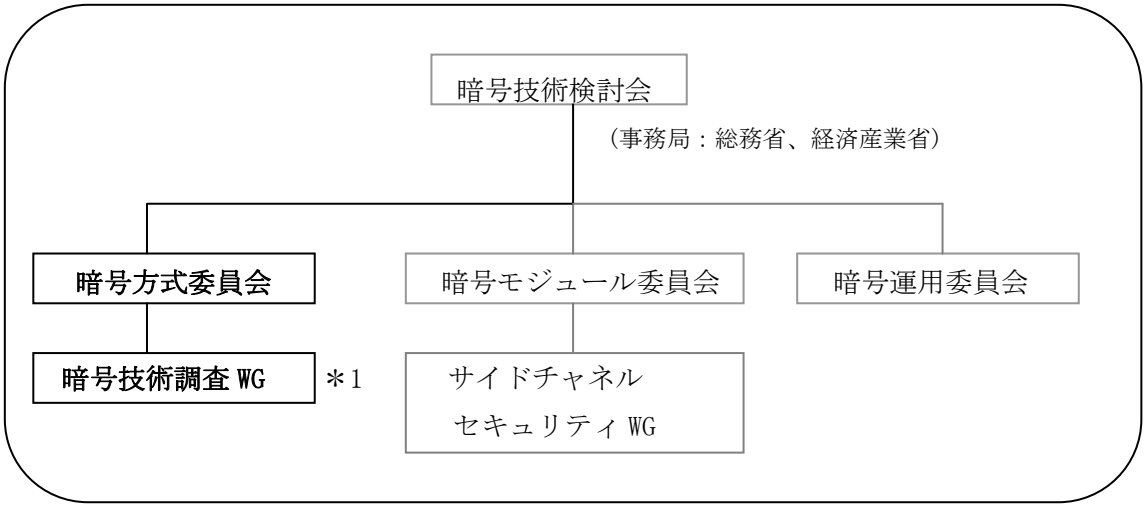
【問合せ先】　info@cryptrec.go.jp

委員会構成

暗号方式委員会(以下「方式委員会」)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、独立行政法人情報通信研究機構(NICT)と独立行政法人情報処理推進機構(IPA)が共同で運営する。方式委員会は、暗号技術の安全性及び信頼性確保の観点から、電子政府推奨暗号の監視、電子政府推奨暗号に関する暗号アルゴリズムを主な対象とする調査・検討を適宜行う等、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、将来的には、電子政府推奨暗号リストの改訂に関する調査・検討を行う予定であり、暗号技術関連学会や国際会議等を通じての暗号技術に関する情報収集、関係団体の Web サイトの監視等を行う。

暗号技術調査ワーキンググループ(以下「調査 WG」)は、方式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、方式委員会活動に関連して必要な項目について、方式委員会の指示のもとに調査・検討活動を担当する作業グループである。方式委員会の委員長は、実施する調査・検討項目に適する主査及びメンバーを、方式委員会及び調査 WG の委員の中から選出し、調査・検討活動を指示する。主査は、その調査・検討結果を方式委員会に報告する。平成 21 年度、方式委員会の指示に基づき実施されている調査項目は、「電子政府推奨暗号リストに関するガイドの作成」である。

方式委員会と連携して活動する「暗号実装委員会」及び「暗号運用委員会」も、方式委員会と同様、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。



＊1 今年度実施されている調査項目：

・電子政府推奨暗号リストに関するガイドの作成

図 1　CRYPTREC 体制図

委員名簿

暗号方式委員会

委員長	今井 秀樹	中央大学 教授
顧問	辻井 重男	中央大学研究開発機構　教授
委員	太田 和夫	国立大学法人電気通信大学 大学院 教授
委員	金子 敏信	東京理科大学 教授
委員	佐々木 良一	東京電機大学 教授
委員	高木 剛	国立大学法人九州大学 大学院 教授
委員	田中 秀磨	独立行政法人情報通信研究機構 グループリーダー
委員	松本 勉	国立大学法人横浜国立大学 大学院 教授
委員	山村 明弘	国立大学法人秋田大学 大学院 教授
委員	渡辺 創	独立行政法人産業技術総合研究所 副研究センター長

暗号技術調査ワーキンググループ

主査	手塚 悟	東京工科大学 教授
委員	稲葉 厚志	GMO グローバルサイン株式会社 室長
委員	佐野 文彦	東芝ソリューション株式会社 研究主務
委員	羽根 慎吾	株式会社日立製作所 主任研究員
委員	松尾 真一郎	独立行政法人情報通信研究機構 主任研究員
委員	盛合 志帆	ソニー株式会社 主任研究員

オブザーバー

中嶋　良彰	内閣官房情報セキュリティセンター
山口　利恵	内閣官房情報セキュリティセンター
根本　農史	内閣官房情報セキュリティセンター
末澤 洋	警察庁 情報通信局[2010 年 7 月まで]
初川 泰介	警察庁 情報通信局[2010 年 7 月より]
松本 和人	総務省 行政管理局[2010 年 7 月まで]
松宮 志麻	総務省 行政管理局[2010 年 7 月より]
大西 公一郎	総務省 自治行政局 住民制度課[2010 年 7 月より 2 月まで]
浦上 哲郎	総務省 自治行政局 住民制度課[2010 年 2 月より]
山﨑 敏明	総務省 自治行政局 住民制度課
浦舟 利幸	総務省 自治行政局 地域政策課[2010 年 7 月より]
島田 淳一	総務省 情報通信国際戦略局[2010 年 7 月まで]
古賀 康之	総務省 情報通信国際戦略局[2010 年 7 月まで]
梶原 亮	総務省 情報通信国際戦略局[2010 年 7 月まで]

齊藤 修啓	総務省 情報通信国際戦略局[2010 年 7 月まで]
水野 伸太郎	総務省 情報流通行政局[2010 年 7 月より]
佐々木 信行	総務省 情報流通行政局[2010 年 7 月より]
谷岡 大祐	総務省 情報流通行政局[2010 年 7 月より]
佐久間 明彦	外務省 大臣官房
山中 豊	経済産業省 産業技術環境局
下里 圭司	経済産業省 商務情報政策局[2010 年 6 月まで]
森川 淳	経済産業省 商務情報政策局[2010 年 6 月より]
池西 淳	経済産業省 商務情報政策局
坂下 圭一	防衛省 運用企画局
石川 正興	防衛省 技術研究本部[2010 年 7 月より]
滝澤 修	独立行政法人情報通信研究機構
大塚 玲	独立行政法人産業技術総合研究所[2010 年 9 月まで]
花岡 悟一郎	独立行政法人産業技術総合研究所[2010 年 9 月より]

事務局

独立行政法人 情報通信研究機構 （篠田陽一[2010 年 7 月まで]、高橋幸雄[2010 年 7 月より]、近藤玲子、田中秀磨、松尾真一郎、大久保美也子、黒川貴司、金森祥子、多賀文吾、赤井健一郎、持永大）

独立行政法人 情報処理推進機構（矢島秀浩、山岸篤弘、大熊建司、神田雅透、小暮淳、近澤武、鈴木幸子）

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、暗号技術は情報セキュリティシステム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。

高度情報通信ネットワーク社会形成基本法（IT 基本法）が策定された 2000 年以降、行政の情報化及び公共分野における情報通信技術の活用に関する様々な取り組みが実施されてくるにつれて、情報セキュリティ問題への取組みを抜本的に強化する必要性がますます認識されるようになってきた。

2006 年 2 月、内閣官房情報セキュリティセンター(NISC)の情報セキュリティ政策会議(議長：内閣官房長官)において、我が国の情報セキュリティ問題全般に関する中長期計画(2006～2008 年度の 3 ケ年計画)として「第 1 次情報セキュリティ基本計画」（第 1 次基本計画）が決定され、同計画において、暗号技術に関して今後取り組むべき重点政策として、「電子政府の安全性及び信頼性を確保するため、電子政府で使われている推奨暗号について、その安全性を継続的に監視・調査するとともに、技術動向及び国際的な取組みを踏まえ、暗号の適切な利用方策について検討を進める」こととされた。

CRYPTREC では、2005 年度にハッシュ関数の安全性評価を実施し、2006 年 6 月に SHA-1 の安全性に関する見解を公表した。これに基づき、第 1 次基本計画の年度計画である「セキュア・ジャパン 2007」では、「電子政府推奨暗号について、その危殆化が発生した際の取扱い手順及び実施体制の検討を進める」こととされ、NISC をはじめとする政府機関において、暗号の危殆化に備えた対応体制等を整備することが喫緊の課題であることが認識された。そして、2006 年度には素因数分解問題の困難性に関する評価を実施し、RSA1024 の安全性の評価を公表した。これらの SHA-1 及び RSA1024 に関する安全性に関する CRYPTREC からの見解に基づき、NISC が事務局を務める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」が決定されるに至った。

第 1 次基本計画に引き続いて、中長期計画(2009～2011 年度の 3 ケ年計画)として「第 2 次情報セキュリティ基本計画」が NISC の情報セキュリティ政策会議において 2009 年 2 月に決定され、同計画において、「「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」の策定時の経験を適切に継承し、安全性が低下した暗号について速やかに安全な暗号への移行を進める」こととされた。

このように、電子政府推奨暗号の監視等の機能は非常に重要であり、暗号技術の危殆化を予見し、電子政府システムで利用される暗号技術の安全性を確保するためには、最新の暗号理論の研究動向を専門家が十分に情報収集・分析することが必要であることはもちろんのこと、今後も、CRYPTREC が発信する情報を踏まえ、各政府機関が連係して情報通信システムをより安全なものに移行するための取り組みを実施していくことが必要不可欠である。

1.2 暗号方式委員会

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（CRYPTREC: Cryptography Research and Evaluation Committees）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（付録１参照）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。暗号技術監視委員会の責務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である。さらに、暗号技術監視委員会は電子政府推奨暗号の監視活動のほかにも、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を委ねられている。

平成２０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、平成２１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。

平成２１年度に行っ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、平成２２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た。評価結果については、第 2 章及び付録 4 を参照のこと。また、平成２１年度に引き続き、暗号技術調査ワーキンググループ（リストガイド）において、暗号技術に詳しくない情報システム調達担当者及び運用担当者を対象とした、電子政府推奨暗号リストの適切な利用のため技術的解説書の作成を継続して行っている。詳細については、第 4 章を参照こと。

1.3 電子政府推奨暗号リスト

平成１２年度から平成１４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、平成１４年に暗号技術検討会に提出され、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」（付録１参照）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

なお、平成２１年度は、平成２０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。

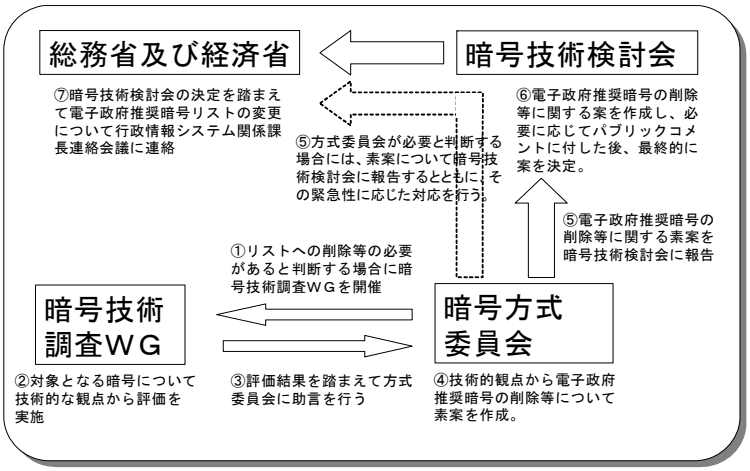
1.4 活動の方針

電子政府推奨暗号リスト掲載の暗号に関する研究動向を把握して、暗号技術の安全性について監視を行い、必要に応じて電子政府システムにおける暗号技術の情報収集と電子政府推奨暗号リストの改訂について暗号技術検討会(総務省・経済産業省)に対して助言を行う。また、暗号理論全体の技術動向を把握して、最新技術との比較を行い、電子政府システムにおける暗号技術の陳腐化を避けるため、将来の電子政府推奨暗号リストの改正を考慮して、電子政府推奨暗号に関する調査・検討を行う。監視活動は、情報収集、情報分析、審議及び決定の３つのフェーズからなる。

暗号技術検討会における電子政府推奨暗号の監視に関する基本的考え方は以下の通りである。

(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。

電子政府推奨暗号の削除等の手順



第２章 電子政府推奨暗号リストの改訂について

2.1. 改訂の背景

CRYPTREC は、客観的な評価により安全性及び実装性に優れると判断される暗号技術をリストアップすることを目的に、2000 年度に暗号技術の公募・評価活動を開始し、2002 年度末に電子政府推奨暗号リスト（以下、「現リスト」）を発表した。

その後、各府省に対してその利用を推奨することにより、電子政府の高度な安全性と信頼性を確保することを目指して、2003 年度から監視活動及び安全性評価を継続して行ってきた。これにより、現リストの信頼性は高められ、また、それらの活動に基づいた暗号の危殆化への対応・提言は電子政府において広く認知されてきた。

現リストには、策定時点において、今後 10 年間は安心して利用できるという観点で選定された暗号が掲載されている。しかし、策定から 5 年余りが経過し、暗号技術に対する解析・攻撃技術の高度化や、新たな暗号技術の開発が進展している状況にある。

また、今日では CRYPTREC への要望が、暗号技術に対する安全性評価とその周知のみならず、安心・安全な情報通信システムを構築する上で、暗号技術の危殆化及び移行対策等を含めた、適切な暗号技術の選択を支援するものへと変化しつつある。

さらに、暗号技術の評価の面において、政府調達等における入手し易さや導入コスト、相互運用性と普及度合いの観点も取り入れる必要性が指摘されているところである。

これらの状況を踏まえ、2012 年度、現リストを改訂することが必要である。

2.2. 現リストの改訂の目的

今回の改訂においては、第一に、電子政府において暗号技術を利用する際に安全な暗号技術を選択するための指針を与えること、第二に、暗号を利用した技術をシステムのセキュリティ要件に合わせて正しく組み込むための指針を与えることを目的とする。次期リストは、内閣官房情報セキュリティセンター（NISC）の調整により、情報セキュリティ政策会議で決定された「政府機関の情報セキュリティ対策のための統一基準」等から参照されることを想定している。

このため、今回の改訂にあたっては、新たに暗号技術の公募を行うとともに、現リストに掲載されている暗号技術の見直しを行い、現リストの全体の構成を改めることとする。

2.3. 電子政府推奨暗号リスト改訂のための暗号技術の公募（2009 年度）

2.3.1. 公募の概要

CRYPTREC は評価対象暗号技術を公募し、暗号技術評価を実施する。特に、安全性及び実装性で、現リストに記載されている暗号アルゴリズムよりも優位な点を持ち、国際学会で注目されている新技術が提案されている暗号技術カテゴリであること、及び、現リストに掲載されている暗号技術と同カテゴリに属する暗号技術については、それらの暗号技術よりも、安全性もしくは実装性において優れた暗号技術であることを指針としている。

暗号技術評価の実施にあたっては、暗号技術評価に実績のある国内及び国外の専門家に委託した評価や学会及び論文誌等で発表された評価を踏まえ、各暗号技術の安全性及び実装性等の特徴を整理する。その結果は、事務局が開催するシンポジウムや報告書等を通じて、一般に公表することを予定している。

2009 年度から 2010 年度にかけては、主に応募された暗号技術の評価を実施する。また、2011 年度には、応募された暗号技術の評価を継続するほか、現リストに掲載されている暗号技術の再評価も行う。

暗号方式委員会、暗号実装委員会及び暗号運用委員会が、評価結果に基づき、「CRYPTREC 暗号リスト（仮称）」（以下、「次期リスト」という。）への暗号技術の記載について判定し、暗号技術検討会に報告する。報告された暗号技術の次期リストへの記載については、暗号技術検討会での検討を経た後、最終的に総務省及び経済産業省において決定される。決定については、2012 年度実施を予定している。

2.3.2. 公募の対象

2009 年度公募対象の暗号技術の種別は、以下のとおり（表 3.1）である。ただし、主な留意事項としては、

- 応募される暗号技術は、2010 年 9 月末までに、査読付きの国際会議、又は、査読付きの国際論文誌で発表されているか、あるいは、採録が決定されているもの。
- 評価する際に知的財産の利用が無償で行えるもの。
- 公募する暗号技術、又はそれを実装した製品が、電子政府等の利用に際し、次期リスト策定後 3 年以内までに調達可能なもの。

等を挙げていた。

表 3.1　2009 年度公募対象の暗号技術の種別

暗号技術の種別	仕様の概要
ブロック暗号	平文及び暗号文ブロックサイズが 128 ビットであり、鍵長が 128 ビット、192 ビット又は 256 ビットであるブロック暗号で、現リストに掲載されている暗号技術と同等以上の特長（安全性又は実装性）を持つもの。
暗号利用モード	秘匿に関する 128 ビットブロック暗号及び 64 ビットブロック暗号を対象にした利用モード。
メッセージ認証コード	鍵長が 128 ビットである 128 ビットブロック暗号及び 64 ビットブロック暗号を利用したメッセージ認証コード。
ストリーム暗号	鍵長が 128 ビット以上であり、平文をビット単位もしくはバイト単位で暗号化するストリーム暗号。
エンティティ認証	電子政府推奨暗号リストに掲載された共通鍵暗号、公開鍵暗号、ハッシュ関数、メッセージ認証コードの組み合わせによって実現されるエンティティ認証、あるいは、安全性を計算量的な困難さに帰着できるエンティティ認証を公募する。エンティティ認証を構成する要素技術は、現リストに掲載されている暗号技術を用いることを原則とする。 要素技術として、現リストに掲載されていない共通鍵暗号、メッセージ認証コードを用いる場合は、これらの要素技術を同時に応募する必要がある。また、上記以外の要素技術を用いたエンティティ認証技術の応募も可能。

表 3.2　2009 年度応募暗号技術一覧

暗号種別	暗号技術名	応募者
128 ビットブロック暗号	CLEFIA	ソニー株式会社
	HyRAL	株式会社ローレルインテリジェントシステムズ
ストリーム暗号	Enocoro-128v2	株式会社日立製作所
	KCipher-2	KDDI 株式会社
メッセージ認証コード	PC-MAC-AES	日本電気株式会社
エンティティ認証	無限ワンタイムパスワード認証方式（Infinite One-Time Password）	日本ユニシス株式会社

※暗号利用モードについては応募なし。

2.3.3. 公募期間

2009 年 10 月 1 日～2010 年 2 月 4 日 17 時

2.3.4. 応募暗号技術

2009 年度において、上記のとおり（表 3.2)、6 件の暗号技術について応募があった。

2.3.5. 事務局選出暗号技術

CRYPTREC におけるリストガイド策定時の検討結果などを参考に、国際標準化等の実績がある以下の暗号技術について、CRYPTREC 事務局より選出した。

表 3.3　2009 年度事務局選出暗号技術一覧

暗号種別	暗号技術名	評価仕様
メッセージ認証コード	CBC-MAC	ISO/IEC 9797-1
	CMAC	NIST SP 800-38B
	HMAC	NIST FIPS 198-1
暗号利用モード	CBC モード	NIST SP 800-38A
	CFB モード	NIST SP 800-38A
	OFB モード	NIST SP 800-38A
	CTR モード	NIST SP 800-38A
	GCM モード	NIST SP 800-38C
	CCM モード	NIST SP 800-38C
エンティティ認証	共通鍵暗号利用による認証プロトコル	ISO/IEC 9798-2、対称暗号化アルゴリズムを使用する機構
	電子署名利用による認証プロトコル	ISO/IEC 9798-3、デジタル署名技術を使用する機構
	検査関数（MAC）による認証プロトコル	ISO/IEC 9798-4、暗号検査機能を使用する機構

※128 ビットブロック暗号及びストリーム暗号については選出なし。

2.4. 応募暗号の評価スケジュール

2012 年度の電子政府推奨暗号リストの改訂に向けた応募暗号の評価スケジュールをまとめると以下の通り。

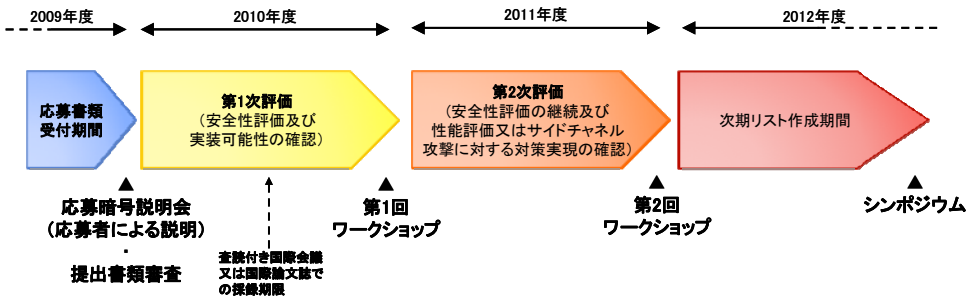


図 3.4 評価スケジュール

CRYPTREC シンポジウム 2010 開催：	2010 年 3 月 2 日・3 日
第 1 次評価実施：	2010 年 4 月～2011 年 3 月
CRYPTREC ジンポジウム 2011 開催：	2011 年 3 月 2 日
第 2 次評価実施：	2011 年 4 月～2012 年 3 月
CRYPTREC シンポジウム 2012：	2012 年 3 月頃
CRYPTREC シンポジウム 2013：	2013 年 3 月頃

2010 年度にかけては、主に応募された暗号技術の評価を実施した。また、2011 年度には、応募された暗号技術の評価を継続するほか、現リストに登録されている暗号技術の再評価も行う。

暗号方式委員会及び暗号実装委員会が、評価結果に基づき、「CRYPTREC 暗号リスト（仮称）」（以下、「次期リスト」という。）への暗号技術の記載について判定し、暗号技術検討会に答申する。答申された暗号技術の次期リストへの記載については、暗号技術検討会での検討を経た後、最終的に総務省及び経済産業省において決定される。決定については、2012 年度実施を予定している。

2.5. 応募暗号の評価項目

安全性評価項目と実装性評価項目の 2 つに大別される。

（1）安全性評価項目

既知の一般的な攻撃法に対する耐性を評価する。また、その暗号に特化した攻撃法や、ヒューリスティックな安全性の根拠も評価の対象とすることがある。

（2）実装性評価項目

提出資料に基づいて、実現可能性の確認を行う。性能の評価に関して、ソフトウェア実装では、標準的なプラットフォーム上での性能（処理速度、メモリ使用量等）を評価する。また、ハードウェア実装（エンティティ認証を除く）では、使用するプロセス（FPGA[1]、ASIC[2]

[1] FPGA：Field Programmable Gate Array

等）別に性能（処理速度、使用セル数又はゲート数等）を評価する。また、一部の暗号技術に対しては、サイドチャネル攻撃に対する対策実現の確認も行う。

なお、2009 年度公表した公募要項では、実装性評価の実施に際して、明確でない部分があったため、2010 年度暗号実装委員会において詳細を検討した。その結果は、CRYPTREC 統一 Web サイト（http://www.cryptrec.go.jp/）などを通じてアナウンスする予定である。

2.6. 第 1 次評価の進捗状況

2010 年度における応募暗号技術及び事務局選定暗号技術に関する第 1 次評価の進捗状況は以下の通りである。

2.6.1. 応募暗号技術の評価状況

表 3.5　応募暗号技術の第 1 次評価結果

暗号種別	暗号技術名	提案者	評価継続の要否
128 ビットブロック暗号	CLEFIA	ソニー株式会社	引き続き第 2 次評価を行う。
	HyRAL	株式会社ローレルインテリジェントシステムズ	128 ビット鍵長から 255 ビット鍵長においては、現在のところ問題点は見つかっていないが、256 ビット鍵長の場合、極小的な数であるが等価鍵の発見及び現実的な計算量での導出法が示された。よって、現リストに掲載されている暗号技術と同等以上の安全性を持たないと判断し、第 1 次評価までで評価終了とし、次期リストには掲載しない。
ストリーム暗号	Enocoro-128 v2	株式会社日立製作所	引き続き第 2 次評価を行う。
	KCipher-2	KDDI 株式会社	引き続き第 2 次評価を行う。
メッセージ認証コード	PC-MAC-AES	日本電気株式会社	引き続き第 2 次評価を行う。

※ 暗号利用モードについては応募なし。

※ エンティティ認証に応募された無限ワンタイムパスワード認証方式については、2010 年 9 月末までに、査読付きの国際会議又は査読付きの国際論文誌で発表されなかったことにより、応募資格を喪失した。

[2] ASIC：Application Specific Integrated Circuit

2.6.2. 事務局選出暗号技術の評価状況

表 3.6　応募暗号技術の第 1 次評価結果

暗号種別	暗号技術名	評価仕様	評価継続の要否
メッセージ認証コード	CBC-MAC	ISO/IEC 9797-1	今後、注意すべき利用方法や利用方法に関する注釈等について検討した上で、次期リストに掲載する。
	CMAC	NIST SP 800-38B	
	HMAC	NIST FIPS 198-1	
暗号利用モード	CBC モード	NIST SP 800-38A	
	CFB モード	NIST SP 800-38A	
	OFB モード	NIST SP 800-38A	
	CTR モード	NIST SP 800-38A	
	GCM モード	NIST SP 800-38C	
	CCM モード	NIST SP 800-38C	
エンティティ認証	共通鍵暗号利用による認証プロトコル	ISO/IEC 9798-2、対称暗号化アルゴリズムを使用する機構	一部のタイプに脆弱性を発見したので、それらについては利用しないよう注釈を付けた上で、次期リストに掲載する。ただし、脆弱性の発見されたタイプに関しては、修正方法が存在するので、ISO/IECに対して修正を求め、修正が完了し次第、注釈に関して再検討を行う。
	電子署名利用による認証プロトコル	ISO/IEC 9798-3、デジタル署名技術を使用する機構	
	検査関数（MAC）による認証プロトコル	ISO/IEC 9798-4、暗号検査機能を使用する機構	

※128ビットブロック暗号及びストリーム暗号については選出なし。

2.7. CRYPTREC シンポジウム 2011 の開催

2010 年度は、電子政府推奨暗号リストの改訂のための暗号技術公募（2009 年度）に応募された暗号技術に関する安全性評価を実施した。本シンポジウムにおいて、最新の評価結果を公表し、それらについて検討した。

2.7.1. プログラムの概要

日時：2011 年 3 月 2 日（水）10：00～16：00
場所：コクヨホール
主催：独立行政法人情報通信研究機構、独立行政法人情報処理推進機構
共催：総務省、経済産業省

参加人数：約 200 名

表 3.7　プログラム

3 月 2 日(水)	
時間	内容
10:00	開会挨拶
10:05	応募暗号技術の安全性評価について 1 ・ 128 ビットブロック暗号 -CLEFIA -HyRAL ・ メッセージ認証コード -PC-MAC-AES ・ エンティティ認証 -無限ワンタイムパスワード
11:50	昼休み
13:00	応募暗号技術の安全性評価について 2 ・ ストリーム暗号 -Enocoro-128v2 -KCipher-2
14:00	事務局選出暗号の安全性評価について
13:45	実装評価の方法について
15:40	安全性評価に関するまとめ
15:55	閉会挨拶

2.7.2. 本シンポジウムで寄せられた意見・コメント等

シンポジウムでは、応募者等から応募暗号の安全性評価及び実装性評価に対する意見・コメントが寄せられた。以下にそれらの概要を記す。

（1） 応募暗号技術の安全性評価について

① CLEFIA

- 「弱鍵組」という表現は適切ではない。
  - 「弱鍵組」のような特性が関連鍵攻撃のような安全性評価につながるかどうか、現時点でははっきりしていない。

② HyRAL

- Double Key Modeにおいて排他的論理和を止めれば、鍵スケジュールの安全性は保たれる。
  - 本公募ではアルゴリズムの修正は認められない。

③ PC-MAC-AES

- 安全性証明における 2^{56} がタイトであるかどうかについては未解決である。
- 安全性証明よりもむしろ最終的にどの程度安全なのかどうかについて議論すべきである。
  - 一般的にブロック暗号利用モードにおいて 2^{64} はジェネリックなバウンドと考えられるので、それと比較するのも 1 つの考えである。攻撃手法の妥当性については学会の動向を見ていくのが良いのではないか。

④ Enocoro-128v2

- たくさんの鍵の中でどれか 1 個を解読できたら攻撃成功とみなすという攻撃シナリオは攻撃者にとってメリットが非常に小さいと思うが、これを有効とみなすと安全性は 64 ビットレベルに落ちてしまうので、現状で特に問題とは認識されていないのかどうか。
- 今後評価を進めていくと現行リスト掲載暗号、たとえば MUGI 等との優位性が問題となるが、アピールする点を確認したい。
  - MUGI は汎用性の高いストリーム暗号である。Enocoro は非常に小さく作れることを主眼にした、ハードウェアをメインのプラットフォームと考えている。小型実装の観点では、回路規模が小さくて速いのが特徴である。

⑤ KCipher-2

- 現行リスト掲載暗号との比較について、アピールする点はないか確認したい。
  - ソフトウェア実装に優れているという点がある。

（2） 事務局選出暗号

- ISO/IEC 9798-2 と ISO/IEC 9798-4 については現在定期見直しの時期にあることから、今回の評価結果を ISO に提出して、修正すべき点を提案したい。次期リストに付ける注釈について、今後、CRYPTREC において検討していくことが必要になるものと考えられる。
  - 一般ベンダやユーザの立場からは、リストを参照する上で、専門家が書いた前提条件などの注釈よりも、使って良いのか悪いのかの観点の方が重要である。
- エンティティ認証に対する中間者攻撃については、フォーマルメソッドを使った今回の評価において実施されている。

（3） 安全性評価のまとめ

- 関連鍵攻撃やキャッシュ攻撃を評価項目として、現時点で実現性に疑問があるから対象外とするか、長い間安全に使っていくことを念頭に入れ、より安全性の高いものを選出するために対象とすべきかどちらの方が良いか。攻撃の実現性の観点をどの程度考慮に入れて評価に反映させるか。
  - 可能な限り、より安全性の高い暗号を推奨していくのが良いと思う。
  - 正しく使用しても物理的な環境によってシナリオが成立してしまうものと、基本的に正しく使用していない場合に成立してしまうものとでは攻撃の性質が異なるので、別々に考えるべきである。
  - 関連鍵攻撃に関しては、シンプルな関連鍵を使うものから、暗号アルゴリズム事態をオラクルに使うようなものまでいろいろなレベルがあり、それぞれ実現可能性が異なるので、個々に判断すべきである。
  - 関連鍵攻撃やキャッシュ攻撃に対して攻撃が有効とされた AES に関して落とすのは現実的ではない。普及していて取り扱いを変えるという議論とより安全性の高い暗号を選択していくという議論は別にすべきである。普及状況に配慮して攻撃が有効という事実を隠すべきではなく、こういう問題点があるという注釈をつけて、広く情報提供するのが良い。
  - 次期リスト構成は 3 つのブロックに別れていて、利用実績や製品化実績も考慮に入れるので、少々の欠点が見つかっても非常に普及しているような暗号については何らかの配慮が入る場合がある。
- 暗号利用モードの ECB モードに関して、現場では使っている可能性があるので、次期リストの注釈を書くときに配慮をして欲しい。

（4） 実装評価の方法について

- キャッシュ攻撃を外しているのは、評価リソースが限られているので、電力解析に注力しているからである。AES-NI[3]を使った評価については今後の検討課題である。
- 現行リスト掲載暗号に対してサイドチャネル攻撃対策の有効性確認を行わない理由はなぜか。公平な比較ができるものに関しては、同一環境で同じ実装者が行う方が適切だと思うが、今回の応募暗号については応募者が実装することになったのはどうしてか。
  - サイドチャネル攻撃については対策できることの確認を行うレベルであり、現行リスト掲載暗号と応募暗号との比較は行わないためである。現行リスト掲載暗号は提案されてから時間が経過しており、最適化手法のノウハウも蓄積されている段階にあるが、新規に提案された暗号は最適化の知見が評価側

[3] Advanced Encryption Standard New Instructions

にはあまりないものと考えられる。提案がいかに良いのかということをアピールする形で、応募者の方から現行リスト掲載暗号の性能面で上回る結果を出して欲しい。

- 情報を出したくない応募者はデータを出さなくても良いという選択肢が欲しい。
  - 提出して頂いた性能が本当に出せるのかどうかを検証するのが目的である。推奨する側の CRYPTREC の立場からすれば、きちんと確認し自信をもって推奨できるものを取り揃えたいので、評価を行いたい。
- 今後、電子政府においてもスマートフォン環境における利用が増えると思うので、ARM や Java のような環境における評価が必要である。
- NIST の SHA-3 の選考が行われた後は、ハッシュ関数に関する現行リストの更新が行われると思うが、スケジュールはどうなっているのか。
  - SHA-3 の選考後に検討を開始するものと思う。他のカテゴリについても、重要性の高いものから随時リストの更新を検討していくことになっている。
- ハードウェア実装評価において、ブロック RAM を使っても良いか。
  - 情報提供を主眼としているので、例えばブロック RAM を利用した場合には、どれだけ使ったということを明記して頂きたい。
- サイドチャネル攻撃に関する研究があまり活発でなかった頃に、開発時にサイドチャネル攻撃に対する考慮がされていないとするならば、現行リスト掲載暗号の方が潜在的なリスクが高いと考えられる。新規提案に対して情報提供をして欲しいというからには、現行リスト掲載暗号に対しても情報提供をお願いするか、将来的に CRYPTREC として評価を進めるかどうかの考え方を明確にして欲しい。
  - 現行リスト掲載暗号についても、耐性がどの程度で、対策実装を行った場合、どの程度コストがかかり、どの程度処理性能が低下するのか検証すべきである。
  - 最終的に電子政府推奨暗号を決める段階になって、現行リスト掲載暗号を含めて、改めてサイドチャネル攻撃評価を総合的に考えて欲しい。
- ハードウェア実装評価に関する提出物については、公開等は予定されているのか。
  - ノウハウの塊を公開することは考えていない。ブラックボックスで評価できるように情報提供して頂ければと考えている。

第３章 監視活動

3.1. 監視活動報告

電子政府推奨暗号の安全性評価について 2010 年度の報告時点では収集した全ての情報が「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。

3.1.1. 共通鍵暗号に関する安全性評価について

AES に対する攻撃の研究が盛んな状況は変わらないが、今年度、目立った動きとしては、関連鍵攻撃における解析の自動化と単一鍵攻撃研究の再活性化がある。AES-128 と AES-192 の関連鍵攻撃について、次のような従来より効率の良い結果が得られた。

・AES-128: 7 段(10 段中)を選択平文 2^{97} 個、計算量 2^{97} で攻撃可能
・AES-192: 12 段(12 段中)を選択平文 2^{116} 個、計算量 2^{169} で攻撃可能

一方、AES の単一鍵攻撃について、次のような従来より効率の良い結果が得られた。

・AES-192: 8 段(12 段中)を必要平文数 2^{113}、必要メモリ量 2^{129}、必要計算量 2^{172}
・AES-256: 8 段(14 段中)を必要平文数 2^{113}、必要メモリ量 2^{129}、必要計算量 2^{196}

3.1.2. 公開鍵暗号に関する安全性評価について

昨年度の暗号技術検討会報告書でも報告済みであるが、素因数分解問題に関して、The RSA Factoring Challenge[1]の RSA-768（768 ビット RSA 合成数）一般数体ふるい法で素因数分解されたことが Crypto 2010 で発表された。その後、この記録が更新されたという報告はない。

3.1.3. ハッシュ関数に関する安全性評価について

Asiacrypt 2010 において、中間一致攻撃の改良によるハッシュ関数 Tiger、MD4、縮約版 SHA-2 への原像攻撃が発表された。SHA-2 への攻撃は IACR の ePrint 2010/016 によると、42 段 SHA-256 の場合 $2^{251.7}$ の計算量で、また 42 段 SHA-512 の場合 $2^{494.6}$ の計算量で、原像を求めることができるとされている。

[1] RSA 社（米国）の素因数分解問題に関するコンテスト。既に終了している。

また、NIST は 2010 年 12 月 9 日付けで SHA-3 コンペティションの最終 5 候補を発表した（表 5.2 参照)。今回の選考では安全性評価に重点が置かれた模様で、第 2 ラウンドの 14 候補に唯一残りハードウェア性能に優れていた日本提案の Luffa は残念ながら落選した。NIST は今後､2012 年春に最後の SHA-3 Candidate Conference を開催､2012 年の終盤に SHA-3 を決定するとしている。

表5.2　第3ラウンド(最終ラウンド)に進んだSHA-3候補一覧

名称	筆頭投稿者	開発国
BLAKE	Jean-Philippe Aumasson	スイス
Grøstl	Lars R. Knudsen	デンマーク、オーストリア
JH	Hongjun Wu	シンガポール
Keccak	The Keccak Team	ベルギー
Skein	Bruce Schneier	米国、ドイツ

第 2 ラウンド候補のハッシュ関数の評価結果は、NIST が「Status Report on the Second Round of the SHA-3 Cryptographic Hash Algorithm Competition」[2]として公表している。

3.2. 暗号技術標準化動向

暗号標準化動向としては、暗号アルゴリズムの掲載数に関する議論がある。現在、「暗号アルゴリズム」(18033)は、第 1 部:総論、第 2 部:非対称暗号、第 3 部:ブロック暗号、第 4 部:ストリーム暗号の 4 部で構成されている。「暗号アルゴリズム」(18033)に対する最近の改訂で第 2 部と第 3 部に新規のアルゴリズムが追加され、掲載数が各々、8 方式と 5 方式となる予定であり、増加傾向にある。2010 年 10 月のベルリン会議において、欧州の暗号研究プロジェクト ECRYPT-II のリエゾンでもある Preneel 教授 (ベルギー、KUL) が、第 3 部 (ストリーム暗号) に ECRYPT-II のストリーム暗号に関するコンペティションで落選した方式が標準に採用される等という問題が生じ、採用基準を厳しくして掲載数を絞るように提案した。この提案をうけ、SC 27/WG 2 の上位組織である SC 27 では、WG 2 内で研究期間(Study Period)を開始することとし、アンケートと寄書募集の実施が決まった。この検討結果は、CRYPTREC の活動に影響を与える可能性があり､今後とも注意深く SC 27/WG 2 の動向調査し、慎重な対応する必要がある。

[2] http://csrc.nist.gov/groups/ST/hash/sha-3/Round2/documents/Round2_Report_NISTIR_7764.pdf

3.3. 学会等参加記録

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3.2に示す通りである。

表 3.2 国際会議への参加状況

学会名・会議名		開催国・都市	期間
PKC 2010	International Conference on Practice and Theory in Public Key Cryptography	フランス パリ	2010年5月26日～5月28日
LCD	Lattice Crypto Day	フランス パリ	2010年5月29日
Eurocrypt 2010	International Conference on the Theory and Applications of Cryptographic Techniques	フランス ニース／モナコ	2010年5月30日～6月3日
SAC 2010	Selected Areas in Cryptography	カナダ・ウォータールー	2010年8月12日～8月13日
Crypto 2010	International Cryptology Conference	米国・サンタバーバラ	2010年8月15日～8月19日
CHES 2010	Workshop on Cryptographic Hardware and Embedded Systems	米国・サンタバーバラ	2010年8月18日～8月20日
FDTC 2010	Fault Diagnosis and Tolerance in Cryptography	米国・サンタバーバラ	2010年8月21日
2nd SHA-3 Conference	Second SHA-3 Candidate Conference	米国・サンタバーバラ	2010年8月23日～8月24日
IWSEC 2010	International Workshop on Security	日本・神戸市	2010年11月22日～11月24日
Asiacrypt 2010	International Conference on the Theory and Application of Cryptology and Information Security	シンガポール・シンガポール	2010年12月5日～12月9日
Pairing 2010	International Conference on Pairing-Based Cryptography	日本・加賀市	2010年12月13日～12月15日
FSE 2011	International Workshop on Fast Software Encryption	デンマーク・リンビー	2011年2月14日～2月16日
SKEW 2011	Symmetric Key Encryption Workshop	デンマーク・リンビー	2011年2月16日～2月17日
PKC 2011	International Conference on Practice and Theory in Public Key Cryptography	イタリア・タオルミーナ	2011年3月7日～3月9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について述べ

る。

3.3.1. ブロック暗号の解読技術

Key Recovery Attacks of Practical Complexity on AES-256 Variants with up to 10 Rounds [Eurocrypt 2010]

Crypto 2009 と Asiacrypt 2009 で、フル・ラウンドの AES-192(192 ビット鍵の AES)と AES-256 が関連鍵ブーメラン攻撃で破れることを示した。しかし、これらの攻撃に必要な計算量は現時点の計算機技術では実現がほぼ不可能である。そこで、本論文では、実現可能な計算量で、AES-256 が 14 段中何段まで攻撃可能か検討したところ、次の値が得られた。

9 段では単純な関連鍵攻撃を使い、2 個の関連鍵、暗号化 2^{39} 回分の計算で攻撃可能。

10 段では、より強力な関連サブ鍵攻撃(related sub-key attack)を使い、2 個の関連鍵、暗号化 2^45 回分の計算で攻撃可能。11 段では、より強力な関連サブ鍵攻撃を使い、2 個の関連鍵、暗号化 2^{70} 回分の計算で攻撃可能。実現可能な計算量を 2^56 とすると、AES-256 は 10 段まで関連鍵攻撃可能という結果になった。

Automatic Search for Related-Key Differential Characteristics in Byte-Oriented Block Ciphers: Application to AES, Camellia, Khazad, and Others [Eurocrypt 2010]

ブロック暗号の差分解読に対する安全性の研究は比較的進んでおり、安全性の下限を評価する単純な方法が知られているが、関連鍵攻撃に対する安全性を評価する方法は、まだ整備されていない。本論文は、関連鍵攻撃に対する安全性を評価する方法を確立するための第1歩として、ブロック暗号に対する最大の関連鍵差分特性確率を自動的に探索するツールを開発し、既存の暗号、AES, byte-Camellia, Khazad, FOX, Anubis に適用して有効性を検証した。ここで、byte-Camellia とは、探索ツールが効果的に機能するように Camellia を変形したもので、データ・ランダム化部の FL/FL^-1 関数を取り除き、鍵スケジュール部のシフトをバイト単位に置き換えたものである。探索の結果見つかった関連鍵差分経路を使って、攻撃を設計したところ、以下に上げるもので、既存を上回る有効性を示した。

AES-128: 7 段(10 段中)を選択平文 2^{97} 個、計算量 2^{97} で攻撃可能

AES-192: 12 段(12 段中)を選択平文 2^{116} 個、計算量 2^{169} で攻撃可能

AES-256: 既存の攻撃を下回る。既存の結果次の通り、

14 段(14 段中)を選択平文 $2^{99.5}$ 個、計算量 $2^{99.5}$ で攻撃可能

byle-Camellia-128: 18 段(18 段中)を選択平文 $2^{6.17}$ 個、計算量 $2^{6.17}$ で攻撃可能

Khazad: 7 段(10 段中)を選択平文 2^{50} 個、計算量 2^{50} で攻撃可能

Khazad: 8 段(10 段中)を選択平文 2^{55} 個、計算量 2^{55} で攻撃可能

Improved Single-Key Attacks on 8-round AES-192 and AES-256 [Asiacrypt 2010]

近年、フルラウンド AES-192/256 の関連鍵攻撃による解読が注目されているが、攻撃成立の条件が厳しいため現実的な脅威であるというコンセンサスはできておらず、従来型の単一鍵に対する

解読研究による安全性評価は重要である。この論文では、multi tabulation, differential enumeration, key bridging という新規に開発された3種類のテクニックを AES-192 と AES-256 に適用した結果が報告された。最大攻撃段数は 8 段のままで更新できなかったものの、必要な選択平文数と計算量ともに従来より削減することに成功した。

AES-192: 必要平文数 2^{113}、必要メモリ量[3] 2^{129}、必要計算量[4] 2^{172}
AES-256: 必要平文数 2^{113}、必要メモリ量 2^{129}、必要計算量 2^{196}

A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony [Crypto 2010]

第３世代の携帯電話規格では、MISTY1 をベースとする KASUMI が A5/3 ブロック暗号として秘匿に利用されている。この論文では、フルラウンドの KASUMI が関連鍵とブーメラン攻撃の改良版であるサンドイッチ攻撃を使って、現実的な計算量で攻撃可能であることを示した。具体的には、KASUMI(フルスペックが 8 段)の 7 段が 2^{-14} という高い確率の識別子(distinguisher)を持つことを利用し、4 個の関連鍵、2^{26} 個のデータ(暗号文 2^{25} 個と対応する平文 2^{25} 個)、2^{30} バイトのメモリ、復号 2^{32} 回分の計算量で攻撃可能と評価した。なお、携帯電話電話の通常の利用においては、この攻撃が現実的な脅威となる可能性は低い。この内容は Asiacrypt 2009 のランプセッションで紹介されたものであるが、正式に論文として発表されたのは今回が最初である。

3.3.2. ストリーム暗号の解読技術

A Byte-Based Guess and Determine Attack on SOSEMANUK [Asiacrypt 2010]

eSTREAM のポートフォリオに載るストリーム暗号 SOSEMANUK が 2176 の時間計算量で攻撃できることが発表された。鍵ビット長が 176 ビットを超えるときは、全数探索よりも効率がよくなる。

3.3.3. ハッシュ関数の解読技術

Advanced Meet-in-the-Middle Preimage Attacks: First Results on Full Tiger, and Improved Results on MD4 and SHA-2 [Asiacrypt 2010]

シンガポール・南洋理工大学のグオらにより、中間一致攻撃の改良によるハッシュ関数 Tiger、MD4、縮約版 SHA-2 への原像攻撃が発表された。SHA-2 への攻撃は紙数制限から予稿には記載されていないが、IACR の ePrint 2010/016 によると、42 段 SHA-256 の場合 $2^{251.7}$ の計算量で、また 42 段 SHA-512 の場合 $2^{494.6}$ の計算量で、原像を求めることができる。

[3]必要メモリ量の単位: AES のブロックサイズ(=128 ビット)
[4]必要計算量の単位: AES 暗号化 1 回分

Advanced Meet-in-the-Middle Preimage Attacks: First Results on Full Tiger, and Improved Results on MD4 and SHA-2 [ePrint 2010/016]

シンガポール・南洋理工大学のグオらにより、中間一致攻撃の改良によるハッシュ関数 Tiger、MD4、縮約版 SHA-2 への原像攻撃が発表された。SHA-2 への攻撃は、42 段 SHA-256 の場合２２５１．７の計算量で、また 42 段 SHA-512 の場合２494．6 の計算量で、原像を求めることができる。この結果は Asiacrypt 2010 で発表されたが、ページ数制限のため SHA-2 に対する解析結果は予稿集に記載されていない。

Matrix Representation of Conditions for the Collision Attack of SHA-1 and its Application to the Message Modification [IWSEC 2010]

ＳＨＡ－１の衝突攻撃における Chaining Variable Condition (CVC) / Message Condition (MC) の行列表現を提案する。メッセージ修正(MM ： Message Modification)を構築するプロセスにおいて本方式を適用することにより、SHA-1 の衝突探索攻撃の計算量を削減することができる。

3.3.4. 公開鍵暗号の解読技術

Maximizing Small Root Bounds by Linearization Applications to Small Secret Exponent RSA [PKC 2010]

多項式の小さな解を見つける最適な格子の構成法を与えた。これにより、$d <= N^{0.292}$ の場合の Boneh-Durfee 攻撃に初めての証明を与え、更に Jochemsz-May の $dp,dq <= N^{0.073}$ の場合の攻撃の部分格子構造を特定した。Jochemsz-May の漸近的な上界を改良することはできなかったが、実験的にはより大きなビットに関する解読が可能となった。

Implicit Factoring with Shared Most Significant and Middle Bits [PKC 2010]

ある特定の条件を満たす場合の素因数分解の方法を与えた。2 個の RSA 合成数 N１=p１q１、N2=p2q2 が与えられ、各 qi はαビットの素数であり、pi は最上位 t ビットを共有し、t>=2α＋3 を満たすならば、logN1=logN2 の 2 次の計算量で N1、N2 の素因数分解を与えるアルゴリズムを示した。

Using Equivalence Classes to Accelerate Solving the Discrete Logarithm Problem in a Short Interval [PKC 2010]

ニュージーランド・オークランド大学/イギリス・ロイヤルホロウェイ大学のガルブレイスらは、離散対数問題の解が含まれる区間サイズが N の場合に、同値類を用いることにより、Pollard の Kangaroo 法の解読計算量を 2√N から 1.36√N に改良した。ただし、実験では、フルーツレスサイクルの出現等により、理論通りの高速化にはならない。

Solving a 676-Bit Discrete Logarithm Problem in GF(26n) [PKC 2010]
GF(3n)上の超特異曲線におけるη_Tペアリングを用いた暗号の安全性と関連のあるGF(36n)上の離散対数問題の解読実験にn=71の場合に成功し、拡大体上の離散対数問題の世界記録を達成した。80コアのCPUを用いて33日間で676ビットの解読に成功した。

Algebraic Cryptanalysis of the PKC 2009 Algebraic Surface Cryptosystem [PKC 2010]
東芝/北海道大学により提案された代数曲面暗号を解読した。求セクション問題を直接解くのではなく、暗号文から得られるイデアル分解により、秘密鍵に関し準線型の計算量でメッセージを回復することができる。推奨パラメーターにおける実験では、しばしば、通常の復号処理よりも高速に解読に成功した。

Lattice Enumeration using Extreme Pruning [Eurocrypt 2010]
Schnorr らが Eurocrypt 1995 等で発表した方法を解析し、大幅に探索空間を減らした"extreme pruning"を提案した。驚くべきことに、提案法によって、指数的な高速化が実現することが、理論と計算機実験によって示された。extreme proningによって解が見つかる確率は、例えば0.1%程度に低下するが、計算効率は1000倍以上となり、全体として探索効率が向上することが示されている。

3.3.5. その他の解読技術

Advanced Meet-in-the-Middle Preimage Attacks: First Results on Full Tiger, and Improved Results on MD4 and SHA-2 [ePrint 2010/016]

シンガポール・南洋理工大学のグオらにより、中間一致攻撃の改良によるハッシュ関数Tiger、MD4、縮約版 SHA-2 への原像攻撃が発表された。SHA-2 への攻撃は、42 段 SHA-256 の場合 $2^{251.7}$ の計算量で、また 42 段 SHA-512 の場合 $2^{494.6}$ の計算量で、原像を求めることができる。この結果はAsiacrypt 2010で発表されたが、ページ数制限のためSHA-2に対する解析結果は予稿集に記載されていない。

3.4. 暗号調査ワーキンググループ開催状況

2010 年度は、各ワーキンググループ（WG）が活動した主要活動項目は、表 3.3 の通りである。

表 3.3　2010 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
リストガイド WG	手塚 悟	暗号技術の専門家並びに暗号実装・運用等に関わる専門家の知見を集約し、統一基準 1.5.2.4(1)(b)項に示される暗号鍵におけるフェーズごとの管理手順について、情報提供ならびに推奨事項を取り纏めてリストガイドの作成

3.5. 委員会開催記録

2009 年度、暗号方式委員会は、表 3.4 の通り 2 回開催された。暗号技術調査ワーキンググループは、表 3.5 の通り計 3 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。

(1) 暗号方式委員会

表 3.4　暗号方式委員会の開催

回	年月日	議題
第 1 回	2010 年 7 月 20 日	活動方針の検討、監視状況報告
第 2 回	2011 年 2 月 7 日	WG 活動報告、監視状況報告、報告書の検討

(2) 暗号技術調査ワーキンググループ

表 3.5　暗号技術調査ワーキンググループ(リストガイド)の開催

回	年月日	議題
第 1 回	2010 年 9 月 27 日	リストガイド策定方法の検討
第 2 回	2010 年 12 月 2 日	リストガイド執筆内容の論点整理と議論、ヒアリング先の検討
第 3 回	2011 年 2 月 4 日	リストガイド（案）レビュー結果に対する修正検討、残課題に関する検討

第４章 暗号技術調査ワーキンググループ

4.1. リストガイドワーキンググループ

4.1.1. 活動目的

CRYPTREC の暗号監視報告並びに国内外の暗号鍵管理等に関連する標準文書を基に、暗号技術の専門家並びに暗号実装・運用等に関わる専門家の知見を集約し、統一基準 1.5.2.4(1)(b)項に示される暗号鍵におけるフェーズごとの管理手順について、情報提供ならびに推奨事項を取り纏めて、リストガイドを作成した。

4.1.2. 委員構成（敬称略、五十音順）

主査： 手塚 悟 （東京工科大学）
委員： 稲葉 厚志 （GMO グローバルサイン株式会社）
委員： 佐野 文彦 （東芝ソリューション株式会社）
委員： 羽根 慎吾 （株式会社日立製作所）
委員： 松尾 真一郎 （独立行政法人情報通信研究機構）
委員： 盛合 志帆 （ソニー株式会社）
委員： 山村 明弘 （秋田大学）
委員： 渡辺 創 （独立行政法人産業技術総合研究所）

4.1.3. 活動方針

本年度の活動項目としては、電子政府システムにおける一般的なガイドについて作成を行うべく、米国における鍵管理の標準である NIST SP 800-57 をベースに、電子政府推奨暗号リストに掲載される公開鍵及び共通鍵暗号について、暗号鍵管理における暗号鍵の生成、有効期限の設定、廃棄、更新、鍵が露呈した場合の各フェーズを検討範囲とした。

4.1.4 活動概要

第 1 回 WG（2010 年 9 月 27 日）では、今年度作成するリストガイド（鍵管理）の執筆内容、作業内容について議論を行った。作業方針としては、事務局で文書作成を行い、作業過程で生じた論点について WG で討議を行うとともに、委員各位にレビューを実施していただき、その結果を反映していくこととなった。また、実務経験者へのヒアリング等を行い、内容の充実をはかることとなった。本年度作成するリストガイド（鍵管理）の記述範囲に

ついては、個別システムを念頭に作業ならびにレビューを実施することとなったが、具体的な個別システムについては言及しないこととなった。加えて、個別の暗号プリミティブに関する情報については、監視報告の結果を流用するにとどめ、具体的なパラメータ等の扱いは時間的制約から別途検討することとなった。

第 2 回 WG（2010 年 12 月 2 日）では、作業過程で抽出された論点について議論を行うとともに、レビューの実施要領について合意した。議論を行った論点と議論の概要を以下に示す。

■　論点 1　鍵の種類に関する取り扱い範囲

- 鍵共有、権限付与に関する鍵は除外する
- 擬似乱数生成器については、リストガイド（擬似乱数生成器）への参照を行う
- SP 800-131 に示される鍵長および有効期限については、米国連邦政府機関内での推奨であることを鑑み、CRYPTREC としての取扱いを検討する必要がある
- 証明書の種類に応じ様々な有効期限があるが、今年度は電子署名法に準拠し「最長 5 年」とし、個別事例については今後の課題とする
- 日本の電子政府の実態に即した鍵の分類に関する議論を行う必要があるが、時間的制約から今後の検討課題とする
- 昨今の社会情勢を鑑み、権限付与に関する鍵の取扱いについても検討が必要である
- IPsec をはじめとする暗号プロトコルにおける暗号鍵の取扱いについて、リストガイド（鍵共有）およびリストガイド（暗号プロトコルにおける暗号鍵管理）の作成が必要である

■　論点 2　鍵の有効期限の設定指針

- 将来的な鍵の伸長について将来的な鍵長の扱いについて言及を行うべきである
- 有効期限切れ後の対応について、共通鍵の場合については検討が必要である

■　論点 3　危殆化時の手順

- 鍵の漏洩時の対策に限定する
- 共通鍵暗号において具体的な対策を提供できない場合の取扱いについて検討が必要である
- 章のタイトルを内容に合わせて修正すべきである

■　論点 4　SP 800-57 で参照されるドキュメントの取扱い

- FIPS 140-2 に言及される部分については「ISO 19790 に準拠」に修正すること

■　論点 5　その他（用語等）

- レビューにて対応する

第 2 回 WG 終了後、12 月 22 日から 1 月 11 日までの期間で、リストガイド（鍵管理）素案に関する委員レビューを実施した。

第 3 回 WG（2011 年 2 月 4 日）では、委員レビューの結果を集約し、18 の検討項目について議論を行った。主な検討項目とその概要を以下に示す。

■ 暗号技術の用途と異なる用途での鍵の利用

- 同一の鍵を別用途で利用してよいか、電子政府の現状を踏まえてその可否を検討することが必要である

■ 署名生成鍵等の有効期限について

- 今年度のリストガイド（鍵管理）では、長期署名等は取り扱い範囲外としたが、今後検討を行う必要がある
- 署名生成鍵の有効期間と証明書の有効期間を分けて、今後検討を行う必要がある。署名生成鍵と署名検証鍵の有効期間と証明書の有効期間の関係など、法制度等も含めて検討する必要がある

■ 鍵の廃棄手順について

- コピーなどが行われている場合には、トレースや消去したことを確認する必要があるが、技術的な保証と枠組みとしての保証が必要である
- 今年度は、可能な範囲でまとめて、次年度以降の課題とする

4.1.5 成果概要

ワーキンググループの活動結果、SP 800-57 をベースに、2010 年度版のリストガイドをとりまとめた。その目次を以下に示す。

目次

5.1.2　完全性
5.1.3　守秘性
5.1.4　用途またはアプリケーションとの関係性
5.1.5　その他のエンティティとの関係性
5.1.6　その他関連情報との関係性
5.2　ストレージ上での鍵の保護
5.2.1　可用性
5.2.2　完全性
5.2.3　守秘性
5.2.4　用途またはアプリケーションとの関係性
5.2.5　その他のエンティティとの関係性
5.2.6　その他関連情報との関係性

詳細については、別冊の 2010 年度版リストガイドを参照のこと。

4.1.6　今後の予定

暗号方式委員会では、2011 年度においても継続的に電子政府推奨暗号に対する監視活動を実施する、また、2010 年度に第 1 次評価を実施した応募暗号技術のうち、継続評価と決まった暗号技術について現在の電子政府推奨暗号リストに掲載されている暗号技術に対する優位性を中心に、第 2 次評価を実施する。さらに、急激な安全性の低下が発生した場合の暗号方式委員会の役割、および活動についての議論を行う。

また、2010 年度に鍵管理について実施した暗号技術調査ワーキンググループ活動については、典型的な暗号技術における鍵管理手法などについて、継続してリストガイドの作成を実施する。

付録 1

電子政府推奨暗号リスト

平成 15 年 2 月 20 日
総　　務　　省
経　済　産　業　省

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSASSA-PKCS1-v1_5
		RSA-PSS
	守秘	RSA-OAEP
		RSAES-PKCS1-v1_5(注 1)
	鍵共有	DH
		ECDH
		PSEC-KEM(注 2)
共通鍵暗号	64 ビットブロック暗号(注 3)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES(注 4)
	128 ビットブロック暗号	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
		SC2000
	ストリーム暗号	MUGI
		MULTI-S01
		128-bit RC4(注 5)
その他	ハッシュ関数	RIPEMD-160(注 6)
		SHA-1(注 6)
		SHA-256
		SHA-384
		SHA-512
	擬似乱数生成系(注 7)	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

注釈：

(注 1)　SSL3.0/TLS1.0 で使用実績があることから当面の使用を認める。

(注 2)　KEM (Key Encapsulation Mechanism) -DEM(Data Encapsulation Mechanism)構成における利用を前提とする。

(注 3)　新たな電子政府用システムを構築する場合、より長いブロック長の暗号が使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。

(注 4)　3-key Triple DES は、以下の条件を考慮し、当面の使用を認める。

1) FIPS46-3 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

(注 5)　128-bit RC4 は、SSL3.0/TLS1.0 以上に限定して利用することを想定している。なお、リストに掲載されている別の暗号が利用できるのであれば、そちらを使用することが望ましい。

(注6)　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。

(注7)　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。したがって、ここに掲載する擬似乱数生成アルゴリズムは「例示」である。

別添

電子政府推奨暗号リストに関する修正情報

修正日付	修正箇所	修正前	修正後	修正理由
平成 17 年 10 月 12 日	注釈の注 4)の 1)	FIPS46-3 として規定されていること	SP800-67 として規定されていること	仕様変更を伴わない､仕様書の指定先の変更

付録 2

電子政府推奨暗号リスト掲載暗号の問い合わせ先一覧

1. 公開鍵暗号技術

暗号名	DSA
関連情報	仕様 ・NIST Federal Information Processing Standards Publication 186-2 (+ Change Notice) (January 2000, Change Notice 1 は October 2001), Digital Signature Standard (DSS) で規定されたもの。 ・ 参照 URL <http://csrc.nist.gov/publications/PubsFIPS.html>

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://jp.fujitsu.com/group/labs/techinfo/technote/crypto/ecc.html 英文：http://jp.fujitsu.com/group/labs/en/techinfo/technote/crypto/ecc.html
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：soft-crypto-ml@ml.css.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/> 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	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.2.1) ・参照 URL <http://www.rsa.com/rsalabs/node.asp?id=2124> 和文： なし 英文： http://www.rsa.com/rsalabs/node.asp?id=2005
問い合わせ先	〒100-0005 東京都千代田区丸の内 1-3-1 東京銀行協会ビルヂング 13F RSA セキュリティ株式会社 ソリューション営業本部 副本部長 齊藤賢一 TEL：03-5222-5210, FAX：03-5222-5270, E-MAIL：ksaito@rsasecurity.com

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.2.1) ・参照 URL <http://www.rsa.com/rsalabs/node.asp?id=2124> 和文：　なし 英文：　http://www.rsa.com/rsalabs/node.asp?id=2125
問い合わせ先	〒100-0005 東京都千代田区丸の内 1-3-1 東京銀行協会ビルヂング 13F RSA セキュリティ株式会社 ソリューション営業本部 副本部長　齊藤賢一 TEL：03-5222-5210, FAX：03-5222-5270, E-MAIL：ksaito@rsasecurity.com

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.2.1) ・参照 URL <http://www.rsa.com/rsalabs/node.asp?id=2124> 和文：　なし 英文：　http://www.rsa.com/rsalabs/node.asp?id=2146
問い合わせ先	〒100-0005 東京都千代田区丸の内 1-3-1 東京銀行協会ビルヂング 13F RSA セキュリティ株式会社 ソリューション営業本部 副本部長　齊藤賢一 TEL：03-5222-5210, FAX：03-5222-5270, E-MAIL：ksaito@rsasecurity.com

暗号名	RSAES-PKCS1-v1_5
関連情報	仕様 ・PKCS#1 RSA Cryptography Standard (Ver.2.1) ・参照 URL < http://www.rsa.com/rsalabs/node.asp?id=2125>
問い合わせ先	〒100-0005 東京都千代田区丸の内 1-3-1 東京銀行協会ビルヂング 13F RSA セキュリティ株式会社 ソリューション営業本部 副本部長　齊藤賢一 TEL：03-5222-5210, FAX：03-5222-5270, E-MAIL：ksaito@rsasecurity.com

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/>　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。
関連情報 2	仕様 ・NIST Special Publication 800-56A (March 2007), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revides) 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://csrc.nist.gov/publications/PubsSPs.html>

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://jp.fujitsu.com/group/labs/techinfo/technote/crypto/ecc.html 英文:http://jp.fujitsu.com/group/labs/en/techinfo/technote/crypto/ecc.html
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：soft-crypto-ml@ml.css.fujitsu.com
関連情報 2	仕様 ・NIST Special Publication SP 800-56A (March 2007), Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revides) において、C(2,0,ECC CDH)として規定されたもの。 ・参照 URL <http://csrc.nist.gov/publications/PubsSPs.html>

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 情報流通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@lab.ntt.co.jp

2. 共通鍵暗号技術

暗号名	CIPHERUNICORN-E
関連情報	公開ホームページ 和文：http://www.nec.co.jp/cced/SecureWare/advancedpack/index.html
問い合わせ先	〒211-8666 川崎市中原区下沼部 1753 日本電気株式会社　第二 IT ソフトウェア事業部 セキュリティ G TEL：03-3454-3388 E-MAIL: https://www.nec.co.jp/cgi-bin/contact/input.cgi

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) 東芝 研究開発センターコンピュータ・ネットワークラボラトリー 主任研究員 秋山浩一郎 TEL：044-549-2156, FAX：044-520-1841 E-MAIL:crypt-info@isl.rdc.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	〒100-8310　東京都千代田区丸の内 2-7-3（東京ビル） 三菱電機株式会社　インフォメーションシステム事業推進本部 情報セキュリティ推進センター　担当課長　畠山有子 TEL:03-3218-3406　FAX:03-3218-3638 E-MAIL:Hatakeyama.Yuko@aj.MitsubishiElectric.co.jp

暗号名	Triple DES
関連情報	仕様 ・NIST SP 800-67 (Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, May 2004) ・参照 URL〈http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf〉

暗号名	AES
関連情報	仕様 ・FIPS PUB 197, Advanced Encryption Standard (AES) ・参照 URL〈http://csrc.nist.gov/CryptoToolkit/tkencryption.html〉

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 情報流通プラットフォーム研究所 Camellia 問い合わせ窓口　担当 TEL. 0422-59-3456　　FAX. 0422-59-4015 E-MAIL: camellia@lab.ntt.co.jp

暗号名	CIPHERUNICORN-A
関連情報	公開ホームページ 和文： http://www.nec.co.jp/cced/SecureWare/advancedpack/index.html
問い合わせ先	〒211-8666 川崎市中原区下沼部 1753 日本電気株式会社　第二 IT ソフトウェア事業部 セキュリティ G TEL：03-3454-3388 E-MAIL: https://www.nec.co.jp/cgi-bin/contact/input.cgi

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) 東芝 研究開発センターコンピュータ・ネットワークラボラトリー 主任研究員 秋山浩一郎 TEL：044-549-2156, FAX：044-520-1841 E-MAIL:crypt-info@isl.rdc.toshiba.co.jp

暗号名	SC2000
関連情報	公開ホームページ 和文： http://jp.fujitsu.com/group/labs/techinfo/technote/crypto/sc2000.html 英文: http://jp.fujitsu.com/group/labs/en/techinfo/technote/crypto/sc2000.html
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：crypto-ml@ml.soft.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	〒244-8555 神奈川県横浜市戸塚区戸塚町 5030 番地 (株) 日立製作所 ソフトウェア事業部 システム管理ソフトウェア本部　担当本部長　松永和男 TEL： 045-862-8498,　FAX： 045-865-9055 E-MAIL： kazuo_matsun.bz@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	〒244-8555 神奈川県横浜市戸塚区戸塚町 5030 番地 (株) 日立製作所 ソフトウェア事業部 システム管理ソフトウェア本部　担当本部長　松永和男 TEL： 045-862-8498,　FAX： 045-865-9055 E-MAIL： kazuo_matsun.bz@hitachi.com

暗号名	RC4
関連情報	仕様 ・問い合わせ先 EMC ジャパン株式会社 RSA 事業本部(http://japan.rsa.com) ・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.rsa.com/rsalabs/node.asp?id=2149>

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, SHA-256, SHA-384, SHA-512
関連情報	仕様 ・FIPS PUB 186-2, Secure Hash Standard (SHS) ・参照 URL <http://csrc.nist.gov/CryptoToolkit/tkhash.html>

4. 擬似乱数生成系

暗号名	PRNG in ANSI
関連情報	仕様

	・ANSI X9.42-2001, Public Key Cryptography for The Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography ・参照 URL <http://www.x9.org/> 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	**PRNG in ANSI X9.62-1998 Annex A.4**
関連情報	仕様 ・ANSI X9.62-1998, Public Key Cryptography for The Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA) ・参照 URL <http://www.x9.org/> 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	**PRNG in ANSI X9.63-2001 Annex A.4**
関連情報	仕様 ・ANSI X9.63-2001, Public Key Cryptography for The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography ・参照 URL <http://www.x9.org/> 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	**PRNG for DSA in FIPS PUB 186-2 Appendix 3**
関連情報	仕様 ・FIPS PUB 186-2, Digital Signature Standard (DSS) ・参照 URL <http://csrc.nist.gov/CryptoToolkit/tkrng.html>

暗号名	**PRNG for general purpose in FIPS PUB 186-2 (+ change notice 1) Appendix 3.1**
関連情報	仕様 ・FIPS PUB 186-2, Digital Signature Standard (DSS) ・参照 URL <http://csrc.nist.gov/CryptoToolkit/tkrng.html>

暗号名	**PRNG in FIPS PUB 186-2 (+ change notice 1) revised Appendix 3.1/3.2**
関連情報	仕様 ・FIPS PUB 186-2, Digital Signature Standard (DSS) ・参照 URL <http://csrc.nist.gov/CryptoToolkit/tkrng.html>

付録 3

応募暗号技術等に関する安全性評価報告書(2010 年度版)

1　128 ビットブロック暗号

1.1　CLEFIA

1.1.1　技術概要

128/192/256 ビットの鍵長をサポートする 128 ビット共通鍵ブロック暗号である。データ処理部は 4 系列 type2 一般化 Feistel 構造であり、128 ビット鍵長の場合は 18 ラウンド構成、192 ビット鍵長の場合は 22 ラウンド構成、256 ビット鍵長の場合は 26 ラウンド構成である。鍵処理部はデータ処理部と同様の構造であり、128 ビット鍵長の時は 4 系列 12 段構成、192/256 ビット鍵長の時は 8 系列 10 段構成となる。拡大鍵の代わりに定数が入力される。データ処理部と鍵処理部が同じ構造であるため、データ処理部の安全性評価をそのまま関連鍵攻撃の安全性評価に適用できる特徴がある。

1.1.2　安全性評価

差分攻撃　基本的には active S-box 数をカウントすることによる評価であるが、自己評価時よりも以下の点で詳細な解析が行われている。

- ラウンド関数で用いられている 2 種類の S-box(S_0, S_1) の差分確率を独立に使用
- Viterbi 探索を用いた差分パスの存在確認

その結果、128/192/256 ビットの鍵長に対する上界が、自己評価時にはそれぞれ $2^{-205.48}$、$2^{-256.85}$、$2^{-303.55}$ であるのに対し、それぞれ $2^{-227.42}$、$2^{-282.78}$、$2^{-338.46}$ と、より精密な評価となった。鍵長に基づく安全性指標を上回る段数がそれぞれ 12 ラウンド、16 ラウンド、20 ラウンドであり十分な安全性を有すると結論付けることができる。

不能差分攻撃　既存の評価結果である辻原 [1] らの結果が現時点における最良パスであることが確認された。これは 9 段の不能差分パスを用いて 12 段構成が攻撃可能とするものであり、仕様構成に対して十分な安全性を有すると結論付けることができる。

線形攻撃　差分攻撃同様の詳細な評価が行われた。その結果、128/192/256 ビットの鍵長に対する上界が、自己評価時にはそれぞれ $2^{-201.48}$、$2^{-240.90}$、$2^{-289.08}$ であるのに対し、それぞれ $2^{-222.54}$、$2^{-277.38}$、$2^{-331.38}$ と、より精密な評価となった。鍵長に基づく安全性指標を上回る段数がそれぞれ 12 ラウンド、16 ラウンド、21 ラウンドであり十分な安全性を有すると結論付けることができる。

高階差分攻撃 (飽和攻撃)　高階差分特性については自己評価時と同様に 32 階差分による 6 段の高階差分特性が存在することが確認された。自己評価時にはこの特性を利用し 8 段 96 階差分特性へ拡大し、10 段構成が攻撃可能であると報告されている。同様の性質を用いた攻撃手法に角尾らによるバランス状態 [2] を用いてより効果的な手法が検討された。その結果、同じ段数構成に対してより少ない選択平文組数と計算量で攻撃が可能であることが明らかとなったが、仕様構成に対しては攻撃が実行できないことが明らかとなった。

その結果、仕様構成は高階差分攻撃に対して十分な安全性を有すると結論付けることができる。

補間攻撃及び代数的攻撃　2 種類の S-box(S_0, S_1) のブール多項式表現を求め、次数がそれぞれ 6 次、7 次であることが確認された。自己評価時は段数の上昇に伴い単純に 6 または 7 のべき乗で評価されているが、実際には 2 段目及び 3 段目ではそれを下回り、それぞれ 28 次、31 次であることが確認された。

しかしながら仕様構成に対して適用すると自己評価時の結論と同様に補間攻撃や代数攻撃の実行は困難であることが確認された。

関連鍵攻撃・弱鍵　関連鍵攻撃や弱鍵の発見につながる特性は発見されていないが、鍵処理部に関して以下のような特徴が報告されている。

- **高階差分特性**

  192/256 ビット鍵長の場合、フルラウンドの 10 段構成の 32 階差分特性が存在する。また 9 段構成に対しては 8 階差分特性が存在する。これをそのまま攻撃に用いる手法は見つかっていない。

- **弱鍵組**

  中間鍵 L が all-zero もしくは all-one になる鍵 K_0 と K_1 が鍵拡大関数を逆算することで求められる。鍵処理部の仕様から K_0 及び K_1 から導出される拡大鍵のそれぞれの拡大鍵差分が求められる [3]。

今後の検討事項

- **鍵処理部の安全性評価の必要性**

  現時点では安全性に影響を与えない弱鍵組の発見であるが、CLEFIA と同様の鍵処理部構成を持つ共通鍵ブロック暗号は多数あるため、留意すべき話題である。このような特性を利用した攻撃手法に関する情報収集が必要である。特に鍵処理部の安全性評価は具体的には実施されてこなかった経緯もあるため、今後の検討が必要と考えられる。

- **関連鍵攻撃の取り扱い**

  CRYPTREC では、ブロック暗号は秘匿の目的での使用しか想定していないため、ハッシュ関数の部品として利用された場合の安全性は評価項目として挙げてこなかった。関連鍵攻撃に対する安全性の取り扱いの検討も必要である。

1.1.3　第 1 次評価としての取り扱い

仕様構成の CLEFIA に対して安全性指標である 2^{128} を下回る計算量で実行できる攻撃手法は確認されていない。現時点では十分な安全性を有すると結論できる。引き続き第 2 次評価を行うこととする。

参考文献

[1] 辻原、茂、洲崎、川崎、角尾, “CLEFIA の新たな不能差分”, 信学技報 vol.108, no.38, ISEC2008-3, pp.15–22

[2] 角尾、辻原、久保、茂、川崎,“一般化 Feistel 構造の飽和特性”, 電子情報通信学会論文誌 A, Vol.J93-A, No.4, pp.269–276, 電子情報通信学会, 2010

[3] “Evaluation of security level of CLEFIA Version 1.0,” CRYPTREC 技術報告書, No.2002, 2011. Available at `http://www.cryptrec.go.jp/report.html`

[4] “共通鍵ブロック暗号 CLEFIA の安全性評価報告書,” CRYPTREC 技術報告書, No.2001, 2011. Available at `http://www.cryptrec.go.jp/report.html`

1.2 HyRAL

1.2.1 技術概要

128~256 ビットの鍵長をサポートする 128 ビット共通鍵ブロック暗号である。G_1,G_2,F_1,F_2 の 4 種類の関数で構成され、それぞれ 4 段の 4 系列変形 Feistel 構造を有する。鍵長は 128~256 ビットをサポートし、128 ビット鍵長の時は計 24 段構成、129~256 ビット鍵長の時は計 32 段構成である。鍵処理部は G_1,G_2 で構成され 128 ビット鍵長の時 Single Key Mode で動作し、129 ビット以上の時は Double Key Mode で動作する。

1.2.2 安全性評価

差分攻撃　active S-box 数をカウントすることによる評価であり、Viterbi 探索を用いて差分パスが検証されている。128/129~256 ビットの鍵長に対する上界が、それぞれ 2^{-222}、2^{-342} と示されている。新たに 11 段構成での active-Sbox の数は最大 21 個であり、差分特性が 2^{-126} であることが示されている [4] が仕様構成に対する安全性に問題はない。

不能差分攻撃　既存の評価である芝山らの結果 [2] が現時点で最良であることが確認された。すなわち 128/192 ビット鍵長の場合は 15 段以上、256 ビット鍵長の場合は 16 段以上で適用可能な手法が発見されていない。従って仕様構成に対する安全性に問題はないと結論できる。

線形攻撃　active S-box 数をカウントすることによる評価であり、Viterbi 探索を用いてパスが検証されている。128/129~256 ビットの鍵長に対する上界が、それぞれ 2^{-228}、2^{-318} である。自己評価時の結果が妥当であることが確認された。

高階差分攻撃 (飽和攻撃)　実質的には 4 段構成に対する特性であるが、拡大鍵が入力されていない部分があるため G_1-F_2 及び F_1-F_1 の関数結合による 8 段構成の 32 階差分特性が発見されている。HyRAL の構造において、これが攻撃手法に結びつく特性ではないため実質的にはアルゴリズムの安全性に影響はない。

補間攻撃及び代数的攻撃　各関数で使用されている S-box 及び MDS の仕様から、“Full-Diffusion”が達成されているので適用は困難であると結論できる。

関連鍵攻撃・弱鍵　256 ビット鍵に対しては 2^{50} 組の等価鍵ペアが存在することが示されている。また等価鍵の導出アルゴリズムが提示されており、必要な計算量は $2^{48.8}$ であり実際の導出が可能なレベルである。本攻撃手法は 128~255 ビット鍵長の場合は有効ではない。鍵長を長くすることで安全性を高めるはずが、等価鍵の排除という運用的な問題が発生することを示している [1]。

今後の検討事項　128 ビットより長い鍵長の安全性について

CRYPTREC では 2^{128} より大きい安全性を有することが要求されている。この安全性指標は 128 ビット鍵長の場合は適切であるが、それより長い鍵長の場合は適切とは言えない。192/256 ビット鍵長に対する安全性指標について検討すべきである。

1.2.3　第 1 次評価としての取り扱い

128 ビット鍵長から 255 ビット鍵長においては、現在のところ問題点は見つかっていないが、256 ビット鍵長の場合、極小的な数であるが等価鍵の発見及び現実的な計算量での導出法が示された。よって、現リストに掲載されている暗号技術と同等以上の安全性を持たないと判断し、第 1 次評価までで評価終了とする。

参考文献

[1] 浅野, 柳原, 岩田, “256 ビット鍵 HyRAL の等価鍵”, 暗号と情報セキュリティシンポジウム SCIS 2011, 予稿集 2B2-3, 2011

[2] 芝山, 五十嵐, 金子, 半谷 “共通鍵ブロック暗号 HyRAL の不能差分攻撃について”, 情報科学フォーラム FIT 2010, 予稿集 L-022, 2010

[3] CRYPTREC シンポジウム 2010 応募暗号説明会

[4] “Security Analysis of HyRal,” CRYPTREC 技術報告書, No.2004, 2011. Available at http://www.cryptrec.go.jp/report.html

[5] “HyRAL 安全性評価報告書,” CRYPTREC 技術報告書, No.2003, 2011. Available at http://www.cryptrec.go.jp/report.html

2 ストリーム暗号

2.1 Enocoro-128v2

2.1.1 技術概要

Enocoro-128v2 は、Enocoro の初期版は 2007 年に提案された擬似乱数生成器 (ストリーム暗号) であり [1]、CRYPTREC に応募された方式は、Enocoro-128v2 と呼ばれる Enocoro の中では最新の方式である [3]。128 ビットの鍵、64 ビットの初期値 (IV) を入力として、最大で 2^{64} バイトの鍵ストリームを生成する[1]。内部状態は 272 ビット (34 バイト) あり、PANAMA 型と呼ばれる構造をしている。

2.1.2 安全性評価結果

タイム-メモリ-データ-トレード-オフ攻撃 (TMDTO 攻撃)　Enocoro は内部状態 272 ビット、鍵サイズ 128 ビットある。TMDTO 攻撃に関しては、Babbage-Golić 及び Biryukov-Shamir により提案されている方法があるが、現時点において、特に問題点は認められなかった。

推測決定攻撃　計算量が 2^{152} を下回るものは見つからなかったので、現時点においては、特に問題点は認められない。

分割統治攻撃　Enocoro の内部状態は、$a^{(t)}$ と $b^{(t)}$ からなり、状態更新関数は、ρ と λ という 2 つの関数からなる。どちらの関数にも、$a^{(t)}$ と $b^{(t)}$ の両方が入力されるので、分割統治攻撃を適用することは困難であると考えられる [4]。

代数的攻撃　自己評価書 [4] では、Cube 攻撃 [7] に対する安全性評価の記述はないが、s_8 の代数次数は 6 であり、s_8 をブール多項式で表現したとき、各出力ビットの入力ビットに関する項の出現頻度が密であることから、Cube 攻撃には耐性があるものと考えられる。他の代数的攻撃に対しても、特に問題点は認められなかった。

識別攻撃　乱数との識別性については、偏差が 2^{-180} を上回るものは見つからなかったので、現時点においては、特に問題点は認められない。

線形攻撃　s_8 の最大線形確率 $p = 2^{-4}$ なので、active S-Box の最小数が 32 以上になると攻撃に対して安全と考えられる。条件付きで探索した結果、最大差分特性確率が 2^{-128} を上回る証拠は得られなかったので、現時点においては、特に問題点は認められない。

[1] 仕様書において、「Enocoro-128v2 では、1 組の鍵と初期ベクトルに対して 2^{64} バイトより大きな鍵ストリームを生成してはならない。」と記載されている。

差分攻撃　s_8 の最大差分確率 $p = 2^{-4.678}$ なので、active S-Box の最小数が 28 以上になると攻撃に対して安全と考えられる。条件付きで探索した結果、最大差分特性確率が 2^{-128} を上回る証拠は得られなかったので、現時点においては、特に問題点は認められない。

- 選択 IV 攻撃については、現時点においては、特に問題点は認められなかった。
- 関連鍵攻撃については、現時点においては、特に問題点は認められなかった。

その他

- Maximum Degree Monimial Test については、現時点においては、特に問題点は認められなかった。
- 統計的性質については、現時点においては、特に問題点は認められなかった。

安全性評価結果のまとめ　現時点において、特に安全性に問題点は認められなかった。

2.1.3　第 1 次評価としての取り扱い

2.1.2 節に示された評価結果から、引き続き第 2 次評価を行うこととする。

参考文献

[1] D. Watanabe and T. Kaneko, ”A construction of light weight Panama-like keystream generator,” IEICE Technical Report, ISEC2007-78, 2007 (in Japanese).

[2] K. Muto, D. Watanabe, and T. Kaneko, “Security evaluation of Enocoro-128 against linear resynchronization attack,” The 2008 Symposium on Cryptography and Information Security, SCIS 2008, 4A1-1, January 2008 (in Japanese).

[3] D. Watanabe, T. Owada, K. Okamoto, Y. Igarashi, and T. Kaneko, “Update on enocoro stream cipher,” In International Symposium on Information Theory and its Applications (ISITA), 2010, pages 778-783, 2010.

[4] 株式会社日立製作所, “疑似乱数生成器 Enocoro 評価書,” http://www.cryptrec.go.jp/topics/cryptrec_20101001_callforattack.html、2010.

[5] “Enocoro-128v2 の安全性評価,” CRYPTREC 技術報告書, No.2007, 2011. Available at http://www.cryptrec.go.jp/report.html

[6] ”Security Evaluation of Stream Cipher Enocoro-128v2,” CRYPTREC 技術報告書, No.2008, 2011. Available at http://www.cryptrec.go.jp/report.html

[7] I. Dinur and A. Shamir, “Cube Attacks on Tweakable Black Box Polynomials,” In A. Joux, editor, Advances in Cryptology—EUROCRYPT 2009, Volume 5479 of Lecture Notes in Computer Science, pages 278-299. Springer-Verlag, 2009.

2.2 KCipher-2

2.2.1 技術概要

KCipher-2 は、SASC2007 において K2 という名前 (商標上の理由で KCipher-2 に変更) で最初のバージョン [1] が示され、後に、SECRYPT2007 において K2 v2.0 という名前で初期化処理等を修正したバージョン [2] が示されている。32 ビットワードの FSR(feedback shift register) のフィードバック関数に対して、DFC(dynamic feedback control) を行う擬似乱数生成器 (ストリーム暗号) である[2]。128 ビットの鍵サイズ、128 ビットの初期値 (IV) を入力として、鍵ストリームとして 1 サイクルあたり 32 ビットワードを 2 つ出力する。

2.2.2 安全性評価結果

タイム-メモリ-データ-トレード-オフ攻撃 (TMDTO 攻撃)　KCipher-2 の内部状態のサイズは 512 以上である。現時点においては、特に問題点は認められない。

推測決定攻撃　現時点においては、特に問題点は認められなかった。

代数的攻撃　連立方程式の数と変数の数に関して考察したが、現時点においては、特に問題点は認められなかった。

識別攻撃

- 乱数との識別性については、Modular Addition を Exclusive OR に代えて、非線形関数に関する評価を行ったところ、偏差が 2^{-156} を上回るものは見つからなかったので、現時点においては、特に問題点は認められない。
- Ideal cipher との識別性については、Mod n 攻撃 [6] に関して、縮小版に対する Mod n 攻撃について検討した結果、問題点は認められなかった。

相関攻撃　現時点においては、特に問題点は認められなかった。

差分攻撃

- 関連鍵攻撃については、最大差分特性確率が 2^{-198} で押さえられているので、現時点においては、特に問題点は認められない。
- 関連 IV 攻撃については、最大差分特性確率が 2^{-180} で押さえられているので、現時点においては、特に問題点は認められない。
- 関連鍵／IV 攻撃については、8 ラウンド後に active S-Box の最小数は 32 となったので、現時点においては、特に問題点は認められない。

[2]仕様書において、「再初期化は、最大で 2^{58} クロック (2^{64} ビットの鍵ストリーム出力) 以内に行うことを強く推奨する。この場合, 同一の初期鍵や同一の初期ベクトルは、2^{58} クロックを超えて使用されない。」と記載されている。

その他

- 周期と線形複雑度については、現時点においては、特に問題点は認められなかった。
- 統計的性質については、現時点においては、特に問題点は認められなかった。

安全性評価結果のまとめ　現時点において、特に安全性に問題点は認められなかった。

2.2.3　第 1 次評価としての取り扱い

2.2.2 節に示された評価結果から、引き続き第 2 次評価を行うこととする。

参考文献

[1] S. Kiyomoto, T. Tanaka, and K. Sakurai, "A Word-Oriented Stream Cipher Using Clock Control," Proc. of SASC2007, pp.260-273, 2007.

[2] S. Kiyomoto, T. Tanaka, and K. Sakurai, "K2: A Stream Cipher Algorithm Using Dynamic Feedback Control," Proc. of SECRYPT2007, pp.204-213, 2007.

[3] 株式会社 KDDI 研究所, KCipher-2 自己評価書, http://www.cryptrec.go.jp/topics/cryptrec_20101001_callforattack.html, 2010.

[4] KCipher-2 の安全性に関する評価, CRYPTREC 技術報告書, No.2009, 2011. Available at http://www.cryptrec.go.jp/report.html

[5] Security Evaluation of the K2 Stream Cipher, CRYPTREC 技術報告書, No.2010, 2011. Available at http://www.cryptrec.go.jp/report.html

[6] J. Kelsey, B. Schneier, and D. Wagner, "Mod n Cryptanalysis, with Applications Against RC5P and M6," In L. R. Knudsen, editor, FSE, volume 1636 of Lecture Notes in Computer Science, pages 139-155. Springer, 1999.

3 メッセージ認証

3.1 PC-MAC-AES

3.1.1 技術概要

使用するブロック暗号の証明可能安全性を狙いとし、CMAC のモードの構成を利用した構成となっている。また，高速処理を狙いとし、ブロック暗号として用いるアルゴリズムを、full-AES の代わりに 4-round AES を用いた構成となっている。AES の 4 段関数へは AES の暗号化関数を用いた鍵スケジュールにより鍵を設定している。

処理速度を比較すると，PC-MAC-AES は、CBC MAC に比べ 1.4 〜 2.5 倍 処理速度が速い。

3.1.2 安全性評価結果

安全性評価については、提案者から安全性証明が示されているが、評価者による証明の見直しにより、攻撃者成功確率について upper bound が見直されている [1]。また、評価者による解析結果から、新たに得られた結果がいくつか挙げられている [2]。以下に両評価者の評価結果の概要をまとめる。

[証明可能安全性] ：提案者らが示した安全性評価では、ある (短いメッセージ長しか問い合わせないような) 限定的な攻撃者を想定した評価となっており、攻撃者の成功確率の upper bound を $O(q^2\rho^2/2^n)$ として見積もり、上記の場合必要となる time complexity は 2^{56} だと示している。(ここで，q は クエリの最大回数、ρ は 1 回のクエリで問える最大ブロック長、n は出力ビット長) 評価者は，より一般的な攻撃者の設定の下で、提案者らが示した論拠に基づくと、time complexity は，提案者らが示した程 (2^{56}) までには到達できず、もっと小さく (2^{33} 程度に) なってしまうことを指摘した。

一方、評価者自らの証明手法を用いてより一般的な攻撃者の設定の下で、攻撃者の成功確率の upper bound を $O(q\sigma^2/2^n)$ に抑えられることを示した。上記の場合必要となる time complexity は 2^{42} だと示している。(σ は q クエリで得られたトータルのブロック長)

更に別の手法で証明を行い，攻撃者の成功確率の upper bound を $O(\sigma^2/2^n)$ で抑えられることを示した。上記の場合必要となる time complexity は 2^{56} だと示している。

[解析] : PC-MAC の構成は、以下のようなカテゴリに属すると考えられる。

- CBC-MAC
  - MacDES
  - EMAC
    - TMAC
      - CMAC
      - PC-MAC

上記カテゴリに基づき、PC-MAC に適用可能な解析について、表 1 に示すように、網羅的に示した。

本評価結果では、新たに、Subkey Recovery 攻撃が示せ、また、RF(Random Permutation) から識別可能であることが示された。

更に、PC-MAC に 4 ラウンドの AES を用いた場合の解析も行い、新たな攻撃方法も示された。(ここで提案された攻撃は，PC-MAC に閉じたものではなく、CBC-MAC に属するいずれの方式にも適用可能なものである。)

総じて，評価者の示した全ての攻撃法の計算量は、提案者の示した安全性証明のバウンドよりも多くのコストを必要とするものであった。

- PC-MAC の構造に起因する攻撃：今回の評価で新たに Subkey-recovery attack,、Distinguish PC-MAC-AES from PC-MAC-AES-RP が示された。
  - Subkey-recovery attacks: PC-MAC-AES は、従来知られている、TMAC の L をリカバする攻撃は、PC-MAC-AES にも適用でき、内部の処理に用いられている Subkey L をリカバできる。L がリカバできると、L を用いて、簡単に各ブロックで用いられている Subkey を全てリカバすることができる。其々の subkey を求めるのに必要となるコストは、(攻撃者が選択した) 1 クエリのみである。トータルで必要となるコストは、2^{65} クエリである。
  - Distinguish PC-MAC-AES from PC-MAC-RP: PC-MAC を RP(Random Permutation) を用いて構成した場合と 4-round AES を用いて構成した場合とを識別できることを示した。必要となるコストは、2^{65} クエリ である。
- 4 ラウンド AES を用いた場合の解析：各ラウンドに用いられている Subkey $K1$、$K2$、$K3$、$K4$ を求める攻撃手法を示した。4 ラウンド AES を用いた CBC-MAC に分類される構造に汎用的に適用できるものである。4 ラウンド AES を用いた CBC-MAC は、2^{67} の クエリと 2^{40} の 計算量でラウンド鍵と中間値を求めることができる。

3.1.3 第 1 次評価としての取り扱い

3.1.2 に示された両評価者による評価結果から、事務局としては、以下の点についてさらに評価検討が必要であるとの見解を得た。引き続き第 2 次評価を行うこととする。

- 安全性証明に関し、評価の異なる結果に対するそれぞれの結果の妥当性、適切性、および、評価者によって示された攻撃の有効性・現実的脅威の検討。
- CMAC に対する優位性の検討。

  CMAC は、一部で 4 ラウンドの AES を用いると、CMAC の方が PC-MAC-AES に比べコンパクトな実装が可能と思われるが、安全性証明がつけられるかは自明ではない。よって、両方式の検討、比較が必要である。
- (似た構造を持つ PELICAN や alpha-MAC 等に対して、サイドチャネル攻撃も用いた攻撃は示されているので、) サイドチャネル攻撃などと組み合わせた場合の脆弱性について検討する必要がある。

表 1: On Security Margin Loss of CBC MAC Variants

Birthday Bound Attacks ($2^{n/2}$)		
Features	Applicable MACs	Attack Scenario
On-the-fly;	Most CBC MAC variants	$\mathrm{DIS}^{\mathrm{MAC,RF}}$; Existential forgery attack; Selective forgery attack;
On-the-fly; Suffix;	EMAC; XCBC; ANSI retail MAC; TMAC, CMAC; **PC-MAC**	$\mathrm{DIS}^{\mathrm{MAC,RF}}$; Existential forgery attack; Selective forgery attack; Internal-state recovery attack; Universal forgery attack; Low complexity-on-average universal forgery attack;
On-the-fly; Suffix; Tweaking key;	XCBC; TMAC; CMAC; **PC-MAC**	$\mathrm{DIS}^{\mathrm{MAC,RF}}$; Existential forgery attack; Selective forgery attack; Internal-state recovery attack; Universal forgery attack; Low complexity-on-average universal forgery attack;
	TMAC, CMAC; **PC-MAC**;	Low complexity-on-average Internal-State-Recovery Attack
	TMAC; **PC-MAC**;	Partial-key Recovery Attack;
Specific Attacks on **PC-MAC**: Subkey Generation Algorithm		Subkey-Recovery Attack; DIS-PC-MAC$^{E_K(\cdot),\mathrm{RP}}$;
Attack beyond Birthday Bounds (2^k)		
On-the-fly; Suffix;	EMAC; XCBC; ANSI retail MAC; TMAC; **PC-MAC**;	Full-key recovery attack; (complexity: 2^{k+1})
On-the-fly; Suffix; Tweaking key;	TMAC; **PC-MAC**;	Full-key recovery attack; (complexity: 2^k)

参考文献

[1] “CRYPTREC evaluation report on PC-MAC-AES,” CRYPTREC 技術報告書, No.2006, 2011. Available at `http://www.cryptrec.go.jp/report.html`

[2] “Security Evaluation of PC-MAC-AES,” CRYPTREC 技術報告書, No.2005, 2011. Available at http://www.cryptrec.go.jp/report.html

4 事務局選出：暗号利用モード

4.1 暗号利用モード

4.1.1 技術概要

Mode of operation の各種バリエーションについての評価を行う。

今回は、対象として、17 種類のモードについての評価を実施した。FIPS198-1、ISO/IEC 9797-1、SP 800-38A、SP 800-38B、SP 800-38C、SP 800-38D、SP 800-38E に掲載される mode は、以下のように分類される。

- Confidentiality Modes : ECB, CBC, CFB, OFB, CTR, XTR
- Authenticity Modes : CMAC, HMAC, GMAC, MAC algorithms 1-6 of ISO 9797-1
- Authenticated-Encryption Modes : CCM, GCM

4.1.2 安全性評価結果

評価者による評価報告書 [1], [2] から、以下の評価結果を得た。

[Confidentiality Modes] 基本的な 4 種類のモード (ECB, CBC, CFB, OFB) については、ECB モード以外は、適応的選択平文攻撃に対する安全性証明を有しており、実用上問題となる脆弱性の指摘されていないブロック暗号を用いる場合は、ブロック長を b とし、攻撃に要するブロック暗号へのクエリ数 $O(2^{b/2})$ であると考えることができる。しかし、効率が悪く、使い方を誤りやすい。また、以下の点で注意が必要となる。

- いずれのモードも容易な適応的選択暗号文攻撃が存在する。
- CBC モードに関しては、以下の条件の下で選択平文攻撃が存在する。
  - 平文ブロックごとに暗号文が得られるような場合。
  - nonce を平文と同じ鍵で暗号化して初期ベクトル IV を生成する場合。

NIST は CBC や CFB に用いる IV として単なる nonce を用いる場合を指摘し、NIST SP 800-38A の Appendix C で改善方法を示している。[3]また，OFB の IV の生成方法については nonce であることだけが条件として示されており、識別できない値であることは求められていない。しかし、IV のシーケンスを意図的に変えることができてしまうと攻撃が存在してしまう。

CTR は、Confidentiality モードの中ではもっとも良い選択肢であるといえる。probabilistic encryption よりも強い暗号アルゴリズムの概念として定義されうる nonce-based encryption として、適応的選択平文攻撃に対する安全性証明を有する。利用する際に一度使ったカウンタの値は再度用いないこと、authenticity や nonmalleability や 選択暗号分攻撃に対する

[3]それらの方法を用いたとしても probabilistic encryption よりも強い暗号アルゴリズムの概念として定義されうる nonce-based encryption としては、安全性を示せない。

安全性を有しないことを留意すべきである。カウンタはユーザ自らの設定に依る。NICT は、NIST SP-800-38A Appendix B でどのようにカウンタを構成し、またその再利用を避けるべきかについて言及している。また、実装面については、ソフトウェア及びハードウェアいずれについても優れている。

XTR は、他のモードと異なり ストレージデバイス上のディスクの暗号化などの用途を意図して考えられており、固定長の暗号化が意識されている。繰り返し回数 (The equality of block across time) はリークしてしまうが、ブロック位置 (The equality of block across position) に関してはリークしない。(ECB mode では両方リークしてしまう。) 任意長のブロック暗号に対する安全性を確保する代わりに弱い安全性を確保しつつ効率性を重視した方式となっている。しかし、敢えてこの方式を選択するのが好ましい場合は少ないのではないかと考えられる。

[Authenticity Modes] ISO/IEC 9797-1 では、6 種類の MAC アルゴリズムが規定されている。また，3 種類のパティング法が規定されている。いくつかは、安全性証明が示されているが中には安全性証明が示されていないものもあり、具体的な攻撃が示されているものややや時代遅れなものも含まれる。また、key-separation [4] に関しては、あまりにも乱雑な取り扱いである。明確な定義がなく、それがゆえにいくつかのバリエーションではテストベクトルも提示されていない状態である。ISO/IEC 9797-1 の方式を選択する場合には、注意深い選択が必要であり、無差別に選択するのは推奨しない。推奨される MAC アルゴリズムとパティングの組み合わせは、アルゴリズム 1 とパティング 1 もしくは 3 / 2-key を用いるバージョンのアルゴリズム 2 と独立な鍵を用いる場合のパティング 2 / アルゴリズム 3 とパティング 2 / 6-key を用いるバージョン (実際には、この設定は仕様では許されていない) アルゴリズム 6 とパティング 2、が挙げられる。また、いずれの方式も、CMAC の構成には不適合である。改訂版 (ISO/IEC FDIS9797-1:2010) が間もなくリリースされる。効率性に関しては、あまり優れていない。

CMAC は、birthday-bound attack が存在するが、これは XCBC、TMAC、OMAC、EMAC いずれも同様である。実用上問題となる脆弱性の指摘されていないブロック暗号を用いる限りにおいては、適応的選択文書攻撃に対する存在的偽造不可能性、識別不能性の証明可能安全性を有する。この場合、攻撃に必要となるブロック暗号のクエリ数はブロック暗号のブロック長を b とし、$O(2^{b/2})$ となる。もし、64 ビットのブロック暗号を用いた場合には、頻繁に鍵を更新することが望ましい。実際 DES などを用いている場合には容易に鍵探索攻撃が可能となってしまう。CMAC の仕様に関連し、MAC の検証に必要となる (生成には必要ない) Sub 鍵 $K1$ と $K2$ は、付加的なものとして位置づけられているが安全性を脅かしやすいものであるので、要求仕様として取り扱った方がよい。

HMAC は、シンプルで証明可能安全性を持つよい方式である。実用上問題となる脆弱性の指摘されていないブロック暗号を用いる場合は、適応的選択文書攻撃に対する安全性証明を有する。この場合、攻撃に必要となるブロック暗号のクエリ数はブロック長を b とし、$O(2^{b/2})$ となる。また、用いるハッシュ関数として、SHA-1 を使用した場合の安全性に対する結果もいくつかあるが、実用上の脅威は報告されていない。

[4] マスター鍵からモードの繰り返し部分に用いられる鍵と出力直前に施される処理に用いられる鍵とを生成する関数 (Sep)

GMAC は、実用上問題となる脆弱性の指摘されていないブロック暗号を用いる限りにおいては、適応的選択文書攻撃に対する証明可能安全性を有しており、GMAC は適応的選択文書攻撃に対して安全な認証用暗号利用モードであると言える。ただし、証明可能安全性に関する攻撃者の優位度は構成に用いられる多数のパラメータに依存しているため、具体的に安全性の強度を測る場合には個別に解析を行うことが求められる。また、その他に挙げられる懸念点として、方式にはタグが用いられているがタグの長さ τ に対し、$2^{\tau/2}$ のクエリにより、もしくは 2^{τ} のブロックを集められれば偽造が成功することが示されている点がある。よって、使われているタグが短い場合、安全性証明の security bounds は小さくなる。また、使いきりの nonce の供給が必要とされているが、nonce を使う必要性が不明瞭である。しかも、それに基づき同じ IV が用いられた場合にはただちに GMAC の安全性は損なわれる。

[Authenticated-Encryption Modes] CCM および GCM は、nonce-based の方式である。メッセージのヘッダなどの”associated-date” を伴い、AEDAD(authenticated-encryption with associated-data) として用いられる。

CCM は、適応的選択平文攻撃に対する証明可能安全性を有しており、実用上問題となる脆弱性の指摘されていないブロック暗号を用いる場合は、ブロック長を b とし、攻撃に要するブロック暗号のクエリ数は、$O(2^{b/2})$ となる。また、GCM に比べてシンプルな構成であり、多くのアプリケーションで実装されている。しかし、処理速度が遅くオンラインでの用途に適していない。

GCM は、適応的選択暗号文攻撃に対する証明可能安全性を有しており、実用上問題となる脆弱性の指摘されていないブロック暗号を用いる限りにおいては、GCM は適応的選択暗号文攻撃に対して安全な Authenticated-Encryption Modes(守秘・認証用暗号利用モード) であると言える。但し、その安全性は多くのパラメータに依存するため、個別のケースについては、解析が重要と考えられる。特に、短いタグは用いるべきではない。(64-bit のタグでも短いと考えるべきである。) 短いタグを用いた場合、初めの偽造が容易になるだけでなく更に続けて偽造することが容易になってしまう。また、ユーザが設定する nonce について一度用いた nonce を再度用いてしまうと安全性が損なわれる。実装面に関しては、構造上並列処理が可能でありハードウェア・ソフトウェアいずれについても CCM よりも優れている。また、オンラインでの使用にも適している。

評価まとめ

[Confidentiality Modes]:

- 利用用途に応じて、慎重に適切な選択を行うべきである。
- 既に示されている脆弱性は理論的な問題にとどまらず、実際の被害を招いているものもある。
- 基本の 4 つのモード (ECB、CBC、CFB、OFB) は、既存のシステムで用いる以外には、新規では用いないことが望ましい。
- 広く実用面で使われることにより、confidentiality のみを目的としたモードであるにも拘らずそれ以外の目的に乱用されるような事態が起こりかねない。

- CTR は、Confidentiality モードの中で最も優れたモードであるといえる。

[Authenticity Modes]:

- CBC-MAC 系については、key-separation は仕様が明確でなく、取り扱い如何によっては安全性を低下させる要因になりかねない。
- CBC-MAC 系はアルゴリズムとパティング法の組み合わせ方により提供される安全性のレベルに違いが生じるので、利用用途に応じて、慎重に適切な選択を行うべきである。
- HMAC は、中で用いられている圧縮関数が衝突困難性の性質を持たない場合であっても、疑似乱数関数の性質を満していれば、その安全性を保つことができる。
- CMAC の仕様外となるが、検証に必要となる Sub 鍵についても MAC として満たすべき要求条件に含めて示したほうが望ましい。
- GMAC を用いる場合は、タグは十分な安全性が保てる長さを用いるべきである。また，一度利用した nonce の再利用はすべきではない。

[Authenticated-Encryption Modes]:

- いくつか不足する部分はあるものの、CCM および GCM いずれも AEAD(Authenticated Encryption with Associated Data) 方式として使うことはできると考えられる。
- CCM は、実装面でハードウェア・ソフトウェアいずれについても効率が悪い。
- GCM については、短いタグの使用は避けるべきである。また，一度利用した nonce の再利用はすべきではない。

4.1.3 第 1 次評価としての取り扱い

4.1.2 に示された両評価者による評価結果から、事務局としては、第 1 次評価としては以下の取り扱いとする。

- CBC-MAC 系について、key-separation の仕様が存在しない点、現在，検証に必要となる Sub 鍵は仕様外となっているが、MAC として満たすべき要求条件に含めて示した方が望ましいと考えられる点、については、推奨される仕様について検討を行う。
- 指摘のあった脆弱性については、その範囲を明らかにし、後に、使用する際の注意事項として明示する。
- 推奨される利用用途、禁じられるべき利用用途、等に関する検討。

参考文献

[1] “Evaluation of Some Blockcipher Modes of Operation,” CRYPTREC 技術報告書, No.2012, 2011. Available at http://www.cryptrec.go.jp/report.html

[2] “暗号利用モードおよびメッセージ認証コードの安全性評価,” CRYPTREC 技術報告書, No.2011, 2011. Available at http://www.cryptrec.go.jp/report.html

5　事務局選出：エンティティ認証

5.1　ISO/IEC 9798

5.1.1　技術概要

ISO/IEC 9798 は、ISO/IEC で標準化されているエンティティ認証プロトコルである。今回の評価対象となっているのは、9798 のパート 2、パート 3、パート 4 に記載されているプロトコルである。

ISO/IEC 9798-2 は共通鍵暗号技術を利用したエンティティ認証技術であり、片側認証と両側認証、信頼できる第三者機関の仮定の有無、通信の回数により 6 つに分類される。また、それぞれの方式において、Time variant parameter として、タイムスタンプ、シーケンス番号、乱数を利用する。この認証方式においては、秘密情報である認証鍵を所有している事を証明することによって認証が実現される。乱数の扱いについては ISO/IEC 18031 に従うものとされる。

ISO/IEC 9798-3 は電子署名技術を利用したエンティティ認証技術であり、片側認証と両側認証、信頼できる第三者機関の仮定の有無、通信の回数により 7 つに分類される。また、それぞれの方式において、Time variant parameter として、タイムスタンプ、シーケンス番号、乱数を利用する。この認証方式においては、秘密情報である認証鍵を所有している事を証明することによって認証が実現される。乱数の扱いについては ISO/IEC 18031 に従うものとされる。

ISO/IEC 9798-4 は暗号チェック関数（CCF）を利用したエンティティ認証技術であり、片側認証と両側認証、通信の回数により 4 つに分類される。また、それぞれの方式において、Time variant parameter として、タイムスタンプ、シーケンス番号、乱数を利用する。この認証方式においては、秘密情報である認証鍵を所有している事を証明することによって認証が実現される。乱数の扱いについては ISO/IEC 18031 に従うものとされる。

5.1.2　安全性評価結果

評価者 A は、評価対象のプロトコルについて大きな問題点を指摘しなかった。一方で、評価対象のエンティティ認証プロトコルには数多くのバリアントが存在し、電子政府システムで利用する際の選択に対して指針を与える必要性を指摘している。特に、ISO/IEC（9798-2, 9798-3, 9798-4）では、Time variant parameter として、タイムスタンプ、シーケンス番号、乱数を利用するが、その使い分けについて推奨を示す必要性を指摘している。

評価者 B は、形式化手法のツールである Scyther を用いて、プロトコル仕様、攻撃環境、セキュリティ要求などを形式化して、その安全性を検証した。Scyther は、boundedn verification と unbounded verification の両方をサポートしているが、本評価対象に対する検証においては攻撃対象のスレッドを 5、1 プロトコルに対する計算機上の評価時間を 10 分に限定した bounded verification を行っている。その結果、評価者 B はほとんどのプロトコルについては問題はないとしたものの、5 つのプロトコルと 2 つのバリアントに対して 3 つの攻撃の存在を指摘している。

Role-mixup attacks　エンティティ認証における認証の性質のうち agreement と呼ばれる性質では、交換されたデータに対する同意だけでなく、お互いのエンティティが実行した役割に関する同意も必要となる。しかし、いくつかのプトロコルでは、相手の実行した役割を確認することができない。そのため、mathcing conversation や同期への問題が発生する。例えば、9798-2-3 では、Alice が Bob が別の役割としてプロトコルを実行していると思わせることが可能となり、状態管理に問題を生じさせることができる。また、プロトコルで規定されているオプションのテキスト領域のデータの同意も崩すことができる。これらの攻撃は暗号そのものを攻撃しなくても可能である。

Role-mixup attacks は、ISO/IEC 9798-2-3 with unidirectional keys, ISO/IEC 9798-2-5, ISO/IEC 9798-3-3, ISO/IEC 9798-4-3 with unidirectional keys で指摘されている。

Type flaw attacks　エンティティの名前が、n ビットのビット列にエンコードされており、また nonce が n ビットで表現されているときに起こる攻撃が指摘されている。つまり、fresh な乱数を受け取ることが期待されている時に、エンティティの名前を誤って乱数として受け取ってしまう。この攻撃は、ISO/IEC 9798-3-7 (Five pass authentication (initiated by B)) の Option 1 で指摘されている。

Reflection attacks　Reflection attack は、Initiator と Responder が同じエンティティの場合に起きる攻撃である。このシナリオの現実性はアプリケーションに依存する。この攻撃は、ISO/IEC 9798-2-3, ISO/IEC 9798-2-5 で指摘されており、暗号化されたデータをそのままプロトコルメッセージとして再利用することで、攻撃が可能となる。これは、オプションフィールドの目的が規定されていないことに依存する、また、9798-1 で定められているセキュリティの要求にも反している。

指摘された攻撃を表 2 に示す。

問題の修正　評価者 B は指摘した問題の修正方法を提示している。

上記に指摘された攻撃は、基本的にあるエンティティから送信されたメッセージが、別のエンティティによって誤って解釈されることが原因であり、暗号によって保護されて送信されるメッセージの中にシステム共有のユニークな定数を入れる手法（tagging）によって防ぐことが可能である。この修正をプロトコルに施すことが必要である。

5.1.3　第 1 次評価としての取り扱い

5.1.2 に示された両評価者による評価結果から、第 1 次評価としては以下の取り扱いを行う。

- 指摘された攻撃については、エンティティ認証中で使われてる暗号アルゴリズムを攻撃する必要がなく、現実的に発生しうると考え、ISO/IEC 9798 を使用する際の注釈として、可能な限り使用しないように明示する。
- ただし、問題を解決する修正が示されているため、ISO/IEC に対して仕様の修正を求め、仕様の修正が完了した後に、改めて注釈の文言などについて検討を行う。

表 2: ISO/IEC 9798 に対する攻撃一覧

No	Protocol	Claim	No type checks Alice-talks-to-Alice initators	Type checks Alice-talks-to-Alice initators	No type checks No Alice-talks-to-Alice initators	Type checks No Alice-talks-to-Alice initators
1	isoiec-9798-2-3	A Agreement(B,TNB,Text3)	•	•		
2	isoiec-9798-2-3	A Weakagree	•	•		
3	isoiec-9798-2-3	B Agreement(A,TNA,Text1)	•	•		
4	isoiec-9798-2-3-udkey	A Agreement(B,TNB,Text3)	•	•	•	•
5	isoiec-9798-2-3-udkey	A Weakagree	•	•	•	•
6	isoiec-9798-2-3-udkey	B Agreement(A,TNA,Text1)	•	•	•	•
7	isoiec-9798-2-5	A Agreement(B,Kab,Text5,Text7)	•	•		
8	isoiec-9798-2-5	A Weakagree	•	•		
9	isoiec-9798-2-5	B Agreement(A,Kab,Text5)	•	•	•	•
10	isoiec-9798-3-3	A Agreement(B,TNB,Text3)	•	•	•	•
11	isoiec-9798-3-3	A Weakagree	•	•	•	•
12	isoiec-9798-3-3	B Agreement(A,TNA,Text1)	•	•	•	•
13	isoiec-9798-3-7-1	A Agreement(B,Ra,Rb,Text8)	•		•	
14	isoiec-9798-4-3	A Agreement(B,TNb,Text3)	•	•		
15	isoiec-9798-4-3	A Weakagree	•	•		
16	isoiec-9798-4-3	B Agreement(A,TNa,Text1)	•	•		
17	isoiec-9798-4-3-udkey	A Agreement(B,TNb,Text3)	•	•	•	•
18	isoiec-9798-4-3-udkey	A Weakagree	•	•	•	•
19	isoiec-9798-4-3-udkey	B Agreement(A,TNa,Text1)	•	•	•	•

参考文献

[1] “ISO/IEC 9798 プロトコルの安全性評価,” CRYPTREC 技術報告書, No.2013, 2011. Available at http://www.cryptrec.go.jp/report.html

[2] “Evaluation of ISO/IEC 9798 Protocols,” CRYPTREC 技術報告書, No.2014, 2011. Available at http://www.cryptrec.go.jp/report.html

発行日　2011年 6月 20日　第1版
発行者
・〒184-8795
東京都小金井市貫井北四丁目2番1号
独立行政法人 情報通信研究機構
（ネットワークセキュリティ研究所 セキュリティ基盤研究室、
セキュリティアーキテクチャ研究室）
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
（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