2013 年度　第 2 回暗号技術検討会

日時：平成 26 年 3 月 27 日(木) 14:00～16:00
場所：経済産業省別館 1 階 104 各省共用会議室

議　事　次　第

１．開　会

２．議　事
(1)　2013 年度　暗号技術評価委員会活動報告について【確認事項】
(2)　2013 年度　暗号技術活用委員会活動報告について【確認事項】
(3)　2013 年度　暗号技術検討会報告書（案）について【承認事項】
(4)　2014 年度　暗号技術検討会活動計画について【承認事項】
(5)　2014 年度　暗号技術評価委員会活動計画について【承認事項】
(6)　2014 年度　暗号技術活用委員会活動計画について【承認事項】
(7)　その他

３．閉　会

（資料番号）	（資　料　名）
資料１	2013 年度 暗号技術評価委員会活動報告
資料２	2013 年度 暗号技術活用委員会活動報告
資料３	2013 年度 暗号技術検討会報告書（案）
資料４	2014 年度 暗号技術検討会活動計画（案）
資料５	2014 年度 暗号技術評価委員会活動計画（案）
資料６	2014 年度 暗号技術活用委員会活動計画（案）

参考資料１	2013 年度 第 1 回暗号技術検討会議事概要
参考資料２	CRYPTREC 暗号技術ガイドライン（SSL/TLS における近年の攻撃への対応）
参考資料３	CRYPTREC 暗号技術ガイドライン（SHA-1）
参考資料４	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
参考資料５	2013 年度　暗号技術検討会　構成員・オブザーバ名簿

資料 1

2013 年度暗号技術評価委員会 活動報告

1. 活動目的

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

(1) 暗号技術の安全性及び実装に係る監視及び評価
(2) 新世代暗号に係る調査
(3) 暗号技術の安全な利用方法に関する調査

2. 活動概要

(1) 暗号技術の安全性及び実装に係る監視及び評価

① CRYPTREC 暗号等の監視

国際会議等で発表される CRYPTREC 暗号リストの安全性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）に関する監視活動を行った。また、CRYPTREC 暗号リストに掲載された暗号技術の仕様書の参照先の変更について検討を行い、CRYPTREC の Web ページで公開した。

② 電子政府推奨暗号リスト及び推奨候補暗号リストからの運用監視暗号リストへの降格 及び 運用監視暗号リストからの危殆化が進んだ暗号の削除

CRYPTREC 暗号リストの安全性に係る継続的な監視活動とともに、リストからの降格や削除、注釈の改訂が必要か検討を行った。

128-bit key RC4 は、現在、運用監視暗号リストに掲載され、「128-bit RC4 は、SSL(TLS1.0 以上)に限定して利用すること」という注釈が付与されているが、近年の攻撃の進化により、SSL/TLS での利用における安全性に懸念が高まったことから注釈の改定の検討を開始した。

③ CRYPTREC 注意喚起レポートの発行

CRYPTREC 暗号リストに掲載されている暗号技術ではないが、NIST Special Publication 800-90A 及び ANS X9.82 に記載されている擬似乱数生成アルゴリズム Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generation)にセキュリティ上の懸念が示されていることを受け、同アルゴリズムを含む暗号ライブラリ等を利用しているユーザー向けへの注意喚起の目的として、2013 年 9 月に米国 NIST が出した声明の概要を CRYPTREC の Web ページにおいて紹介した。

④ 推奨候補暗号リストへの新規暗号（事務局選出）の追加

標準化動向に鑑み電子政府システム等での利用が見込まれると判断される暗号技術の追加を検討した。2013 年度は下記の通り、ハッシュ関数 SHA-224、SHA-512/224、SHA-512/256、SHA-3 の実装評価を実施した。但し、SHA-3 は FIPS Draft が NIST からまだ公開されていないため、Keccak の仕様に基づき評価を行った。

- 既存の実装性能評価に関する研究結果の調査（CRYPTRECからの外部評価）
  依頼先：崎山 一男教授 （電気通信大学）
- FPGA 上での実装性能評価（NICT にて実施）
  依頼先：佐藤 証教授 （電気通信大学）

安全性評価に関しては、来年度以降、SHA-3 の FIPS Draft が公開された後に外部評価を実施する予定である。

⑤ 既存の技術分類の修正を伴わない新技術分類の追加

暗号技術調査ワーキンググループにて調査を行い、暗号技術評価委員会は、その調査結果に基づき追加方針等について検討を行う。2013 年度は該当する技術分類はなし。

(2) 新世代暗号に係る調査

① 暗号技術調査ワーキンググループ(暗号解析評価)

- 離散対数問題の困難性に関する調査

近年、研究の進展している有限体上あるいは楕円曲線上の離散対数問題の困難性に関する調査を行った。2013 年度は、有限体上の離散対数問題の解読記録において、以前より長い鍵長のものが出現しているので、それらについて調査を行った。

- 格子問題等の困難性に関する調査

格子問題のほか、NP 困難に係る問題、多変数多項式に係る問題、符号理論に係る問題等、量子計算機が実現しても安全性が保たれると期待されている「耐量子計算機暗号」を支える数学的問題の困難性に関する調査を行った。2013 年度は、昨年度リストアップした論文の中から注目すべき数学的問題をいくつか取り上げて、安全性について検討を行った。

② 暗号技術調査ワーキンググループ(軽量暗号)

2013 年度は、下記の活動を実施した。

i. 軽量暗号技術に関する現状調査(サーベイ)

軽量暗号アルゴリズム調査（安全性・実装性能)、軽量暗号に関わる新しい技術動向、外部動向（CAESAR プロジェクト)、軽量暗号の活用事例および標準化動向

ii. 軽量暗号のアプリケーションに関する調査

- 軽量暗号の活用が期待される分野
- エンドユーザーからのヒアリング(自動車、制御システム)

iii. 軽量暗号の実装評価

軽量ブロック暗号のハードウェア実装評価及びソフトウェア実装評価

iv. 今後の活動方針に関する議論

- 暗号技術ガイドラインの発行、暗号技術の公募など、どのようなアプローチが望ましいのかの検討
- 2014 年度の検討項目の抽出

(3) 暗号技術の安全な利用方法に関する調査

① 「CRYPTREC 暗号技術ガイドライン(SSL/TLS における近年の攻撃への対応)」の作成

BEAST、TIME、CRIME、Lucky Thirteen などSSL/TLS に対する近年の攻撃の解説を行うとともに、これらの攻撃に対して推奨される対応を示したガイドラインを作成した。また、SSL/ TLSプロトコル内でRC4が用いられた場合の実際の攻撃方法、事例を示し、RC4 を選択しないことなどを述べている。

② 「CRYPTREC 暗号技術ガイドライン(SHA-1)」の作成

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、CRYPTREC運用監視暗号リストに記載されているハッシュ関数SHA-1を利用する際の必要となる情報を示したガイドラインを作成した。SHA-1 に関して、推奨されない利用範囲及び許容される利用範囲について示した。

- 許容されない利用範囲
  - 電子署名における署名生成
- 許容される利用範囲
  - 電子署名における署名検証
  - Keyed-Hash Message Authentication Code (HMAC)
  - Key Derivation Functions (KDFs)
  - 擬似乱数生成系
  - パスワード・ハッシングやチェックサムの計算としての利用 (hash-only applications)

資料１別添１

2013 年度暗号技術調査 WG（暗号解析評価）活動報告

1　活動目的

公開鍵暗号の安全性は、素因数分解の困難性や離散対数問題の困難性などさまざまな数学的問題に依存している。本 WG ではこれまで、素因数分解の困難性及び離散対数問題等の困難性に関する調査を行ってきた。2013 年度も下記(1)及び(2)の調査等を継続して行う。

(1) 離散対数問題の困難性に関する調査

(2) 格子問題等の困難性に関する調査

2　委員構成

主査：高木 剛(九州大学)

委員：青木 和麻呂(NTT)

委員：石黒 司 (KDDI 研究所)

委員：太田 和夫(電気通信大学)

委員：草川 恵太 (NTT)

委員：國廣 昇(東京大学)

委員：下山 武司(富士通研究所)

委員：安田 雅哉(富士通研究所)

3　活動方針

3.1 離散対数問題の困難性に関する調査

近年、研究の進展している有限体上あるいは楕円曲線上の離散対数問題の困難性に関する調査を行う。2013 年度は、有限体上の離散対数問題の解読記録において、以前より長い鍵長のものが出現しているので、それらについて調査を行う。

3.2 格子問題等の困難性に関する調査

格子問題のほか、NP 困難に係る問題、多変数多項式に係る問題、符号理論に係る問題等、量子計算機が実現しても安全性が保たれると期待されている「耐量子計算機暗号」を支える数学的問題の困難性に関する調査を行う。2013 年度は、昨年度リストアップした論文の中から注目すべき数学的問題をいくつか取り上げて、安全性について検討を行う。

4　活動概要

4.1 スケジュール

第 1 回　2013 年 9 月 3 日　　活動計画案や作業内容についての審議と了承
第 2 回　2014 年 2 月 20 日　　調査内容についての審議と了承

4.2 離散対数問題の困難性について

標数が小さい有限体上の離散対数問題を解くことに適したアルゴリズムとして、関数体篩法が知られている。近年、関数体篩法の計算量を改善する方法として、Joux らにより Pinpointing(及びその改良)という手法の概要ついて報告があった。また、この手法の CRYPTREC 暗号リストに掲載の暗号技術への影響についても検討した。

4.3 格子問題等の困難性について

今年度は、昨年度検討予定としていた数学的問題の中から、研究が進んできている下記の数学的問題、

① Shortest Vector Problem (SVP)
② Learning With Errors (LWE)
③ Learning Parity with Noise (LPN)
④ Approximate Common Divisor (ACD)

を選び、その定義や解読アルゴリズム及び計算量について調査を行った。内容及び担当は下表の通りとなった。

表 1 ：調査内容と執筆担当

章	執筆担当	内容
1 章	事務局	調査の目的、まとめ（非専門家向け）
2 章 総論	石黒 司委員	総論(General な攻撃に関する総論):SVP、LLL、BKZ
3 章 LWE	下山 武司委員、 安田 雅哉委員	各問題について以下の項目を記述 (1) 公開鍵方式からの帰着、証明の有無、追加の問題・制約など (2) 攻撃や量子アルゴリズム - General な攻撃との関係 - 固有の攻撃 - 量子アルゴリズムとの関係
4 章 LPN	草川 恵太委員	
5 章 ACD	國廣 昇委員	

4.4 予測図の更新

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.Org[1]において、2013 年 6 月・11 月のベンチマーク結果が追加されたので、素因数分解問題及び楕円曲線上の離散対数に関する２つの予測図を更新した。

5　成果概要

数学的問題の困難性に関する調査報告書の概要は下記 5.1 及び 5.2 の通りである。また、予測図の更新版を 5.3 に掲載する。

5.1 離散対数問題の困難性について

Pinpointing という近年提案された手法により、関数体篩法における篩(sieving)において、一つの relation を得るために必要な候補となる多項式の個数を従来の方法に比べて少なくすることが可能となった。この手法の適用範囲は、有限体の大きさそのものではなく、その中間体及び拡大次数の「バランス」に依存する。

そのため、素体(GF(p),p 素数)上構成されている DSA 及び DH への安全性に影響はない。

5.2 格子問題の困難性について

① 格子の SVP(近似版を含む)のうち、近似因子が次元の多項式で表される場合に適用される、4 つの解読アルゴリズム(LLL、BKZ、篩、ボロノイセル)の計算量等に関する概説、及び、最新の計算機実験(SVP Challenge, Lattice Challenge, Ideal Lattice Challenge)についての報告があった。

② LWE問題は、GapSVP及びSIVPの困難性に関する仮定のもとで解くことが困難であることが知られており、効率的に解くことが困難であると予想されている。完全準同型暗号スキームをはじめ、LWE問題ベースの暗号スキームが提案されてきている。実際の構成の際には、BKZアルゴリズム等の格子縮約アルゴリズムに対し耐性を持つようにパラメータ設定を行う必要があり、安全なLWEパラメータを選択することは今後の課題である。

③ 総当たり法で解く他に、LPN 問題を解くアルゴリズムを大別すると、3 つの解読アルゴリズム(BKW、Arora-Ge による再線形化、シンドローム復号(SD)問題を経由するもの)が知られている。McEliece 暗号や Niederreiter 暗号をはじめ、90 年代から様々な暗号スキームが提案されてきている。BKW アルゴリズムの改良版である LF アルゴリズムの計算機実験例や SD 問題の高速化によるパラメータの評価例がある。

④ ACD 問題を、素因数分解を直接的に経由しないで解くアルゴリズムは、大別すると、組み合わせ論に基づく方法と格子理論に基づく方法がある。前者については、最近提

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

案された Chen-Nguyen のアルゴリズムを使って、実際に提案論文で書かれた推奨パラメタのいくつかが解読されているため、今後の研究の動向に注視する必要がある。

今後は、これらの数学的問題を利用した公開鍵暗号技術とパラメータ選択に関する検討を行いたいと考えている。

5.3 予測図の更新

「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」の更新後の図は、図 1 の通りとなる。

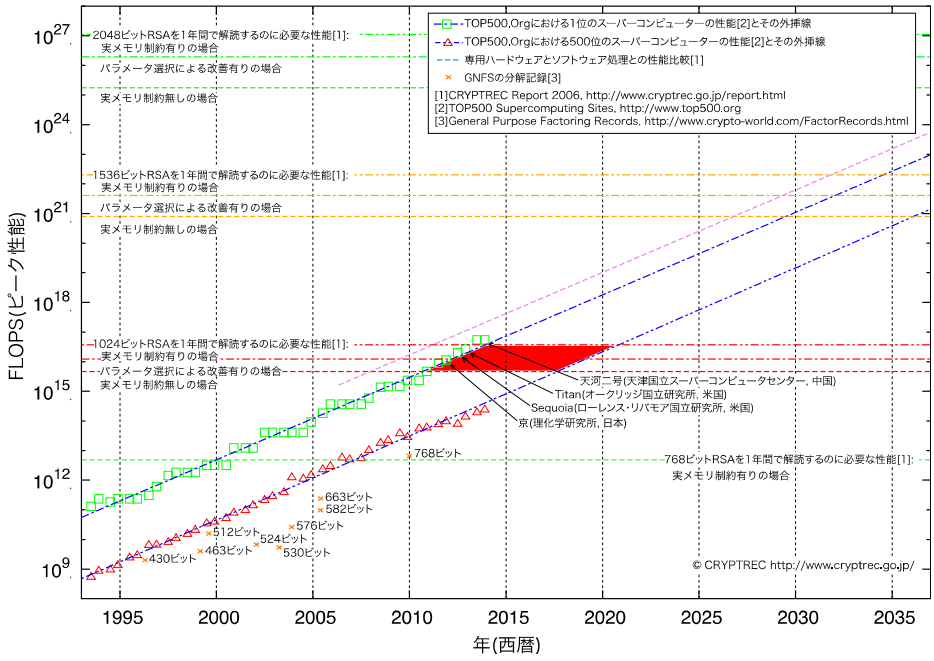


図 1：1 年間でふるい処理を完了するのに要求される処理能力の予測(2014 年 2 月更新)

また、「ρ法でECDLPを1年で解くのに要求される処理能力の予測」の更新後の図は、図2の通りとなる。

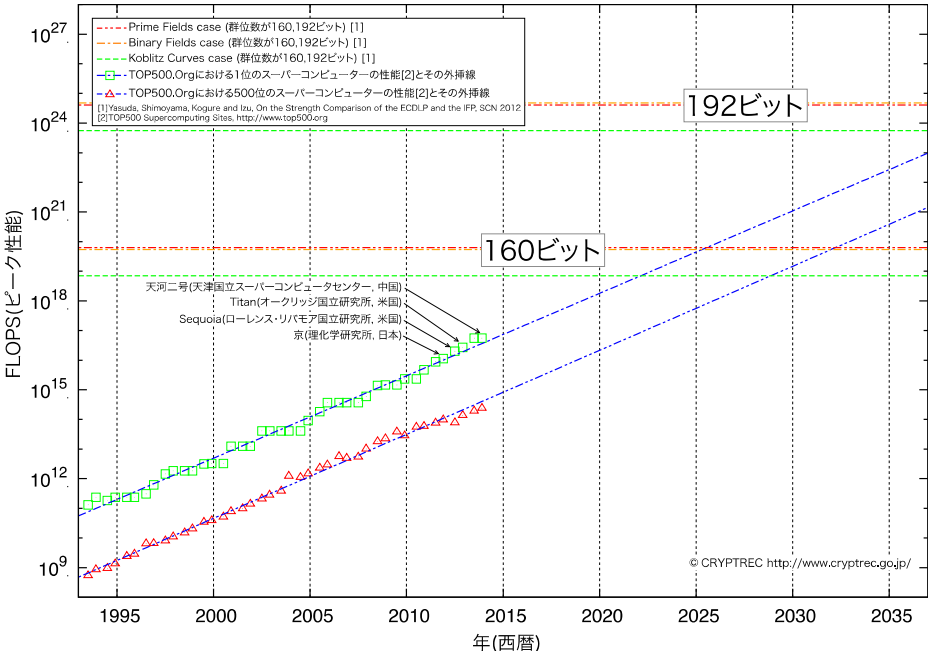


図2： ρ法でECDLPを1年で解くのに要求される処理能力の予測(2014年2月)

以上

資料１別添２

2013 年度暗号技術調査 WG（軽量暗号）活動報告

1　活動目的

軽量暗号 WG は、軽量暗号技術が求められるサービスにおいて、電子政府のみならず利用者が最適な暗号方式を選択でき、容易に調達できることをめざして設置された。

本 WG では、これまでに提案されている軽量暗号の調査（安全性および実装性能、既存技術との比較）を行う。次に今後活用される軽量暗号技術に求められる要求条件を明らかにし、評価方法等を検討する。これらの検討結果をふまえ、軽量暗号について CRYPTREC でどのような活動を進めるのが望ましいかを検討する。

2　委員構成

主査：	本間　尚文	東北大学
委員：	青木　和麻呂	NTT
委員：	岩田　哲	名古屋大学
委員：	小川　一人	NHK
委員：	崎山　一男	電気通信大学
委員：	渋谷　香士	ソニー
委員：	鈴木　大輔	三菱電機
委員：	成吉　雄一郎	ルネサスエレクトロニクス
委員：	峯松　一彦	NEC
委員：	三宅　秀享	東芝
委員：	渡辺　大	日立製作所

3　活動概要

2013 年度は、下記の活動を実施した。

（１）軽量暗号技術に関する現状調査(サーベイ)

・軽量暗号アルゴリズム調査(安全性・実装性能)、軽量暗号に関わる新しい技術動向、外部動向（CAESAR プロジェクト)、軽量暗号の活用事例および標準化動向

（２）軽量暗号のアプリケーションに関する調査

- 軽量暗号の活用が期待される分野
- エンドユーザーからのヒアリング(自動車、制御システム)

（３）軽量暗号の実装評価

軽量ブロック暗号のハードウェア実装評価及びソフトウェア実装評価

（４）今後の活動方針に関する議論

- 暗号技術ガイドラインの発行、暗号技術の公募など、どのようなアプローチが望ましいのかの検討
- 2014 年度の検討項目の抽出

4　スケジュール

第１回　9月17日

- 現状調査(サーベイ)について作業方針・分担の審議
- アプリケーションに関する議論

第２回 12月26日

- 現状調査(サーベイ)に関する中間報告
- エンドユーザーからのヒアリング(自動車、制御システム)
- 今後の活動方針に関する議論

第３回　2月20日

- 今年度実施した調査内容のとりまとめ
- 実装評価報告
- 2014 年度の検討項目の抽出

5　成果概要

5.1 軽量暗号技術に関する現状調査(サーベイ)

2013 年度は、軽量暗号技術に関する現状調査(サーベイ)として、表１に示した項目の調査を行った。

表 1. 軽量暗号技術に関する現状調査(サーベイ)

軽量暗号アルゴリズム調査		
	安全性	**実装性能**
ブロック暗号	青木 和麻呂 委員	渋谷 香士 委員
認証暗号(モード)	峯松 一彦 委員	鈴木 大輔 委員
ストリーム暗号	渡辺 大 委員	
ハッシュ関数	三宅 秀享 委員	
軽量暗号に関わる新しい技術動向		
Low-latency	崎山 一男 委員	
サイドチャネル耐性	成吉 雄一郎 委員	
外部動向		
CAESAR	岩田 哲 委員	
軽量暗号の活用事例および標準化動向		
	小川 一人 委員	

- 軽量暗号アルゴリズム調査（安全性・実装性能）

  軽量暗号アルゴリズム調査では、表２に示したブロック暗号、認証暗号、ストリーム暗号、ハッシュ関数を中心に、安全性および実装性能について学会等で発表されている文献調査を行い、その結果を報告書としてまとめた。

表 2. 調査対象の技術分類とアルゴリズム

技術分類	CRYPTREC (電子政府推奨暗号)	ISO/IEC 29192	その他
ブロック暗号	AES, TDES, Camellia	PRESENT, CLEFIA	LED, Piccolo, TWINE, PRINCE
認証暗号 (モード)	CCM, GCM (CTR, CMAC)		ALE, OCB
ストリーム暗号	KCipher-2	Trivium, Enocoro	Grain, MICKEY
ハッシュ関数	SHA-2	(PHOTON, SPONGENT)	SHA-3 (Keccak), Quark

※下線を引いたアルゴリズムは日本からの提案

- 軽量暗号に関わる新しい技術動向 (低レイテンシ暗号 (low-latency cryptography) 及びサイドチャネル耐性)

  暗号処理における低レイテンシ性は、データ通信における暗号処理時の応答速度を重視するアプリケーション、例えば、車の安全運転支援システム (Car2X communication)、セキュア・ストレージ、CPU-外部ストレージ間のバス暗号化等で求められている。現在、CMOS テクノロジの微細化による集積回路の信号遅延時間短縮はあまり期待できないため、低レイテンシ暗号を実現するためには、暗号処理に要する計算量を大幅に削減する必要があり、軽量暗号が新たに求められる理由のひとつとなっている。例えば, AES では回路規模, レイテンシともに上述のアプリケーションが求める要求は満たせず、数 10kGE の回路規模で, 数 ns のレイテンシでハードウェア実装することは, 現在の実装技術では達成できていない。

  サイドチャネル耐性については、軽量暗号アルゴリズムにおけるリーク解析、電流解析、電磁波解析も含めたサイドチャネル攻撃および故障利用攻撃に関する文献調査を行った。

- 外部動向 (CAESAR プロジェクト)

  2013年1月から開始された「認証暗号」(データの暗号化と認証を同時に行うための共通鍵暗号技術) の選定プロジェクト CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) について調査を行った。本プロジェクトでは「軽量」性についても評価要素に入ることが予想される。AES コンペティション, eSTREAM プロジェクト, SHA-3プロジェクトに続く国際的なコンペティションであり, 本WGで継続的に注視していく。

- 軽量暗号の活用事例および標準化動向

  今後の暗号の開発において、活用事例・標準化動向から軽量暗号に関する要求条件を

導き出し、研究開発、標準化の指針を得ることを目的として調査を行った。活用事例調査としては、軽量暗号が活用されると期待されている分野（RFID、センサーネットワーク（環境測定等）、医療センサー、ＩＴＳ、記録メディア（HDD、SSD 等）、携帯端末（携帯電話、タブレット端末、ポータブルゲーム機等）について公開されている情報を調査するほか、メーカー数社にヒアリングを行った。調査の結果、軽量暗号に対する要求はあるものの、具体的なスペックまで落とし込んだ要求条件は出ていないことが分かった。しかしながら医療センサーの事例で、標準化されれば使用する業者があるということも分かった。CRYPTREC などの機関で評価・選定を行うことで、軽量暗号の利用促進につながると考えられる。

標準化動向調査では、ISO/IEC JTC 1/SC 27/WG 2 で進められてきた標準化状況及び IETF Light-Weight Implementation Guidance (lwig)で開始された軽量暗号の実装に関する活動状況調査を行った。

5.2 アプリケーションに関する調査

下記に挙げられるような軽量暗号の特徴から、軽量暗号の活用が期待されるアプリケーションのリストアップを行った。

軽量暗号の特徴

- ハードウェア規模が小さい，低消費電力で動作，消費電力が少ない，低コスト
- コードサイズが小さい，RAM が少ない
- 低レイテンシ性，リアルタイム性

軽量暗号の活用が期待されるアプリケーション

- RFID タグ，センサー，ワイヤレスセンサー
- IC カード
- 医療機器(体内埋め込みや携帯型など)，ヘルスケア製品
- スマートメータ
- モバイル製品
- バッテリ
- 車，ITS システム

また、エンドユーザーからのヒアリングとして、下記の２名の方から自動車および社会インフラへの軽量暗号技術の応用について意見を伺った。

「自動車におけるITセキュリティ」（トヨタIT 開発センター 小熊 寿氏）

「制御システム向け暗号の要件の考察」（日立製作所 大和田 徹氏）

小熊氏からは、自動車における IT セキュリティでは、例えば、車載ネットワーク CAN のデ

ータ長が８バイトであることから、軽量暗号は、MAC を生成するアルゴリズムとして処理性能や MAC サイズの点で AES よりも有利と思われるとのコメントがあった。また、大和田氏からは、課題からみた制御システム向け暗号の要件が抽出され、高速処理、低処理負荷、柔軟な暗号化対象長、低リソースでの鍵管理・更新機能等の要件で軽量暗号が役立つ可能性があるとコメントがあった。

5.3 軽量暗号の実装評価

5.1 で行った現状調査にも軽量暗号の実装評価は含まれるが、既存文献の調査であることから、文献により評価環境や実装者が異なるため、暗号アルゴリズム間の比較が困難であった。そこで、NICT にて表２に示す軽量ブロック暗号について、同一プラットフォーム上で、同一の実装者または統一的な実装ポリシーによりハードウェア実装およびソフトウェア実装の評価を行い、統一的な評価環境で比較を行った結果が第 3 回軽量暗号 WG にて報告された。実装環境および測定指標は下記の通りである。

- ハードウェア実装評価
  - 標準的な CMOS セルライブラリ：NANGATE Open Cell Library (45nm CMOS)
  - unrolled 実装, round 実装, serial 実装の 3 通りのアーキテクチャ
  - 測定指標：最大動作周波数、処理速度、ゲートカウント、サイクルカウント、消費電力、ピーク電流
- ソフトウェア実装評価
  - プロセッサ：ルネサスエレクトロニクス RL78 (16bit 組み込みマイコン)
  - 測定指標：処理速度, RAM サイズ, ROM サイズ

    ROM, RAM サイズに関して下記4通りの組み合わせで、それぞれの範囲内で処理速度を最大化する実装を行った。

ROM	512B	1024B
RAM	64B	128B

このハードウェア実装評価では、軽量暗号は AES と比較して 1-2Kgate 回路規模が小さく、この違いはマチュアなプロセス(180nm-350nm)において実装の可否に影響する場合があり、アドバンテージとなること、リアルタイムのメモリ暗号化やμ秒クラスのリアルタイム通信などのアプリケーションにおいて優位となる可能性があることが報告された。また、小さい、速いという一つの指標だけだと AES との差分が少ないが、小さく、速く、サイドチャネル対策が容易という複数の軸で比較したときに AES に対する優位性がより明確になると報告された。

ソフトウェア (組み込みマイコン) 実装においては、コードサイズの小さい暗号への要求が高い。メモリが十分あれば (例えば、アルゴリズム単体で暗号復号込みで ROM 1KB あれば)

AES で十分である。よって組み込みマイコンにおいて AES より価値ある軽量ブロック暗号は、暗号・復号込みで ROM　200B 以下、RAM　32B 以下でそれなりの速度が達成できるアルゴリズムと考えられるという報告があった。

5.4 今後の活動方針に関する議論

当初は、今年度中に CRYPTREC における軽量暗号に関する今後の活動方針について WG として結論を出し、暗号技術評価委員会に報告する予定であったが、もう少しじっくり時間をかけて調査、議論を行い、結論を出すべきだという意見が出たことから、2014 年度末に方針を提言することで合意された。CRYPTREC における軽量暗号に関する今後の活動方針とその意義・目的としては、以下のような案が考えられうる（図 1 参照）。

A)　「暗号技術ガイドライン（軽量暗号の最新動向）」の発行

- 軽量暗号の最新技術動向をまとめた技術レポートであり、暗号技術者や専門家等が軽量暗号に関する専門的知識を得るのに活用される。

B)　「暗号技術ガイドライン（軽量暗号の詳細評価）」の発行

- 代表的な軽量暗号の安全性・実装性能を統一的に評価した技術レポートであり、ユーザが軽量暗号アルゴリズムを選択・利用する際の技術的判断材料として活用される。これにより、軽量暗号の利用促進、軽量暗号アルゴリズムの第三者評価レポートとして ISO/IEC 等国際標準化への貢献が期待される。

C)　軽量暗号に関する技術公募の実施

- CRYPTREC 暗号リストへの掲載を視野に、軽量暗号の公募・詳細評価を行い、選定を行う。これにより、軽量暗号が CRYPTREC 暗号リストへ新技術として追加され、電子政府システム等で最適な方式を選択でき、容易に調達できるようになることが期待される。

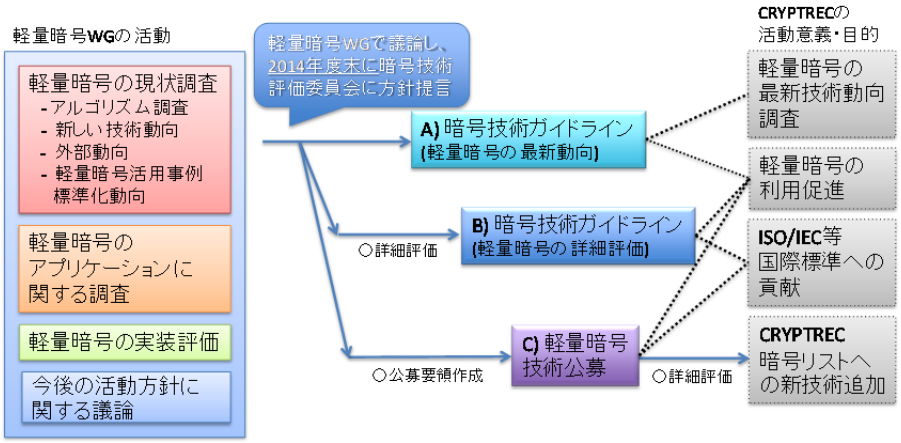


図 1. 今後の活動方針案

6　2014 年度検討項目

① 軽量暗号に関する検討

- 軽量暗号が既存暗号に対してアドバンテージをもつエリア
- 軽量暗号で達成すべき安全性

② 軽量暗号技術に関する現状調査（サーベイ）

- 認証暗号：CAESAR プロジェクト提案アルゴリズム等から軽量性に優れた方式を調査
- ハッシュ関数: SHA-3 の調査

③ 今後の活動方針に関する検討

- A)暗号技術ガイドライン（軽量暗号の最新動向）の発行、B)暗号技術ガイドライン（軽量暗号の詳細評価）の発行、C)軽量暗号に関する技術公募の実施のいずれがよいか検討を行い、暗号技術評価委員会に提言を行う。

資料２

暗号技術活用委員会活動報告

1. 2013 年度の活動内容と成果概要

2.1 活動内容

2013 年度以降の CRYPTREC の活動においては、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)」が策定されたことに鑑み、我が国の暗号政策に係る中長期の視野に立って課題に引き続き取り組むため、平成 24 年度までの暗号方式委員会・暗号実装委員会・暗号運用委員会の 3 委員会体制から、暗号技術評価委員会・暗号技術活用委員会の 2 委員会体制に改組された。

暗号技術活用委員会では、2012 年度暗号運用委員会の全部及び暗号実装委員会の一部からの課題を主に引き継ぎ、暗号技術における国際競争力の向上及び運用面での安全性向上に関する検討を実施する。主な検討課題は以下の通り。

① 暗号の普及促進・セキュリティ産業の競争力強化に係る検討（運用ガイドラインの整備、教育啓発資料の作成等）
② 暗号技術の利用状況に係る調査及び必要な対策の検討等
③ 暗号政策の中長期的視点からの取組の検討（暗号人材育成等）

2013 年度は、暗号技術の利用状況に係る調査を実施する予定がないことから、①暗号の普及促進・セキュリティ産業の競争力強化に係る検討、及び③暗号政策の中長期的視点からの取組の検討（暗号人材育成等）についてのみ実施する。

(A) 暗号の普及促進・セキュリティ産業の競争力強化に係る検討

CRYPTREC 暗号リストの策定により、同リストに掲載されている暗号アルゴリズムの普及が促進し、ひいては日本のセキュリティ産業の競争力強化につながることが期待されている。

しかし、現実には「優れた暗号アルゴリズムがセキュリティ産業の競争力強化に直接的に繋がる」という関連性については、2012 年度運用委員会の委員ならびに CRYPTREC シンポジウム 2013 でのパネリストから極めて懐疑的な意見が多数出された。また、2012 年度の暗号技術の利用状況に係る調査結果からは、旧電子政府推奨暗号リスト策定から 10 年経過していたにもかかわらず、同リストに掲載されていた国産の暗号アルゴリズムの普及がほとんど進んでいない実態も明らかとなった。

そのため、本委員会では、「暗号政策上の課題の構造」や「暗号と産業競争力の関連性」などの課題に対する分析について約 2 年間の集中審議期間を設けることにより、暗号アルゴリズムの普及促進やセキュリティ産業の競争力強化に向けた障壁が何かを明らかにするととも

に、その解決策を取りまとめる。

2013 年度は、上記課題分析を行うにあたっては幅広く現況を俯瞰する必要があることから、議論を行ううえで有用な基礎データの収集を取りまとめる。すぐに対応可能な課題には本年度中に取り掛かるが、本格的な課題分析や具体的な解決策の検討についてはタイムスケジュールを作成する。

- 各種団体（政府機関を含む）等へのヒアリング
- セキュリティ産業競争力の源泉の俯瞰（市場動向など）
- 政策動向（共通番号制度、医療ガイドラインなど）
- 工程表の作成

(B) 暗号政策の中長期的視点からの取組の検討

人材育成の観点に関しては、様々なシステムを安全に動かしていく人材にとって、暗号についての必要な知識やスキルがどういうものかを検討することにより、CRYPTREC として取り組むべき課題を明らかにする。

- 各種団体（政府機関を含む）等へのヒアリング
- 工程表の作成

(C) 標準化推進

様々な標準化機関に対して日本から提案する暗号アルゴリズムが受け入れられるようにするため、標準化活動の取り組みを横断的に支援・意見交換するワーキンググループ（標準化推進ＷＧ）を設置し、日本からの暗号アルゴリズム提案の効率的な横展開を図る。

(D) 運用ガイドライン作成

暗号に関する一定水準以上の知識・リテラシーがあることを前提とせずに、暗号システムとして安全に利用できるようにするための運用ガイドラインを、運用ガイドラインワーキンググループを設置して作成する。

2013 年度は、利用者が非常に多く、また暗号に関するリテラシーのレベルにも大きな差がある「SSL/TLS」について作成する。

2.2　委員構成

暗号技術活用委員会の委員は以下の通り。

委員長	松本　勉	横浜国立大学　大学院環境情報研究院 教授
委員	上原　哲太郎	立命館大学　情報理工学部情報システム学科 教授
委員	遠藤　直樹	東芝ソリューション株式会社　技術統括部 技監
委員	川村　亨	日本電信電話株式会社　研究企画部門 プロデュース担当（セキュリティ） 担当部長／チーフプロデューサ
委員	菊池　浩明	明治大学　総合数理学部　先端メディアサイエンス学科 教授
委員	鈴木　雅貴	日本銀行　金融研究所　情報技術研究センター 主査
委員	高木　繁	株式会社三菱東京 UFJ 銀行　システム部システム企画室 次長
委員	角尾　幸保	日本電気株式会社　パブリックビジネスユニット 宇宙・防衛事業推進本部 主席技術主幹
委員	手塚　悟	東京工科大学　コンピュータサイエンス学部 教授
委員	前田　司	EMC ジャパン株式会社　RSA 事業本部　技術統括部 部長
委員	松井　充	三菱電機株式会社　情報技術総合研究所 技師長
委員	満塩　尚史	内閣官房　IT 総合戦略室 政府 CIO 補佐官
委員	山口　利恵	東京大学　ソーシャル ICT 研究センター 特任准教授
委員	山田　勉	株式会社日立製作所　日立研究所 エネルギーマネジメント研究部　ES3 ユニット ユニットリーダ主任研究員
委員	山本　隆一	東京大学　大学院医学系研究科　医療経営政策学講座 特任准教授

2.3 今年度の委員会の開催状況

委員会の開催状況は以下の通り。

回	開催日	議案
第 1 回	2013 年 9 月 11 日	● 活用委員会活動計画の確認 ● ワーキングループ活動計画案の審議・承認 ● 2013 年度調査方向性の審議 ● ヒアリング内容（ヒアリング先を含む）の審議

第 2 回	2013 年 12 月 13 日	● SSL/TLS サーバ構築ガイドライン（骨子）についてのとりまとめ中間報告及び審議 ● ヒアリング及び標準化推進 WG の中間報告
第 3 回	2014 年 3 月 19 日	● 2013 年度ヒアリング調査の報告 ● 各ワーキンググループからの活動報告 ● SSL/TLS サーバ構築ガイドライン技術的取りまとめ（WG 案）報告及び審議
	2015 年 2 月下旬	● 課題解決に向けた分析結果・対策を取りまとめ

2.3　成果概要

2.3.1　ヒアリング調査について

「暗号政策上の課題の構造」や「暗号と産業競争力の関連性」などの課題に対する分析を行うにあたって幅広く現況を俯瞰すること、並びに様々なシステムを安全に動かしていく人材にとって暗号についての必要な知識やスキルがどういうものかを検討することを目的として、各種団体（政府機関を含む）等へのヒアリング（アンケート形式を含む）を実施した。

主なヒアリング対象は以下のとおりである。

- 政府 CIO
- 政府機関・公的機関
- 業界団体
- サプライヤ（SIer、ベンダ等）
- ユーザ（オンラインショッピング、等）

また、ヒアリングを行う上で、以下のような仮説を立て、それらの視点を考慮してヒアリング項目を審議・作成した。

【設定した仮説】

- **暗号政策としてあるべき姿とは何か**

  仮説１：電子政府推奨暗号リストを具体的な暗号政策に結び付ける施策が必要ではないか

  仮説２：国家安全保障や情報資産保護等の観点を考慮すべきではないか

- **高度な暗号技術を産業競争力に反映させる要素は何か**

  仮説３：実際には暗号アルゴリズムの選択についての自由度が高くないのではないか

  仮説４：技術的な要素よりもそれ以外の要素のほうが暗号アルゴリズムの選択への影響が大きいのではないか

- **国産暗号の利用を促進させるために必要な要素は何か**

  仮説５：国産暗号を使いたいと思っても実際に使おうとすると高い障壁があるのではないか

  仮説６：利用実績や今後の利用可能性なども考慮した今回のリスト改定により、国産暗号の選択が容易になったのではないか
- **暗号に関してのどのような人材が不足しているか**

  仮説７：暗号アルゴリズムの選択等に対する目利き人材が不足しているのはないか

【設定したヒアリング項目一覧】

下線部は、ヒアリング項目における主な候補対象者を示している。例えば、政府担当者とは、政府機関での調達実務者や仕様策定に権限がある担当者が当該項目におけるヒアリング候補先ということを示す。

- **暗号を利用する機会がありますか？**

  政府担当者・業界団体・サプライヤ・ユーザ

  (a-1) 担当業務において、過去にセキュリティ向上策の一環として何らかの形で、暗号を利用したり、利用するように指示・取りまとめをした場面がありましたか。
  - その際のセキュリティ向上策として、暗号以外の対策と比較して、暗号による対策はどの程度重要視されましたか

  政府担当者・業界団体

  (a-2) 現在または近いうちに、暗号アルゴリズムの指定を伴うような調達仕様や規格等を作成・検討している、もしくは予定がありますか。
  - あるとすれば、どのような形で作成・検討が行われますか

- **どのような観点で暗号の選択や利用方法を決めていますか？**

  政府 CIO・政府担当者・業界団体・サプライヤ・ユーザ

  (b-1) 利用する暗号アルゴリズムはどういった経緯で決まりましたか？自ら（自らが開催する委員会等での審議を含む）の暗号アルゴリズム選択自体の検討結果によるものですか、それとも何らかの別の要因で決まったものですか。
  - 前者の場合、利用する暗号アルゴリズムを具体的に決める際に考慮した要件は何でしたか。また、そのうち、もっとも影響する要因は何でしたか

    例えば、
    - 知名度・信頼感

- ◆ 安全性
- ◆ 処理性能
- ◆ コスト（製品開発コスト、購入コスト、運用コスト、移行コストなど）
- ◆ 製品選択の容易性（製品種類の多さ、など）
- ◆ 開発期間（サービス導入・開始までの時間）
- ◆ 特許・ライセンス
- ◆ 輸出管理などの法規制
- ◆ その他

➢ 後者の場合、誰が利用する暗号アルゴリズムを具体的に決めることになりましたか

例えば、

- ◆ トップダウン的に決まっていた
- ◆ 大きな議論なく、なんとなく決まった（初めから一つしか候補がなかった）
- ◆ 暗号研究者などの専門家に選択を委ねた
- ◆ 利用する暗号アルゴリズムは細かく指定せずに（もしくは選択肢を示すだけで）、ベンダやサプライヤ、運用者、利用者などの実質的な担当部門に選択を委ねた
- ◆ その他

政府担当者・業界団体・サプライヤ・ユーザ

(b-2) 期限を切って利用する暗号アルゴリズムを交換するような対策を実施したことがありますか。

➢ その対策は支障なく実施できましたか。

サプライヤ

(b-3) 利用する暗号アルゴリズムによって製品開発コストや利益に違いが生じますか。また、その違いはビジネス的に許容できるレベルを超えていますか。

➢ 違いが生じるとすれば、どのような要因によるものですか。

- **電子政府推奨暗号リストを活用していますか？**

政府 CIO・政府担当者・業界団体・サプライヤ・ユーザ

(c-1) 電子政府推奨暗号リスト、CRYPTREC 暗号リスト、CRYPTREC 等の活動成果を知っていましたか。

➢ 暗号アルゴリズムの選択や利用方法を具体的に決める際に参考にしましたか。参考にしたとすれば、どの程度参考にしましたか

例えば、

- ◆ 具体的な暗号アルゴリズムを選択するにあたっての技術比較として利用
- ◆ 特定の暗号アルゴリズムについての技術的な裏付けとして利用
- ◆ 安全な暗号アルゴリズムの選択肢の提示としての利用
- ◆ その他

サプライヤ

(c-2) 電子政府推奨暗号リストに掲載されている暗号アルゴリズムにもかかわらず、何らかの理由で、当初利用することを予定（提案を含む）していたものとは異なるものに途中で変更したこと、または変更させられたことがありますか。

- ➢ 変更したこと、または変更させられたことがあるならば、どのような要因によるものですか

- **国産暗号アルゴリズムについてどのように考えていますか？**

政府 CIO

(d-1) 国産暗号アルゴリズムの利用が進まない原因はどのようなものだと思いますか。例えば、

- ➢ 国産暗号アルゴリズムを利用しようとは思わない。利用するメリットがない
- ➢ 利用しようとは思っても何らかの障壁がある
- ➢ ベンダやサプライヤ、運用者、利用者などの実質的な担当部門に選択を委ねている

政府担当者・業界団体・サプライヤ・ユーザ

(d-2) 国産暗号アルゴリズムを利用しようと考えたことがありますか。

- ➢ 考えたことの有無にかかわらず、その理由はなんですか

サプライヤ

(d-3) 官公庁向けのシステム・製品において、国産暗号アルゴリズムを利用しましたか。

- ➢ 利用しなかった場合、その理由はなんですか

政府担当者・業界団体・サプライヤ・ユーザ

(d-4) 国産暗号アルゴリズムを利用しようと考えたとき、実際に大きな支障なく利用できましたか。

- 利用しようとは考えたが実際には利用できなかった場合、何が障壁になって国産暗号アルゴリズムを利用することを断念しましたか

政府 CIO・政府担当者・業界団体・サプライヤ・ユーザ

(d-5) 今後、もし国産暗号アルゴリズムを利用しようと考える場合に、利用実績や今後の利用可能性なども考慮した今回のリスト改定で電子政府推奨暗号の国産暗号アルゴリズムの個数が絞り込まれたことにより、国産暗号アルゴリズムを選択することが容易になると思いますか。

- 容易になっていないとすれば、その理由はなんですか

政府 CIO・政府担当者・業界団体

(d-6) 「国家安全保障」や「情報資産保護」、「日本の暗号研究開発力の維持」等の視点から、政府や業界団体などがトップダウン的に国産暗号アルゴリズムの利用を優先させるという考え方をどのように思いますか。

- そのように思う理由はなんですか
- 実際に行うとした場合に何が障壁になりそうですか

サプライヤ・ユーザ

(d-7) 「国家安全保障」や「情報資産保護」、「日本の暗号研究開発力の維持」等の視点から、仮にトップダウン的に国産暗号アルゴリズムの利用促進を図ろうとした場合に、何か困ることが起きそうですか。

- 起きるとすれば、どういったことが予想されますか

政府 CIO・サプライヤ

(d-8) 日本の企業や大学、独立行政法人が国産暗号アルゴリズムを作ることの意義はなんだと考えますか。例えば、

- 日本の国益に直接的にかかわるもの
- 日本の産業力強化に関わるもの
- いざという時のための暗号研究開発力の保持
- 自己のビジネスのため
- 自己満足のため

サプライヤ・ユーザ

(d-9) 「米国政府標準暗号」と「電子政府推奨暗号である国産暗号」のどちらが知名度／信用度／アピール効果を持っていますか。

- どのような点でそのような違いを感じますか

- **暗号アルゴリズムの選択等に対する目利き人材が必要ですか？**

  政府 CIO・政府担当者・業界団体・サプライヤ・ユーザ

  (e-1) 利用する暗号アルゴリズムの選択や安全性動向の把握、暗号アルゴリズムの切り替えなどの技術的課題に対して、現在、どの程度の暗号についての知識やスキルを持っている人が担当していますか？

  - 暗号研究者との間で適切な議論が行える状況にありますか。
  - 実務を行ううえで支障になっていることがありますか。

  政府 CIO・政府担当者・業界団体・サプライヤ・ユーザ

  (e-2) 利用する暗号アルゴリズムの選択や安全性動向の把握、暗号アルゴリズムの切り替えなどの技術的課題に対応できる人材を、自らの組織内に持つ必要があると考えますか。それとも、そういった課題について対応してくれる人材が集約された組織が外部にあれば十分と考えますか。

  - 前者の場合、どの程度の知識やスキルを持つ人材がどの程度の規模（人数）で必要だと思いますか。また、組織体として暗号についての知識やスキルを伝承・維持するための仕組みがありますか。
  - 後者の場合、どういった組織体であることを期待しますか。また、そのような組織体が出す情報について、どの程度の効力を期待しますか。

2013 年度には、政府 CIO、政府機関・公的機関、並びにいくつかの業界団体についてヒアリングを実施した。また、2013 年度にヒアリングが実施できなかった、ユーザ（電子商取引関係（ショッピングモール等）等）やサプライヤ（SIer、ベンダ等)、2013 年度にヒアリングを実施しなかった業界団体については、2014 年度上期にもヒアリングを継続実施する予定である。

なお、ヒアリングの内容については、継続実施する予定のヒアリング調査結果と合わせ、2014 年度の最終報告書の中で取り扱うものとする。

2.3.2 標準化推進 WG 概要報告

【活動目的】

標準化推進 WG は、様々な標準化機関に対して日本から提案する暗号アルゴリズムが受け入れられるようにするため、標準化活動の取り組みを横断的に支援・意見交換し、日本からの暗号アルゴリズム提案の効率的な横展開を図ることを目的として、設置された。

具体的には、委員が活動に関わる各標準化団体における自らの活動状況や日本からの提案事項における交渉ノウハウや課題等を共有・蓄積し、暗号アルゴリズムの標準化提案に当

たっての俯瞰図を取りまとめる。併せて、今後様々な組織が日本から暗号アルゴリズムの提案を行う場合に、その成果が効率的に得られるようにするため、提案機会等の見込みがある標準化団体の選定（提案時期も含む)、提案する組織に当面必要な稼働見積もりや交渉方法等を検討する。

【委員構成】

標準化推進 WG の委員は以下の通り。

	委員氏名	所属	担当領域
主査	渡辺　創	独立行政法人産業技術総合研究所	ISO/IEC JTC1/SC27
委員	江原　正規	東京工科大学	ISO/IEC JTC1/SC31
委員	河野　誠一	レノボ・ジャパン株式会社	TCG
委員	木村　泰司	一般社団法人日本ネットワークインフォメーションセンター	IETF
委員	坂根　昌一	シスコシステムズ合同会社	M2M/IoT
委員	佐藤　雅史	セコム株式会社	長期署名（ETSI）
委員	武部　達明	横河電機株式会社	制御機器・制御システム
委員	廣川　勝久	ISO/IEC JTC1/SC17 国内委員会	ISO/IEC JTC1/SC17
委員	真島　恵吾	日本放送協会	放送
委員	真野　浩	コーデンテクノインフォ株式会社	IEEE802.11
委員	茗原　秀幸	三菱電機株式会社	医療

【活動概要】

2013 年度は、標準化活動の現状を整理するため、各標準化団体における、自らの活動状況や日本からの提案事項における交渉ノウハウや課題等を共有・蓄積した。

各々の標準化団体の活動概要は参考資料として添付する。

【スケジュール】

第 1 回及び第 2 回　2014 年 2 月 10 日（月）

- 委員からの各標準化団体の概要についての報告

【今後に向けて】

今後、様々な日本の組織が国際的に影響力を持つ標準化機関へ暗号アルゴリズムの提案を

行う場合に、提案する組織を横断的に支援し、意見交換を行っていけるように、今年度の成果を踏まえ、以下の議論を継続し、2014 年度に報告書としてまとめる。

- 暗号アルゴリズム提案に当たっての俯瞰図の取りまとめ
- 提案機会等の見込みがある標準化提案先の選定（提案時期も含む）
- 暗号アルゴリズムを提案する組織にとって当面必要な稼働見積りや交渉方法等

2.3.3 運用ガイドライン WG 概要報告

【活動目的】

暗号システムとして安全に利用できるようにするための運用ガイドラインを作成する。2013 年度は、利用者が非常に多く、また暗号に関するリテラシーのレベルにも大きな差がある「SSL/TLS」について作成する。

【委員構成】

運用ガイドライン WG の委員は以下の通り。

主査	菊池 浩明	明治大学
委員	阿部 貴	株式会社シマンテック
委員	漆嶌 賢二	富士ゼロックス株式会社
委員	及川 卓也	グーグル株式会社
委員	加藤 誠	一般社団法人 Mozilla Japan
委員	佐藤 直之	株式会社イノベーションプラス
委員	島岡 政基	セコム株式会社IS研究所
委員	須賀 祐治	株式会社インターネットイニシアティブ
委員	高木 浩光	独立行政法人産業技術総合研究所
委員	村木 由梨香	日本マイクロソフト株式会社
委員	山口 利恵	東京大学

【活動概要】

従来の CRYPTREC が作成してきた報告書等は異なり、暗号技術の記述を中心としたガイドラインではなく、暗号技術をシステムの中での一要素とみなしたうえでの運用ガイドラインを目指したものである。その心は、読者層をある程度の暗号技術の知識を有していなくても内容を正しく理解できること、またガイドラインの有効性の面からも実際に設定ができることを重視したガイドラインを作り上げることにある。

本年度は、多くのユーザが利用している「SSL/TLS」を題材に取り上げた。

なお、対象読者の考え方として、当初は、ブラウザを使う一般のユーザも対象読者に含めることを想定していたが、最近のブラウザではユーザに様々な設定をあえてさせないブラックボックス化を進めることで安全性を高めていること、サーバ側の設定で一定程度のブラウザのコントロールができること、一般のユーザにこの種のガイドラインを読ませることは現実には難しいこと、などの指摘が委員からなされた。これらの指摘を考慮して、WG としては、想定読者から一般のユーザは外し、主に SSL/TLS サーバを実際に構築するにあたって具体的な設定を行うサーバ構築者、実際のサーバ管理やサービス提供に責任を持つことになるサーバ管理者、並びに SSL/TLS サーバの構築を発注するシステム担当者とすることにした。

これに合わせ、SSL/TLS サーバの構築時に注意すべき点をまとめたガイドラインであることを明確にすることから名称を「SSL/TLS サーバ構築ガイドライン」とした。

本ガイドラインのポイントは、「暗号技術以外の様々な利用上の判断材料も加味した合理的な根拠」を重視して、現実的な利用方法をまとめたガイドラインを目指したことである。

例えば、実現すべき安全性についても、必要となる相互接続性とのトレードオフを考慮する観点から、相互接続性を損なってでも極めて高い安全性を重視する「特高セキュリティ型（仮称）」の SSL/TLS サーバを構築するケースから、一定水準の安全性を維持しながら極力相互接続性を確保する「ベースラインセキュリティ型（仮称）」の SSL/TLS サーバを構築するケースまで、複数の設定例を提示している。

また、最低限の安全性を確保するために、ブラウザ等との相互接続をあえて拒否すべき最低基準（バッドプラクティス）を明確にしたのも本ガイドラインの特長である。

【スケジュール】

第 1 回　2013 年 10 月 10 日（木）
第 2 回　2013 年 12 月 4 日（水）
第 3 回　2014 年 3 月 12 日（水）

【今後に向けて】

本ガイドラインは、SSL/TLS サーバの構築において広範囲に活用してもらうべき性質のものであることを考慮し、今後、2013 年度の WG での審議内容を確定する前に外部からの意見聴取等も取り入れ、さらなる精錬化を図ったのち、2014 年度早期に一般公開する予定である。

現時点でのスケジュールとしては、2014 年度第一四半期に外部からの意見聴取を実施し、第二四半期にガイドライン初版を公開する予定としている。

参考　標準化推進 WG 報告書

A. ISO/IEC JTC1/SC27

体制

ISO/IEC JTC1/SC27（以下、SC27 という）は、セキュリティ技術の国際標準化を行っている委員会であり、5 つのワーキンググループ（以下、WG という）から構成されている。5 つの WG は、それぞれ「WG 1: Information security management systems」、「WG 2： Cryptography and security mechanisms」、「WG 3: Security evaluation, testing and specification」、「WG 4: Security controls and services」、及び「WG 5: Identity management and privacy technologies」である。特に、暗号技術に関する国際標準化は、WG2 が担当している。

標準化の概要

SC27 で標準化された規格数は全体で 130 に上る。標準化のプロセスは順に WD、CD、DIS、FDIS を経て進み、提案後 2 年から 4 年ほどで規格（IS）として出版される。CD 以降は投票により、プロセスが進むか否かが決定される。また、投票に参加する P-member は 53 か国、オブザーバを務める O-member は、16 か国である。投票権は 1 か国 1 票であるため、国数が多い欧州が規格の制定に有利な状況である。

SC27 への規格提案では、基本的には 1 規格につき、1 か国で 1 技術までの提案となっている。2 つ目の技術を標準化するには、強い理由が必要である。そのため、同じ国で複数の提案者がいる場合、国内委員会でも調整を行う必要がある。

国際委員会では学術界に近い暗号の専門家が中心となって議論が行われる。規格への採用において、安全性が保証されていることが重要な要件である。ただし、SC27 自体は安全性評価を行わないため、他の機関等の評価結果を基に議論を行う。CRYPTREC による評価の信頼性は高い。また、標準化の際の評価として国内標準になっていることは国際標準化の強い理由となり得る。

暗号に関連する規格等

- 暗号アルゴリズム:ISO/IEC 18033
- デジタル署名：ISO/IEC 14888（添付型）, ISO/IEC 9796（復元型）
- ハッシュ関数：ISO/IEC 10118
- メッセージ認証コード：ISO/IEC 9797
- エンティティ認証：ISO/IEC 9798
- 認証付暗号：ISO/IEC 19772
- 鍵管理：ISO/IEC 11770
- 暗号利用モード：ISO/IEC 10116
- 乱数ビット生成：ISO/IEC 18031
- 素数生成：ISO/IEC 18032
- 楕円曲線ベース暗号技術：ISO/IEC 15946

- 軽量暗号：ISO/IEC 29192
- 匿名デジタル署名：ISO/IEC 20008
- 匿名認証：ISO/IEC 20009

<u>その他</u>

ISO/IEC の標準に掲載されている日本の暗号技術は次のとおりである。

- ISO/IEC 18033 Encryption algorithms
  - Part 2 Asymmetric ciphers（非対称暗号）
    - PSEC-KEM
    - HIME(R)
  - Part 3 Block ciphers（ブロック暗号）
    - MISTY1（64 ビットブロック暗号）
    - Camellia（128 ビットブロック暗号）
  - Part 4 Stream ciphers（ストリーム暗号）
    - MUGI（鍵ストリーム生成）
    - KCipher-2（鍵ストリーム生成）
    - MULTI-S01（出力関数）
- ISO/IEC 29192 Lightweight cryptography
  - Part 2 Block ciphers（ブロック暗号）
    - CLEFIA
  - Part 3 Stream ciphers（ストリーム暗号）
    - Enocoro
- ISO/IEC 14888 Digital signatures with appendix
  - Part 2 Integer factorization based mechanisms（素因数分解問題ベースのメカニズム）
    - ESIGN
- ISO/IEC 20008 Anonymous digital signatures
  - Part 2 Mechanisms using a group public key（グループ公開鍵を用いたメカニズム）
    - Mechanisms 5 and 6

B. ISO/IEC JTC1/SC17

体制

ISO/IEC JTC1/SC17（以下、SC17 という）は、カード及び個人識別について標準化を行っている委員会であり、9 の WG から構成されている。SC17 国内委員会には WG 国内委員会に加え、WG 間及び国内関係機関との連携を図るための SWG 委員会を設置して活動しており、それらの活動成果の国際標準への反映を図るとともに国際役職の引受等も含めて貢献している。以下に、SC17 国内委員会の構成図を示す。

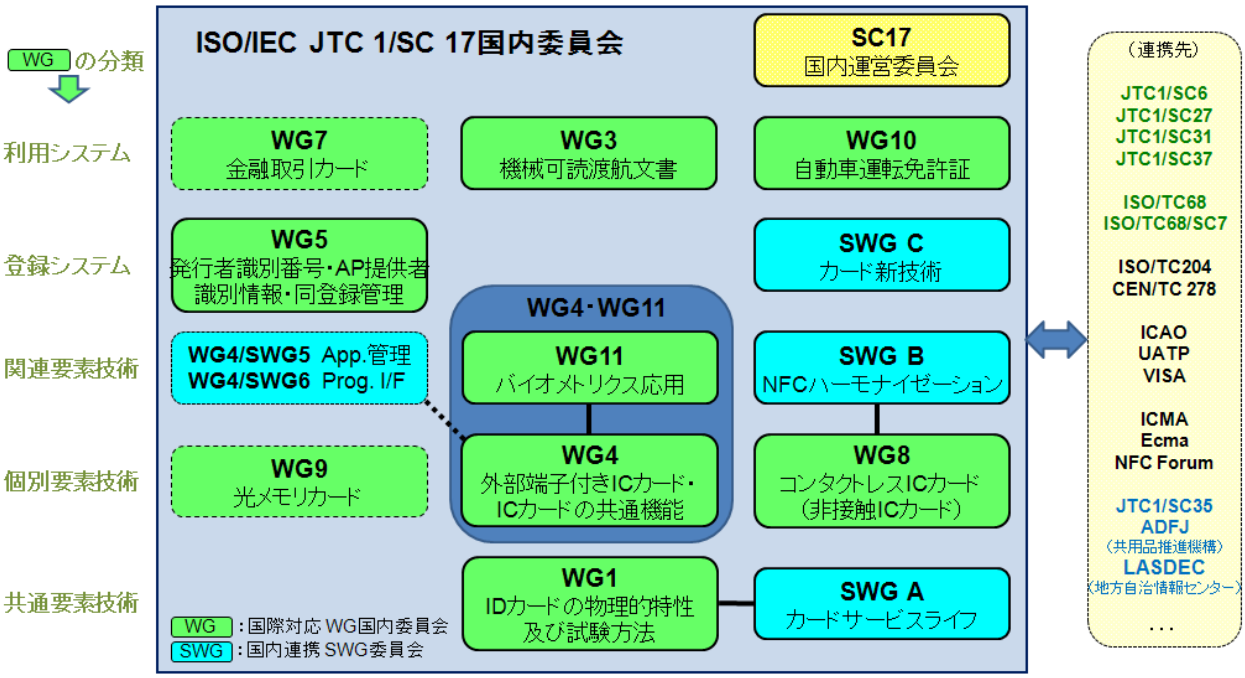


図 1. SC17 国内委員会の構成

標準化の概要

SC17 は、カード及び個人識別を対象とし、その要素技術から利用システム（クレジット・IC 旅券・運転免許証等）までに関する国際標準化と登録管理を担当している。この分野では、アプリケーション面からの標準化ニーズが高まっている。また、既に標準化された要素技術についても機能や性能に関わる追加標準化のニーズが生じている。これはカードが単体ではなくシステムとして利用される段階に進み、広範囲な互換性が求められるようになったことを示している。日本は、実装の実現性・後方互換を含めた互換性・今後の拡張性・全体的整合性等の観点からの詳細レビューと考察及び実験データに基づき意見の反映を図っている。ISO/IEC 7816、ISO/IEC 14443 等の主要規格には日本提案の技術が反映され国際的にも広く活用されており、IC カードの事業基盤形成に貢献している。技術面・アプリケーション面で関係の深まっている JTC1 の各 SC、ISO の各 TC、及びその他関係機関との連携を強化しているが、その範囲は拡がる方向にある。

暗号に関連する規格等

IC カード（SIM 等含む）が色々な応用分野で SE（Secure Element）としての機能を提供するにあたって暗号技術は必須の技術である。SC17 では、IC カードへの暗号技術利用のために、格納すべき暗号関連情報等の識別のための Tag 等を定めるが、暗号技術自体の標準化は行わない。基本的に、SC27 で標準化された暗号技術を前提に、各種の応用分野が求める利用方法をサポートするための IC カード用条件を必要に応じて標準化している。

その他

- 主要な国際標準
  - ID カードの基本規格　：ISO/IEC 7810（ID-1 カード、SIM カード等）
  - ID カードの記録技術：ISO/IEC 7811（エンボス、磁気記録）
  - IC カード（端子付き）：ISO/IEC 7816（Part-1～3, 10,12）
  - 非接触 IC カード：ISO/IEC 14443（近接型）、ISO/IEC 15693（近傍型）
  - IC カードの共通機能:ISO/IEC 7816（Part-4～9, 11,13,15）
  - 光メモリカード：ISO/IEC 11693、ISO/IEC 11694、ISO/IEC 11695
  - 発行者識別番号・同登録管理： ISO/IEC 7812
  - アプリケーション提供者識別情報：ISO/IEC 7816（Part-5）
  - IC 旅券・査証：ISO/IEC 7501
  - IC 運転免許証：ISO/IEC 18013
  - 生体認証応用：ISO/IEC 7816-11、ISO/IEC 17839、ISO/IEC 24787
  - アクセシビリティ：　ISO/IEC 7811-9（TIM）、ISO/IEC 12905（ETA）
  - アプリケーションプログラミングインターフェース：ISO/IEC 24727
  - ヒューマンインタフェース付き IC カード：ISO/IEC 18328
  - 試験規格：ISO/IEC 10373、ISO/IEC 24789、ISO/IEC 18745

C. ISO/IEC JTC1/SC31

体制

ISO/IEC JTC1/SC31（以下、SC31 という）の担当分野は、「Automatic identification and data capture techniques」であり、バーコードや RFID 等に関する標準化を行っている。ISO/IEC JTC1/SC6、SC17 等と関連がある。また、SC31 は WG の下にさらに SG と呼ばれるサブグループを設置している。

組織のメンバーは、米国、欧州、中国が企業中心であるのに対し、韓国は研究機関が中心である。

以下、特に WG7 に限定して説明を行う。

標準化の概要

SC31/WG7 では Automatic identification and data capture techniques のセキュリティに関する標準化を行っている。例えば、エアインターフェースの暗号化や低リソースチップにおける暗号化についての標準として、ISO/IEC 29167 がある（次項目で示す）。WG7 では暗号の決定の基準が Standing Document として次のように規定されている。

- 世界各国、多様な産業において利用されること。
- ISO のパテントポリシーに準拠すること。
- ビジネスニーズがあること。
- 実装可能であること。
- 既存の標準にないものであり、安全・頑丈であること。

暗号に関連する規格等

- ISO/IEC 29167-10 : AES-128
- ISO/IEC 29167-11 : Present-80
- ISO/IEC 29167-12 : ECC-DH
- ISO/IEC 29167-13 : Grain-128A
- ISO/IEC 29167-14 : AES-OFB
- ISO/IEC 29167-15 : XOR
- ISO/IEC 29167-16 : ECDSA-ECDH
- ISO/IEC 29167-17 : cryptoGPS
- ISO/IEC 29167-19 : RAMON

その他

- RFID のセキュリティ標準に関して、例えば、乱数、鍵交換、及び電子署名等のような技術課題がある。

D. 制御機器・制御システム（ISA-99・IEC TC65/WG10）

制御システムのセキュリティ標準について

制御機器・制御システムのセキュリティ標準を行っている団体は数多くあるが、ここでは ISA-99 及び ISA-99 の規格である ISA-62443 を国際標準化している IEC/TC65 WG10 について取り上げる。

標準化の概要

ISA-99 の制御システムのセキュリティ標準である ISA-62443 では、ISA-62443-1「一般」（青）、ISA-62443-2「ポリシー・手順」（緑）、ISA-62443-3「システム」（橙）、ISA-62443-4「コンポーネント」（ピンク）の 4 層で構成されている。

現在 IEC TC65 WG10 では、制御システムのセキュリティについての標準として ISA-62443 等が参照され IEC 62443 の制定が行われている。

以下は ISA-62443 及び IEC 62443 の標準化の状況を示した表である。

ISA Reference	IEC Reference	Title	Status	IEC Status	頁数
ISA-62443-1-1	IEC/TS 62443-1-1	用語・概念・モデル	Published 2007第2版作成中	DC 2013Q1	92
ISA-TR62443-1-2	IEC/TR 62443-1-2	基準用語・略語	執筆中	DTR: 2013Q4	41
ISA-62443-1-3	IEC 62443-1-3	システムセキュリティ適合メトリックス	DC/コメント対応中	CDV: 2013:09.13 PUB: 2014Q2	77
ISA-TR62443-1-4	IEC/TR 62443-1-4	IACSセキュリティライフサイクル・適用例	提案された	未定	
ISA-62443-2-1	IEC 62443-2-1	IACSセキュリティプログラムの確立	Published	CDV: 2013Q3 FDIS: 2014Q1	149
ISA-TR62443-2-2	IEC/TR 62443-2-2	IACSセキュリティプログラムの運用	提案された	CDV:2013Q1	68
ISA-TR62443-2-3	IEC/TR 62443-2-3	IACS環境でのパッチ管理	DC/コメント対応中	DTR: 2013.10.13 PUB: 2014Q2	59
ISA-62443-2-4	IEC 62443-2-4	ベンダーセキュリティ能力	CDV投票中	CDV: 2013Q2 FDIS: 2013Q4	75
ISA-TR62443-3-1	IEC/TR 62443-3-1	IACSのセキュリティ技術	Published	PUB: 2009.07	97
ISA-62443-3-2	IEC 62443-3-2	セキュリティリスク評価とシステム設計 (Zones & Conduits)	DC/コメント対応中	CDV: 2013Q4 FDIS: 2014Q3	28
ISA-62443-3-3	IEC 62443-3-3	システムセキュリティ要件とセキュリティ保証レベル	ISA Published	PUB:2013Q2	74
ISA-62443-4-1	IEC 62443-4-1	プロダクト開発要件	DC/コメント対応中	DC:2012Q2 CDV:2013Q1	74
ISA-62443-4-2	IEC 62443-4-2	IACS構成部品のセキュリティ技術要件	DC/コメント対応中	DC:2012Q1 CDV:2013Q1	137

表 1. ISA-62443 及び IEC 62443 の標準化の状況

表中の 62443-2-4「ベンダーセキュリティ能力」、62443-3-3「システムセキュリティ要件とセキュリティ保証レベル」及び 62443-4-2「IACS 構成部品のセキュリティ技術要件」には暗号の利用に関する記述がある。

暗号に関連する規格等

ISA-62443（IEC 62443）では、直接暗号アルゴリズムの指定はないが、暗号アルゴリズムを規定した他の規格を参照することで、間接的に利用するアルゴリズムを指定している。次に示すのは、ISA-62443（IEC 62443）に記述されている暗号アルゴリズムに関する規格である。

- ISA-62443-3-3
  - IEEE802.11x
  - IEEE802.15.4（Zigbee 、IEC62591-WirelessHART、ISA-100.11a）
  - IEEE802.15.1（Bluetooth）
  - RFC3647
- ISA-62443-4-2
  - ISO/IEC 19790:2012

その他

- 制御システム業界からの暗号技術への要望
  制御組込機器の CPU は、一般の PC 等に搭載されている CPU よりも性能が 1 ケタから 2 ケタ程度劣る。さらに、制御システムはその性質上、処理速度に対する実時間制約が非常に厳しい。そのため、市場（開発側及び購入者側の両方）からはパフォーマンスに優れ、知名度があり、攻撃に対する改善実績や危殆化に対する配慮のある暗号が求められている。特に、制御システムの開発側では暗号の開発・導入に割ける工数が非常に限られるため、暗号を透過的に導入・利用できる開発環境やライブラリ等がパッケージとしてほしいという要求がある。よって、制御システム業界では、軽量な暗号技術や超軽量な暗号技術のシリーズが望まれている。

E. IEEE802.11

体制

IEEE（米国電気電子学会）は、一般的な学会活動の他に IEEE-SA（IEEE Standards Association）にて標準化活動を行っている。IEEE-SA の下には様々な委員会があり、IEEE802 LMSC では LAN/MAN の標準化が行われている。委員会の下には WG が設置されているが、特に IEEE802.11 WG では、無線 LAN の標準化が行われている。また、IEEE802.11 WG は 8 つのタスクグループ（TG)、5 つのスタンディングコミッティ（SC)、及びスタディグループ（SG）から構成されている。

標準化の概要

IEEE802.11 の会合は年 6 回開催され、会合での議決と書面投票によって意思決定が行われる。議決は多数決によって行われ、技術的な事項の議決には 75%の支持を得なければならない。投票は投票権所有者のみが行うことができ、投票権は企業や団体ではなく、「個人」に付与される。議事運営は、ロバートルールによる。

ロバートルールでは、4 つの権利が守られる。①多数決の権利（過半数の賛成）②少数者の権利（少数意見の尊重）③個人の権利（プライバシーの権利擁護）④不在者の権利（不在投票）である。また、その他に守るべきルールとして、例えば、次のようなものがある。

- 発言者は議長とのみ話すことができる。
- 動議提案には 2 人以上の賛成が必要。
- 不十分な動議は棚上げされ、会議満了で失効する。
- 一度議決されたものは審議できない。

投票権は 4 回の連続する Plenary のうち、3 回目の出席で、取得できる。3 回のうち 1 回は Interim で代用できるが、投票権の付与は Plenary のみである。セッションの 75%以上に出席しなければ、「出席」とは認められない。投票権の維持には、直近 4 回の Plenary 中 2 回に出席が必要である。

標準化は TG が行う。TG を作るためには、図 2 に示すように、まず、SG を作り、「Project Authorization Request」及び 5 つの Criteria に関する付随文書を作成しなければならない。5 つの Criteria は、次のようになる。

- その規格を作ることによって、市場が伸びるのか（Broad Market Potential）
- 現在の技術と互換性があるのか（Compatibility）
- その技術は 802.11 WG で標準化すべき技術なのか（Distinct Identity）
- 技術面で実現可能性があるか（Technical Feasibility）
- 経済面で実現可能性があるか（Economic Feasibility）

その後、標準化は、図 3 のプロセスに従って行われる。

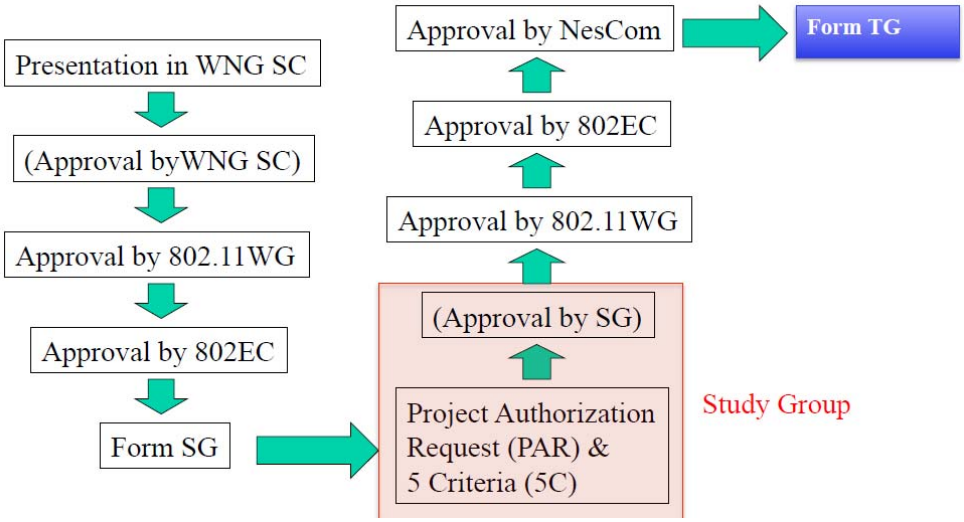


図 2. TG ができるまで

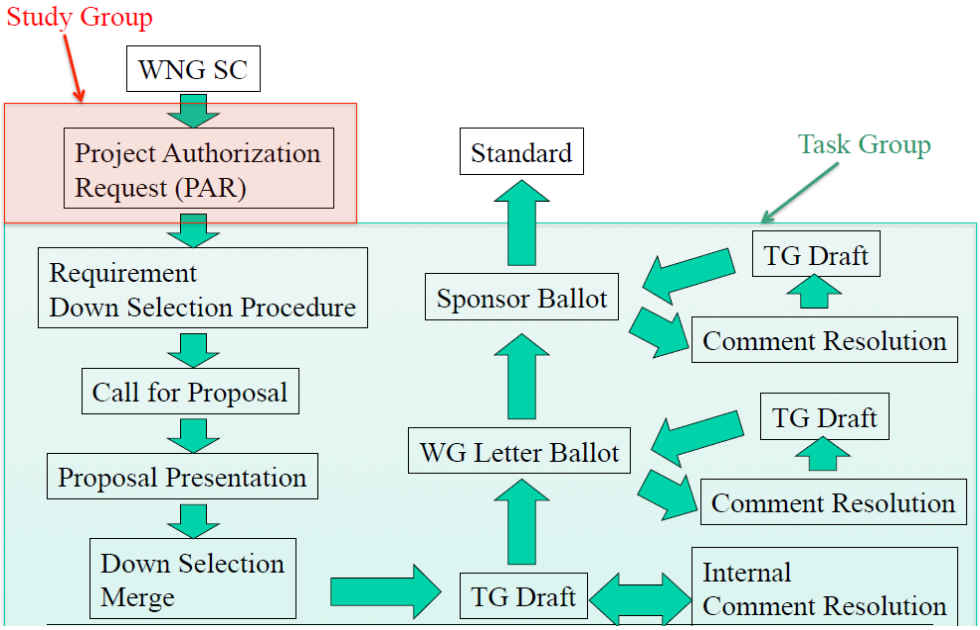


図 3. 標準化のプロセス

暗号に関連する規格等

IEEE802.11 は当初 WEP を採用したが、　セキュリティの脆弱性が指摘され、802.11i によって修正された。IEEE802.11 はセキュリティに対して非常に慎重であり、規格化のためにはセキュリティエキスパートと呼ばれる著名な人のレビューが必要である。また、暗号化アルゴリズム等の採用については NIST の承認が絶対的に必要である。

F. TCG

体制

Trusted Computing Group （以下、TCG）は、国際業界標準規格制定のための組織である。TCG では、会員によって技術仕様の策定が行われ、完成した仕様書は、社会での利用と実装が可能となるよう一般に公開される。TCG の会員による実装は、結果として TCG 技術の実用例となる。TCG の組織は、個々の技術分野の専門家が共同で仕様を開発可能にするため、ワーキンググループモデルで組織されている。このワーキンググループモデルは、協業及び競合の立場にある企業がベンダーに中立的かつ相互運用性のある最も良い仕様を開発できる中立的な環境を保ち続ける。TCG の体制図を次に示す。

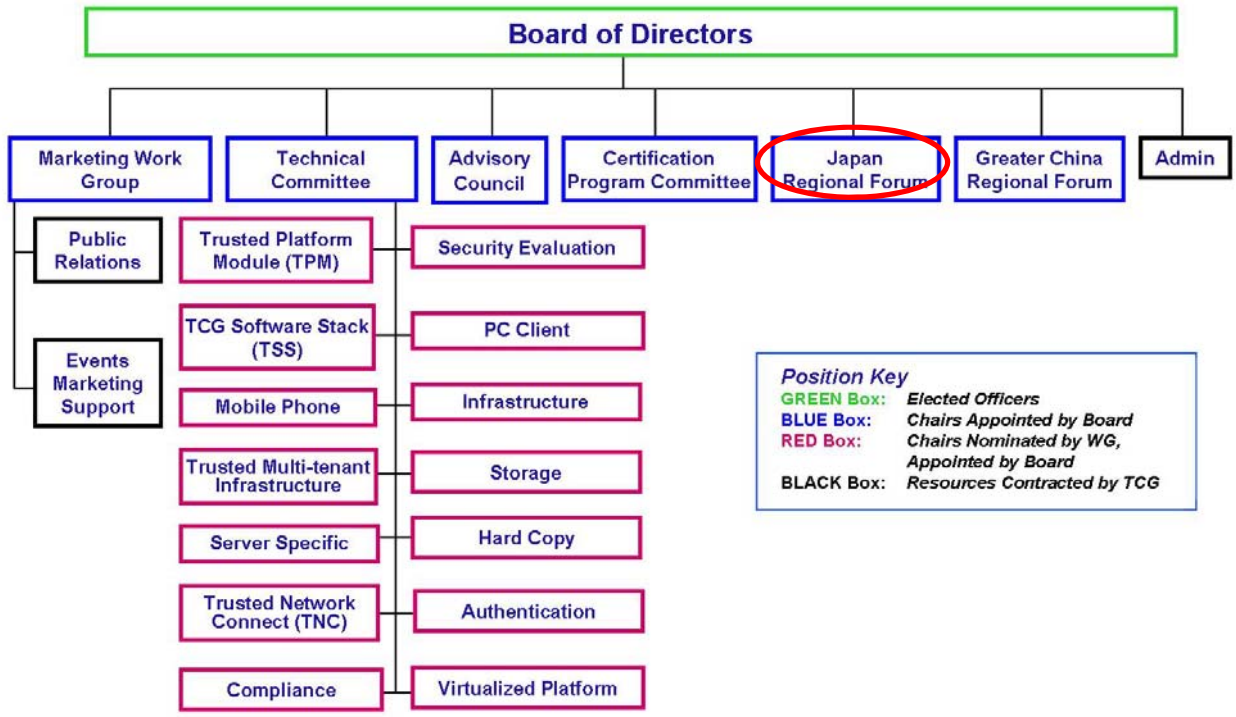


図 4. TCG の体制

Japan Regional Forum（以下、JRF）は TCG 内部の組織であり、日本の TCG 会員により構成される。JRF の目的は、TCG 技術の日本での普及及び採用働きかけ、日本政府・業界・市場と TCG の橋渡し、日本にいる TCG 会員の日本語での TCG 技術に関する情報交換の場を提供することである。

標準化の概要

TCG で策定する標準規格は次のような事項が考慮されている。

- 標準規格のインターフェースを用いた実装による、全世界での相互運用性と互換性の促進。
- TCG 技術による製品を提供する側と利用する側の双方でのコスト削減。

- 標準規格のプロトコルや機構による開発の効率化。
- 標準規格で公開され、専門家による綿密な評価、協力等により国際的に認められたセキュリティのプロトコルや暗号技術の利用。
- ハードウェアとソフトウェアのうまい組み合わせによる、安全なコンピューティング環境の構築。

暗号に関連する規格等

TPM[1]

その他

現在、METI 及び IPA が TPM 2.0 仕様書への日本の暗号アルゴリズム採用に向けた取り組みを行っている。TCG はこの仕様書を、ISO 国際標準とすべく活動をする予定である。METI/IPA は、2012 年 11 月、2013 年 2 月、3 月に Registry 仕様書へのレビュー及びコメントを行い、2013 年 5 月に JRF を通じて TCG の Board of Directors に Camellia 及び KCipher-2 の採用の打診を行った。また、2013 年 10 月には大阪にて、TPM WG へ Camellia の紹介と正式な評価依頼を行った。その後、2014 年 2 月にソルトレークシティ・メンバーミーティングでの活動も含め、現在も採用に向けた取り組みは続いている。

[1] Trusted Platform Module の略

G. 長期署名（ETSI）

体制

日本での電子署名（長期署名を含む）の標準化は日本ネットワークセキュリティ協会（以下、JNSA という）が行っている。電子署名の標準化活動を行う上で、JNSA は、特定認証業務の認定を行う日本情報経済社会推進協会（以下、JIPDEC という）やタイムスタンプ事業者認定等を行う日本データ通信協会（以下、JADAC という）とも調整を行う。また、医療分野における電子署名標準化を行っている保健医療福祉情報システム工業会（以下、JAHIS という）とは専門家同士の交流が行われている。2013 年より、JNSA は ETSI に加入し、日本からの意見を国際標準に反映すべく活動を行っている。

ETSI や CEN は欧州委員会からの標準化の指針に従って技術や運用に関する標準の策定を行う。その標準に従って、欧州内の各国が製品やサービスを開発・運用し、さらには事業者の監査や認定を行う。このようにヨーロッパでは、欧州委員会のトップダウンによる体系化されたアプローチを採り、制度と技術が結びついた整合性のあるフレームワークを目指している。

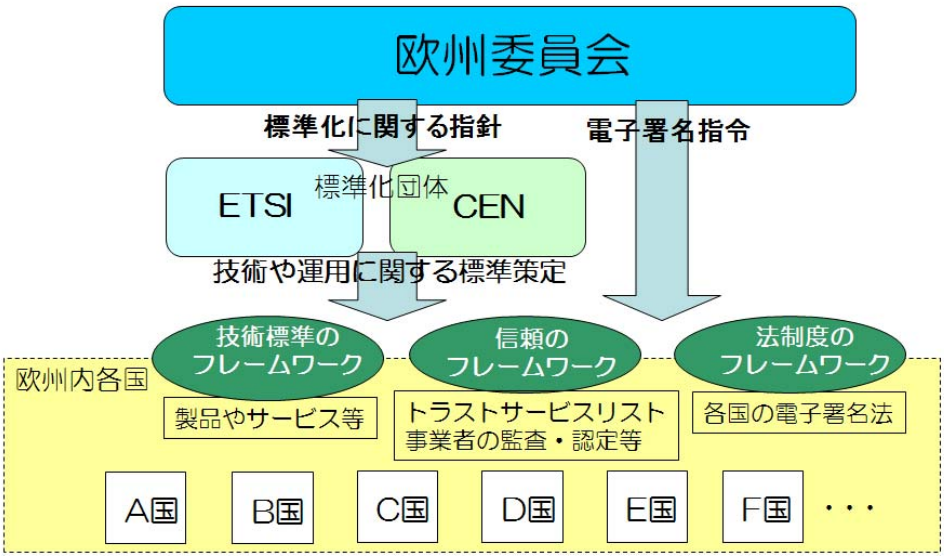


図 5. 欧州の体制

標準化の概要

電子署名は現在、CAdES[2]、 XAdES[3]、 PAdES[4]、ASiC[5]の 4 種類が ETSI で策定されている。このうち CAdES、XAdES については、長期保存のための要件を定めたプロファイル規格を日本が作成し、JIS 化及び ISO 化を行った。このプロファイル規格を元に JAHIS にて医療向けの電子署名プ

[2] CMS Advanced Electronic Signature の略
[3] XML Advanced Electronic Signature の略
[4] PDF Advanced Electronic Signature の略
[5] Associated Signature Container の略

ロファイルを規格化し、現在 ISO 化の作業を行っている。

- JIS X 5092:2008 CMS 利用電子署名(CAdES)の長期署名プロファイル
- 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
- 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)
- 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)

ISO/DIS 17090-4 Health informatics -- Public key infrastructure -- Part 4: Digital Signatures for healthcare documents

日本の電子署名法は市場主導型の米国の電子署名法ではなく、欧州の規制型の電子署名法に近い。ETSI では、法制度と整合性のとれた技術・運用の電子署名標準規格を作成している。ETSI の電子署名標準は国際的な電子署名規格としての影響力を持ち、実証実験等を通じて「使える標準規格」を目指す意識が強い。

上記のように既に欧州で電子署名標準の枠組みが作られており、日本発の電子署名技術を国際的な影響力を持つ標準にすることは難しい現状であるため、日本は欧州の標準に意見を投じ、国際的な標準へ反映させようとしている。その一環として、ETSI の標準化活動に対して、日本は様々な貢献をしている。例えば、電子署名の相互運用性を検証するための ETSI オンライン実証実験は日本で実施した実証実験がモデルとなっている。また、ETSI 電子署名規格への提言を行い改訂に至った。その他には、PDF に対する長期署名規格の必要性を訴えて PAdES 策定のきっかけを作ったり、CAdES 及び XAdES 長期署名プロファイルの ISO 規格を作成したりする等の様々な働きかけを行い、標準化活動に貢献している。

暗号に関連する規格等

電子署名に関する規格は次のように、参照されている。

表 2.電子署名の規格の参照

	ETSI	JIS	ISO	その他
CAdES	ETSI TS 101 733 (v2.2.1)	JIS X 5092:2008	ISO 14533-1 (2012)	JAHIS HPKI署名規格
XAdES	ETSI TS 101 903(v1.4.2)	JIS X 5093:2008	ISO 14533-2 (2012)	JAHIS HPKI署名規格
PAdES	ETSI TS 102 778 (v1.1.2)	検討中	検討中	なし
ASiC	ETSI TS 102 918 (v1.2.1)	なし	なし	なし

欧州ではこれまでも電子署名の規格だけではなく、署名生成デバイスに関する規格や電子証明書を発行する認証局や、タイムスタンプ発行局の運用に関する規格など周辺の様々な規格策定を行ってきた。現在、これらの規格の体系について見直しが行われている。これまでの規格の統廃合、機能領域の分類と整理を行い、新フレームワークを構築している。この新フレームワークには電子署名に用いられる推奨暗号リストの作成も含まれている。

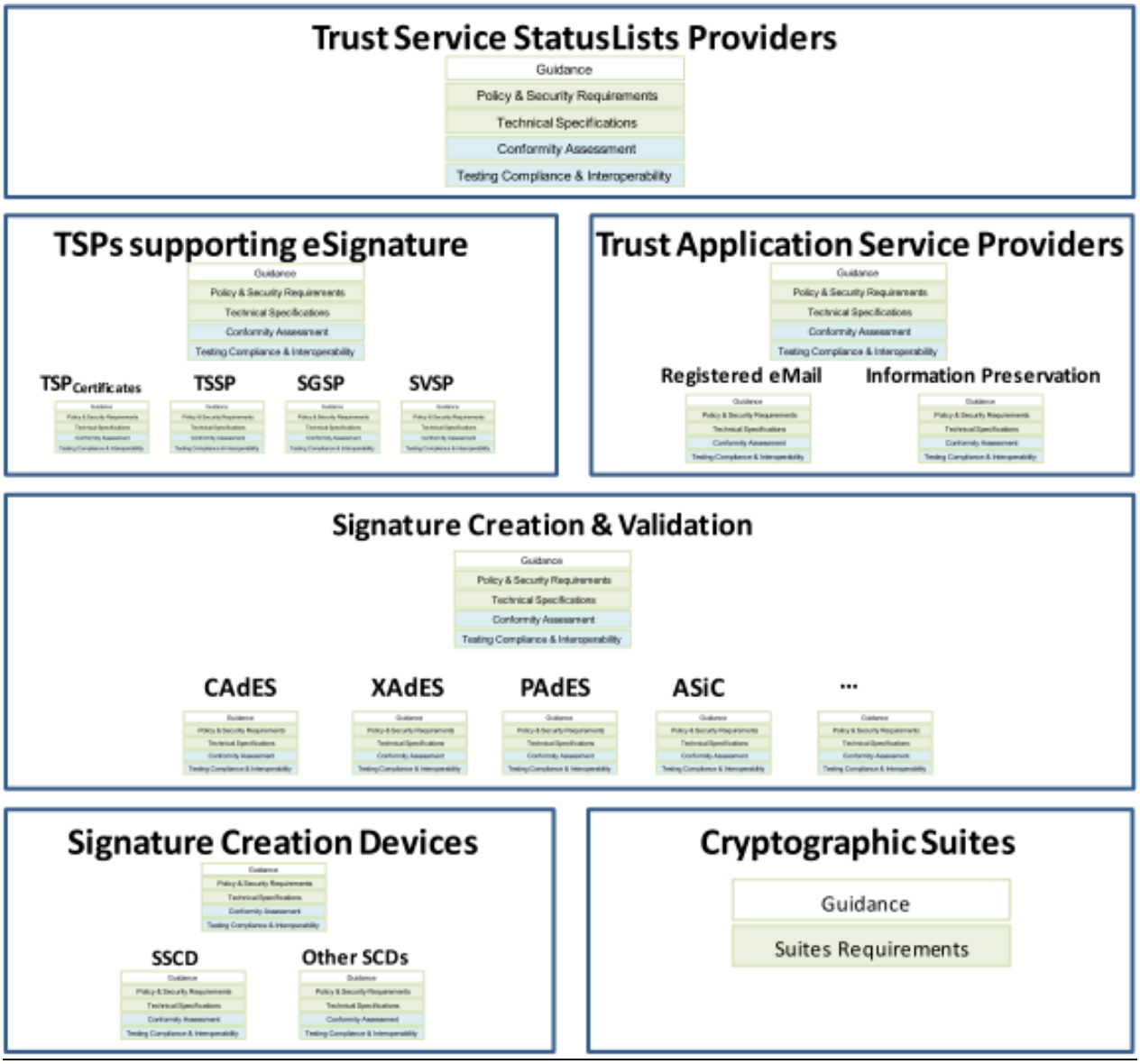


図 6. 欧州の新フレームワーク

<u>その他</u>

- 現状の課題

  ETSI の電子署名標準に関しては、EU 独自の仕様が入り込む可能性がある。標準（規格）が国際的な影響力を持つことを意識しているはずだが、EU のトップダウン的な電子署名指令があり、EU の問題であるという意識を持つ傾向がある。日本からも問題点を指摘し

ているが、全ての意見が反映されるわけではない。

日本の電子署名に関する課題は、国内に長期的展望で標準技術に関与できる組織がないことである。日本の各省庁、各業界団体はそれぞれのスコープに閉じており、全体を俯瞰して議論をする場、技術標準を取りまとめる場が日本にはない。例えば、電子証明書を発行する認証局の特定認証業務の認定は経済産業省、タイムスタンプは総務省といったように、省庁や業界団体が縦割りであり、それぞれのスコープが限定的でビジョンが共有されていない。欧州の新フレームワークのような体系化されたアプローチは困難な状況にある。

- 電子署名標準化に関する今後の予定
  - ISO 14533-1 (CAdES 方式)の改訂作業
    今年発行された新しい ETSI 規格の内容に合わせた ISO 14533-1 (CAdES 方式) の修正作業を行っている。近々DIS 投票が行われる予定である。
  - PDF 電子署名(PAdES 方式)に関する長期保存のためのプロファイル規格策定
    PDF 電子署名 (PAdES 方式) に関する長期保存のためのプロファイル規格を策定し、2月にドラフトを発表した。今後は本規格の ISO 化を目指す。
  - 電子署名の検証規格
    現在、電子署名の検証方法を明確化した規格を ETSI で定めている。欧州内の事情を色濃く反映したものになっているため、日本が代案を提案している。なお、ISO 規格化も視野に入れている。

H. 放送

体制

- 総務省　情報通信審議会
  - ➢ 情報通信技術分科会
    - ✧ 放送システム委員会
- 電波産業会（ARIB）技術委員会

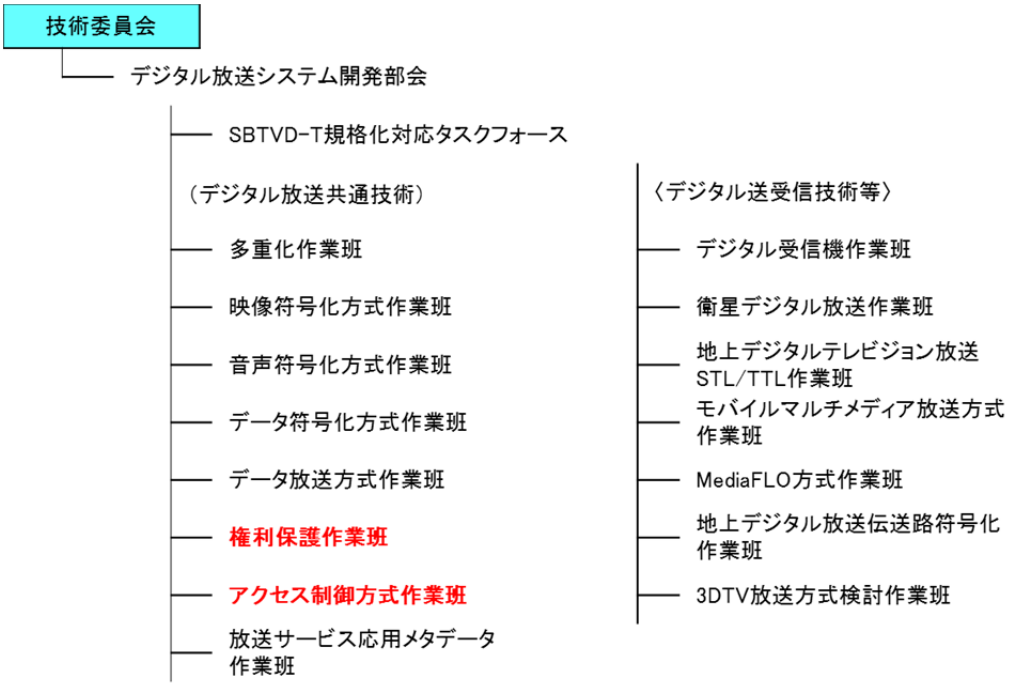


図 7.ARIB 技術委員会 デジタル放送システム開発部会の体制

標準化の概要

放送コンテンツの権利保護とアクセス制御（限定受信方式）には暗号技術が利用されている。現行の BS デジタル放送や地上デジタル放送等のアクセス制御方式（限定受信方式）は、総務省情報通信審議会で審議され策定された。現在、新たな映像符号化方式等、現行の高精細度テレビジョン放送を超える飛躍的な画質の向上に資する映像技術等の研究開発等の進展に伴って、情報通信審議会では、「超高精細度テレビジョン放送」の実用化、普及促進等を図るため、必要な技術的条件が取りまとめられている。

- 情報通信審議会
  - ➢ 超高精細度テレビジョン放送システム標準化の経緯

    通信・放送サービスに関する今後の取組みについて、平成 24 年 7 月、情報通信審議会から「4K・8K（スーパーハイビジョン）」、「スマートテレビ」、「ケーブル・プラットフォーム」の 3 つの WG についての提言が行われた。その具体化に必要な事項を検討することを目的として「放送サービスの高度化に関する検討会」が開催され、「スーパーハイビジョン WG」「スマートテレビ WG」及び「ケーブル・プラットフォーム WG」の 3 つの WG が設置された。平成 25 年 6 月 11 日に検討結果の取りまとめが公

表され、スーパーハイビジョンに関するロードマップが示された。(2014 年に 4K の試験的な放送を開始、2016 年に 8K の試験的なサービスを実施、2020 年に 8K の本放送を開始)

- 情報通信審議会　情報通信技術分科会　放送システム委員会
  5 回にわたり超高精細度テレビジョン放送システム作業班を開催し、2014 年 1 月 31 日に放送システム委員会にて作業班の最終報告を行った。最終報告では、限定受信方式におけるスクランブルサブシステム[6]および関連情報サブシステム[7]の技術的条件等が示された。

- ARIB
  権利保護作業班及びアクセス制御方式作業班（体制図の赤字部）にて、情報通信審議会の答申を受け、超高精細度テレビジョン放送の限定受信方式及びコンテンツ保護方式に関し、A 標準規格「デジタル放送におけるアクセス制御方式」(ARIB　STD-B25）を改定する。

<u>暗号に関連する規格等</u>

- BS デジタル放送：MULTI2
- 地上デジタル放送：MULTI2
- 携帯端末向けマルチメディア放送：MULTI2、AES、Camellia
- 超高精細度テレビジョン放送システム：「AES」と「Camellia」の鍵長 128 ビットから選択可能

<u>その他</u>

超高精細度テレビジョン放送システムにおいて、暗号に関して次のような課題がある。

- スクランブル方式の暗号アルゴリズムの選定にあたっては、次の事項に留意することが望まれる。
  - スクランブル方式は、暗号アルゴリズム自身の安全性だけではなく、受信機における実装面、コスト面及び実用化スケジュールの状況、ならびに、長期にわたってセキュリティリスクを抑える送出運用等を考慮して、民間規格や運用規定に関する検討の場において、放送事業者や受信機製造メーカ等の関係者で最終的に選定する必要がある。
  - 長期的視点で見ると、より効率的な暗号解析手法が見つかる可能性も否定できない。CRYPTREC の電子政府推奨暗号リストの改定等、暗号アルゴリズムの最新動向を引き続き注視する必要があり、また、民間規格や運用規定に関する検討の場において、必要に応じて、さらなる議論、検討が行われる必要がある。

[6]スクランブルサブシステム：未契約者には信号が受信できないように信号を暗号化して送り、既契約の受信機で復号する仕組み
[7]関連情報サブシステム：デスクランブルを行うか否かを制御するための情報（関連情報※）を処理する仕組み

- 超高精細度テレビジョン放送のスクランブル方式に関して、脆弱性が発見された場合においても適切に対応可能とするため、複数の暗号アルゴリズムから選択可能とすることを検討したが、今後、秘匿性維持の観点で、メディアに対して横断的な利用についても検討することが重要である。その際、現行放送との整合性に留意する必要がある。

I. 医療（ISO TC215）

ISO TC215 の対象範囲

ISO TC215/WG4 では、ヘルスケア情報領域におけるセキュリティとプライバシー保護に関する標準の策定を次のために行う。

① ヘルスケア情報の完全性、機密性、可用性の保持と拡大
② 患者の安全に悪影響を与えるものからのヘルスケア情報システムの防護
③ 個人情報に関わるプライバシー保護
④ ヘルスケア情報システムの利用者に対する責任の明確化

体制

ISO TC215 のコンビナーは、Lori Leed Fourquet（米国）であり、2013 年 6 月より二期目就任を果たしている。副コンビナーは茗原秀幸（日本）であり、2013 年 6 月より新任である。また、セクレタリは、Diana Warner（米国）が 2012 年度より就任している。

国内には、ISO TC215 国内対策委員会があり、その下に WG4 作業部会がある。WG4 作業部会の主なメンバーは、JAHIS、JIRA、JAMI、MEDIS-DC、厚生労働省となっている。

標準化について

JAHIS セキュリティ委員会では、ISO TC215/WG4 に関するエキスパートとして国内対策委員会にメンバーを派遣している。セキュリティ委員会では、各規格の対応の検討や投票コメントの検討等を実施している。さらに詳細な検討が必要な場合には、JAHIS の担当 WG にて具体的な翻訳作業、詳細仕様の検討等を実施する。また、JIRA セキュリティ委員会と積極的に意見交換を実施し、産業界としての統一見解の取りまとめを実施している。日本としての投票の際には、JAHIS の見解として ISO TC215 国内対策委員会 WG4 作業部会(大山部会長：東京工業大学) に対して意見具申を行う。その他には、JAHIS 標準類の ISO 規格への組込みを積極的に実施し、逆に制定済み ISO 規格の JAHIS 標準類への反映も実施している。

ISO TC215/WG4 の主要な規格について

ISO TC215/WG4 の主要な規格の例を次に示す。

- Health Informatics - Guidelines on data protection to facilitate trans-border flows of personal health information (IS22857)
  - IS22857 は国や地域をまたがる個人ヘルスケア情報のやりとりにおける個人情報保護の IS であり、WG4 における最初に策定された国際標準である。EU 指令や HIPAA 法等を参照し、個人情報保護に関する要件を定めている。また、各国の慣習や文化の違いを考慮して、各国の法律と本規格に差異があった場合の対処も記載されている。また、JAHIS セキュリティ委員会の検討結果を受けた日本の要請により死者の情報に対しても情報保護を要求する等、ヘルスケア独自の要素が組み込まれている。現在は規格成立 3 年後のシステマティックレビュー（以下 SR）の結果として修正された FDIS 投票

が完了し、出版待ちの状態である。また、CEN の関連規格と統合し新たな規格とする作業項目提案が通過しており IS16864 として検討が開始される予定である。

- **Health informatics - Public key infrastructure (IS17090)**
  - IS17090 はヘルスケア部門向けの PKI（HPKI）に関する IS である。Part1－Part3 は IS として出版され、Part4 は現在策定中である。本規格は日本の厚生労働省の認証局ポリシーと整合性が取られている。
    - ✧ **Part1 Framework and overview**： HPKI のフレームワーク及び概要を記載している。発行対象の種類（自然人、アプリケーション等)、役割の種別等が規定されている。SR の結果、改定版が FDIS を通過して出版された。
    - ✧ **Part2 Certificate profile**： HPKI の証明書に記載される内容について記載している。PKI としての標準的な箇所の定義とヘルスケア独特の hcRole の定義がなされている。SR の結果、改定版の FDIS 投票が行われる予定である。
    - ✧ **Part3 Policy management of certification authority**：認証局における認証ポリシー作成のためのガイドラインを記載している。SR でそのまま承認された。
    - ✧ **Part4 Digital Signatures for healthcare documents**：日本の JAHIS 標準をそのまま ISO に提案したものである。日本主導で規格化を行っている。現在 DIS 投票にかかっている。
- **Health Informatics - Dynamic on-demand virtual private network for health information (TR11636)**
  - TR11636 は VPN を医療分野に適用した場合のメリット等について実際の利用例をベースにまとめた TR である。日本の HEASNET の報告書をベースに策定された。

J. M2M/IoT に関係する標準化団体（ISA-100・IEEE1888・ISO/IEC JTC1/SC6/WG7・IETF）

J.1. ISA-100

体制

ISA-100 の体制についての概略図を次に示す。

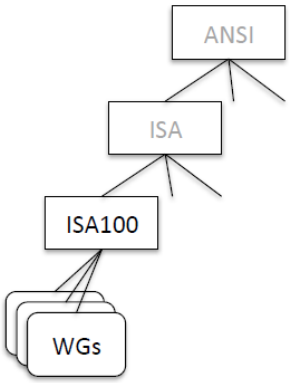


図 8. ISA-100 の体制についての概略図

標準化について

工業向け計測制御無線システムの技術の検討と標準化を行うことを目的としている。データリンク層からアプリケーション層の技術やシステムまでを標準化の対象としている。ISA-100 では、セキュリティは必須項目であり、基本となる技術を規定する ISA100.11a WG では Security Sub-WG が設立された。バックホールを含むシステムについて、ISA-99（工業ネットワークのセキュリティを扱うグループ）とリエゾン関係である。

暗号に関する規格等について

- ISA100.11a では、IEEE802.15.4 で使用する AES128-CCM をエンドノード間の暗号化と認証にも再利用している。
- システム全体では、FW 技術や IPsec、TLS、IEEE802.1X を使用する。
- Wi-Fi Security として WPA/WPA2 を利用する。

J.2. IEEE1888

体制

IEEE1888 の体制についての概略図を次に示す。

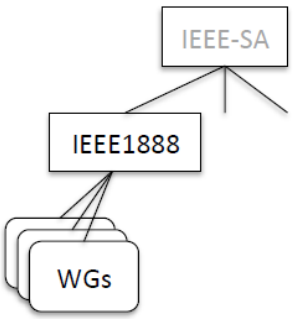


図 9.IEEE1888 の体制についての概略図

標準化について

ビルや設備等の統合エネルギー管理を目的とした通信技術の標準化を行う。トランスポート層からアプリケーション層の技術及びシステムまでを標準化の対象とする。運用実績のある技術を再利用してシステムとして動作する技術を検討している。

暗号に関する規格等について

IEEE1888.3 では、機器の Identifier を定義し、X.509 証明書での表現方法と ACL に対する必須要件、TLS の用法を定義している。トランスポート層のセキュリティとして TLS を参照し、アプリケーション層のセキュリティ技術として X.509 証明書を用いる。

J.3. ISO/IEC JTC1/SC6/WG7

体制

SC6 の体制についての概略図を次に示す。

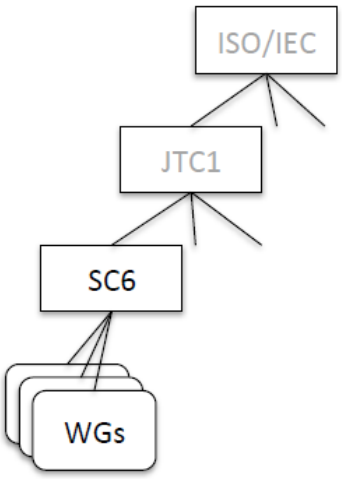


図 10.SC6/WG7 の体制についての概略図

標準化について

情報システム間の通信技術の国際標準化を行うことを目的としている。データリンクより上のレイヤの技術を対象としている。また、“Future Network”も扱う。各国の技術を標準化する傾向が強いため、運用実績や相互接続性のレベルが異なる。なお、セキュリティの専門家は非常に少ない。

暗号に関する規格等について

IETF で標準化された技術を参照し、リエゾンする場合もある。

J.4. IETF

体制

IETF は 8 つの Area、約 120 の WG から構成される。インターネット全般の技術全般を扱うた

め WG は非常に多い。Security Area 以外の WG の参加者はセキュリティの知識が少ない傾向にある。セキュリティプロトコルに関しては、他のグループとリエゾンすることが多い。体制図については、K 節（後述）に示す。

標準化について

インターネット技術全般のデファクト標準化を行うことを目的としている。データリンクより上のシステムを標準化の対象としている。また、アプリケーション層の技術を含む場合もある。会社や国の代表としてではなく、個人として議論に参加する。全ての議論や文書が公開されており、誰でも自由に議論に参加でき、文書を発行できる。また、各標準化団体が定める技術に再利用される傾向が強い。

十分に検討された技術は RFC（Request for Comments）として発行される。運用と相互接続の結果、改定されることがある。十分な動作実績のある仕様と相互接続性が最も重要とされている。

暗号に関係する WG について

Security Area でも暗号アルゴリズムの扱いを議論する WG は限られている。例えば、TLS、kitten、IPsec、PKIX 等である。暗号アルゴリズムについては Security Area Advisory Group で議論される。研究段階のものは、CFRG（IFRG）でも議論される場合がある。NIST からの貢献が非常に大きい。

J.1 から J.4 のまとめ

ISA-100、IEEE1888、ISO/IEC JTC1/SC6/WG7、IETF は M2M/IoT に関係する標準化団体である。各標準化団体はインターネット技術、セキュリティプロトコル及び暗号アルゴリズムにおいては、IETF が策定した技術を利用する傾向が強い。その結果として、IETF に様々な暗号アルゴリズムが提案されている。なお、データリンク層の技術については、IEEE が定めた技術を利用する傾向が見られる。

K. IETF

体制

IETF はインターネット技術の標準仕様を策定することを目的として組織されたグループであり、IETF における技術仕様は RFC（Request for Comments）という名前で文書化され、公開される。RFC は、IESG の承認後、番号が割り当てられ、IANA レジストリに登録される。その後、RFC Editor によって公開される。IETF の体制図を次に示す。

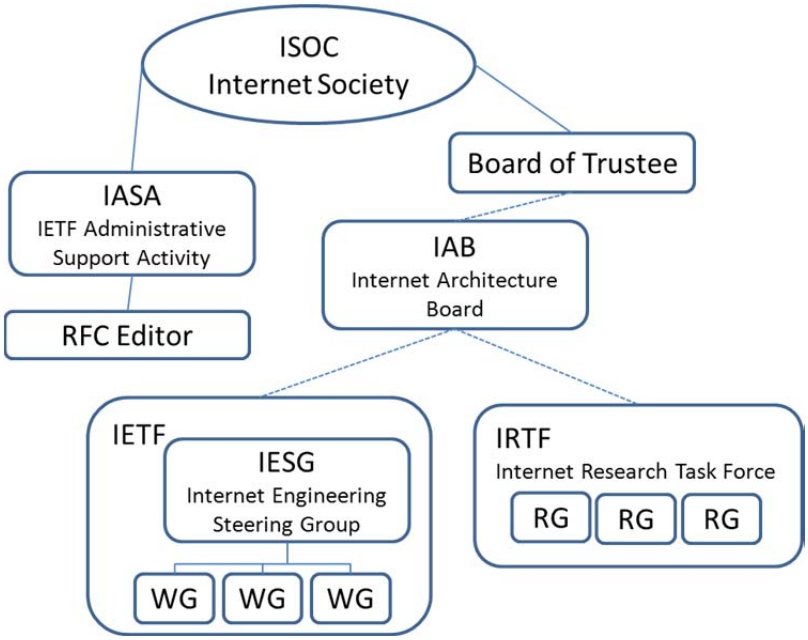


図 11. IETF の体制

標準化の概要

標準化のプロセスを次に示す。

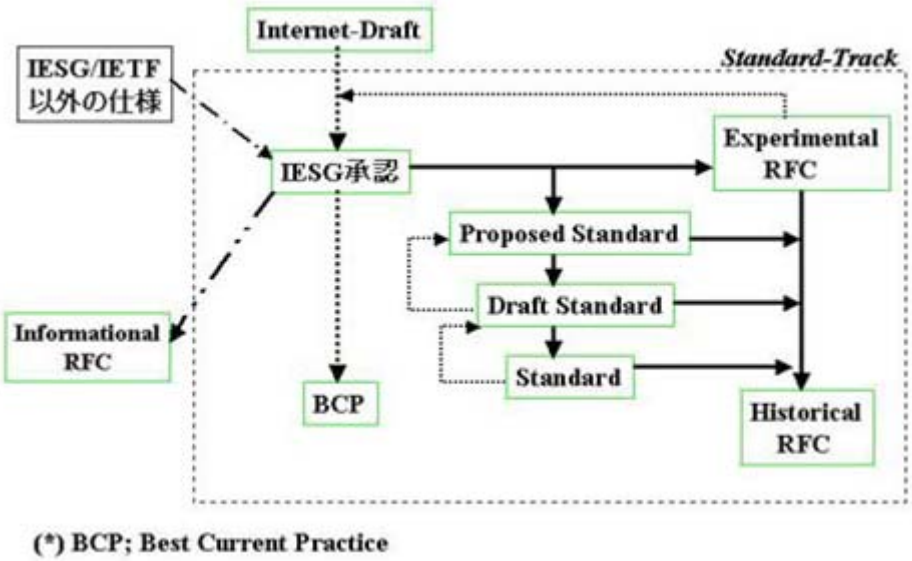


図 12. RFC 化のプロセス

RFC は Informational RFC、Standard Track RFC、Experimental RFC、及び Historical RFC の 4 種類に分かれる。そのうち、標準とされるのは Standard Track である。これは、Working Group でコンセンサスが取られ、業界で国際標準とすべき仕様をまとめたドキュメントである。PS(Proposed Standard)、DS(Draft Standard)を経て、S(Standard)となる。PS は複数の組織での独立な実装テストと相互接続性の確認が条件、DS は実質的かつ広範囲での運用テストが条件となっている。S(Standard)の状態になると、STD 番号が割り振られる。現在、STD 番号を割り振られているドキュメントは非常に少数であり、実質的には、DS の RFC になると、国際標準とみなすことができる。

IETF の標準化活動は、メーリングリスト（以下、ML という）やミーティングにて行われる。ML には、アナウンス ML や WG のディスカッション ML 等がある。IETF のミーティングは年 3 回行われる。その他に WG やワークショップの中間（Interim）ミーティングも行われる。

<u>暗号に関連する規格等</u>

- TLS
  AES-CCM（AES-counter with CBC-MAC）が 2012 年 12 月に RFC6655 として追加された。また、2013 年 11 月の IETF88 にて、ChaCha20 の追加に向けた動きがあった。
- DNSSEC
  特に大きな動きはなく、既存の RSA、GOST、ECDSA 等が IANA レジストリに登録されている。2013 年 4 月に RFC6944 にて、RSA/MD5 が「MUST NOT」となった。
- IPsec
  特に大きな動きはなく、AES-CBC、Camellia-CBC 等が利用可能である。
- RPKI
  2012 年 2 月 RFC6485 にて、RSA2048、SHA-256 のみが指定されている。

資料３

暗号技術検討会

２０１３年度報告書（案）

２０１４年３月

目　　次

１．はじめに

情報通信技術を安心・安全に利用できる環境を構築していくにあたり、暗号技術は必要不可欠なものとなっている。また、昨今暗号技術は、クラウドコンピューティングやビッグデータの活用においても、データの活用とプライバシー保護の両立などのキーテクノロジーとしてますます注目を集めている。このため、暗号解読技術等の進展に注意を払い、適切なものを使用するよう努めることが重要であり、引き続き監視を行っていくことが重要である。

政府においても、情報セキュリティ政策会議（議長：内閣官房長官)において、2013 年 6 月に「サイバーセキュリティ戦略」が決定され、暗号技術については、「安全評価がなされたものの利用」を推進することが示されている。また間もなく改定が予定されている「政府機関の情報セキュリティ対策のための統一基準」では、暗号化及び電子署名のアルゴリズムについて、CRYPTREC 暗号リストに記載されたアルゴリズムを使用することが定められる見込みである。CRYPTREC としても、暗号に関する技術的な評価等を通じて、政府のこれらの動きを適切に支援していく。

CRYPTREC は、「電子政府推奨暗号リスト」（平成 15 年 2 月 20 日公表）を昨年度に改定した「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（CRYPTREC 暗号リスト)」を策定したことを踏まえ、今年度から暗号技術検討会の下に暗号技術評価委員会と暗号技術活用委員会の 2 委員会を設ける体制に移行した。新設の暗号技術評価委員会では前年度の暗号方式委員会の全課題及び暗号実装委員会の一部課題を、また新設の暗号技術活用委員会では前年度の暗号運用委員会の全課題及び暗号実装委員会の一部課題を引き継ぎ、暗号技術に関する継続的な評価・監視を通じてリスト掲載暗号の安全性を担保すると同時に、掲載暗号の利用の取組を推進する。

今年度の委員会別の活動として、暗号技術評価委員会では、暗号技術の安全性及び実装に係る監視及び評価、軽量暗号などの新世代暗号に係る調査、暗号技術の安全な利用方法に関する調査等を行った。暗号技術活用委員会では、運用ガイドラインの検討や標準化推進に向けた調査等の暗号の普及促進・セキュリティ産業の競争力強化に係る検討、暗号技術の利用状況に係る調査及び必要な対策の検討等を行った。なお、2013 年度の活動のうち、詳細な技術的事項については、暗号技術評価委員会及び暗号技術活用委員会における議論を踏まえて、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取りまとめる「CRYPTREC Report 2013」を参照いただきたい。

末筆であるが、本検討会及び関係委員会に御協力いただいた構成員、オブザーバの方々をはじめ、関係者の皆様に心から謝意を表する次第である。

2014 年 3 月

暗号技術検討会

座長　今井　秀樹

２．暗号技術検討会開催の背景及び開催状況

２．１．暗号技術検討会開催の背景

暗号技術は情報セキュリティの基盤技術であり、その安全性を暗号技術の専門家により技術的、専門的な見地から客観的に評価することが重要である。電子政府のセキュリティ確保のためには、安全性に優れた暗号技術を利用することが不可欠である。

このため、総務省及び経済産業省は、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化し、各府省に対してその利用を推奨することにより、高度な安全性と信頼性に支えられ、国民が安心して利用できる電子政府の構築に貢献することを目指し、2001 年度から暗号技術検討会を開催した。

暗号技術検討会において 2002 年度に策定された電子政府推奨暗号リストは、2012 年度に 10 年ぶりの改定が行われ、「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）」（以下、「CRYPTREC 暗号リスト」という。）として発表されたが、その後においても、電子政府推奨暗号等の安全性を評価・監視し、暗号技術の更なる普及促進を行うため、総務省及び経済産業省は、継続的に暗号技術検討会を開催している。

２．２． CRYPTREC の体制

CRYPTREC とは、Cryptography Research and Evaluation Committees の略であり、総務省及び経済産業省が共同で開催する暗号技術検討会（座長：今井秀樹中央大学教授）と、独立行政法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で開催する委員会から構成される暗号技術評価プロジェクトをいう。

2013 年度の CRYPTREC の体制は、前年度の３委員会体制（暗号方式委員会、暗号実装委員会、暗号運用委員会）を再編し、暗号技術検討会の下に、暗号技術評価委員会及び暗号技術活用委員会の２つの委員会を設置し、調査・検討を行った。

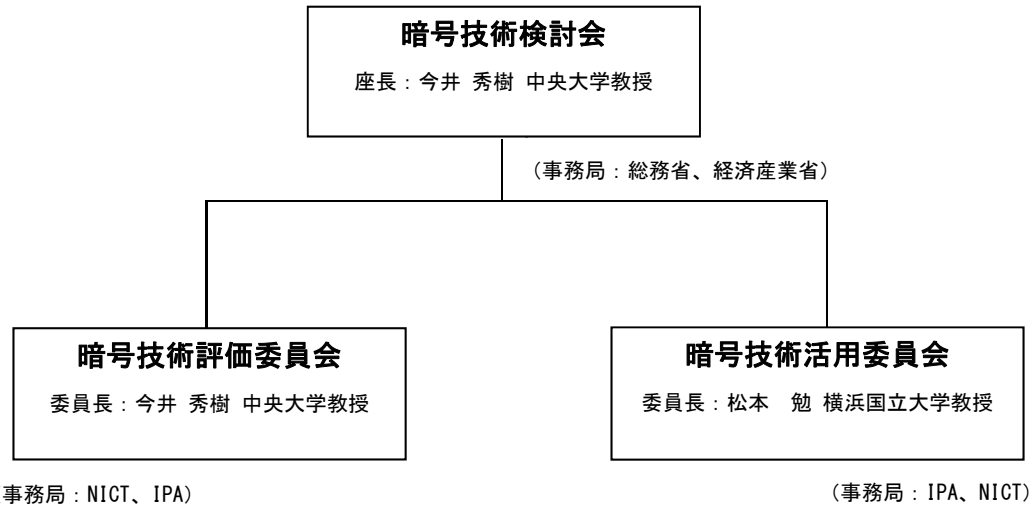


図 2.1　2013 年度 CRYPTREC の体制図

２．３．暗号技術検討会の開催状況

2013 年度の暗号技術検討会は、暗号技術評価委員会及び暗号技術活用委員会の計画及び報告を審議するために２回開催し、その他に暗号技術活用委員会で作成する「SSL/TSL サーバ構築ガイドライン」の策定状況について、メール審議を行った。

【第 1 回】2013 年 7 月 5 日（金）14:00～15:30

（主な議題）

- 暗号技術評価委員会及び暗号技術活用委員会の活動計画について
- CRYPTREC 暗号リストの暗号アルゴリズム仕様書について

（概要）

- 暗号技術検討会の下部委員会である、暗号技術評価委員会及び暗号技術活用委員会の 2013 年度の活動計画について説明を行い、承認を得た。
- 暗号技術活用委員会で作成する、SSL/TLS に関する運用ガイドラインについて、策定に当たっての検討の結果、運用ガイドラインでは必ずしも電子政府推奨暗号リストに掲載された暗号のみを取り上げるわけではないことも想定されるため、これまでの CRYPTREC の活動と整合するかどうか等の観点から作成されたガイドラインを事前に検討会でチェックし、CRYPTREC のクレジットとして発行すべきものか否かを判断する場を設けることとした。
- CRYPTREC ホームページにおいて掲載している CRYPTREC 暗号リストに掲載された暗号技術の仕様書の参照先を更新することにした。

【第 2 回】2014 年 3 月 27 日（木）14:00～16:00

（主な議題）

- 暗号技術評価委員会、暗号技術活用委員会の活動報告について
- 2013 年度暗号技術検討会報告書（案）について
- 2014 年度の暗号技術検討会、暗号技術評価委員会及び暗号技術活用委員会の活動計画について

（概要）

- 本日の議論を踏まえ記載。

【メール審議】2013 年 12 月 24 日（火）～2014 年 1 月 17 日（金）

- 暗号技術活用委員会において策定中の「SSL/TLS サーバ構築ガイドライン」について、第１回暗号技術検討会における議論を踏まえ、中間とりまとめの段階でメール審議を実施した。構成員からは、特段の意見は出されなかった。

３．各委員会の活動報告

３．１．暗号技術評価委員会

３．１．１．活動の概要

暗号技術評価委員会は、2013 年度に新たに発足した委員会であり、2012 年度まで開催していた暗号方式委員会の全課題及び暗号実装委員会の一部課題を主に引き継ぎ、暗号技術の信頼性に関する調査・検討を実施する。

2013 年度は、暗号技術の安全性及び実装に係る監視及び評価、新世代暗号に係る調査、暗号技術の安全な利用方法に関する調査等を行った。以下に、その具体的内容を報告する。

３．１．２．2013 年度の活動内容

暗号技術の安全性及び実装に係る監視及び評価

2013 年度は、研究集会、国際会議、研究論文誌の情報等を収集し、リスト掲載暗号の安全性について監視活動を行った。攻撃研究等に関して、早急な対処が必要なものは存在しなかったが、暗号解読技術等の進展が見られ、これらについて引き続き注視していく必要がある。

また、擬似乱数生成アルゴリズム Dual_EC_DRBG の脆弱性の可能性等、リストに掲載されていない暗号に関しても、社会への影響が大きい話題については注意喚起を実施した。

新世代暗号に係る調査

本項目に係る活動に関しては、暗号技術評価委員会の下に暗号解析評価 WG 及び軽量暗号 WG を設置し、議論した。暗号解析評価 WG では、素因数分解や離散対数問題の困難性等、暗号技術の安全性に係る調査を実施した。軽量暗号 WG では、リソースの限られたデバイスにも実装可能な軽量暗号について、要求条件や評価方法等の検討を行った。

暗号技術の安全な利用方法に関する調査

CRYPTREC 暗号技術ガイドラインとして「SSL/TLS における近年の攻撃への対応」及び「SHA-1」を発行した。前者は、近年効率的な攻撃手法が開発された SSL/TLS について、安全に利用するための適切な設定等を推奨するための文書であり、今年度暗号技術活用委員会において作成された「SSL/TLS サーバ構築ガイドライン」においても参照されている。後者は、現在でも広範に使用されている一方で危殆化が進むハッシュ関数 SHA-1 について、許容される使用例を明示した文書である。

また、「電子政府推奨暗号リスト」の改訂を踏まえたリストガイドの改訂方針を検討した。

３．１．３．暗号技術評価委員会の開催状況

2013 年度、暗号技術評価委員会は計 3 回開催した。各回会合の概要は表 3.1 のとおりである。

表 3.1　暗号技術評価委員会の開催

回	年月日	議題
第 1 回	2013 年　7 月 29 日	暗号技術評価委員会活動方針の検討 WG 活動方針の検討 外部評価についての検討 監視状況報告 改訂された暗号アルゴリズム仕様書に関する検討
第 2 回	2013 年　12 月 13 日	WG 中間活動報告 外部評価についての検討 監視状況報告 暗号技術ガイドラインに関する検討 改訂された暗号アルゴリズム仕様書に関する検討
第 3 回	2014 年　3 月 6 日	WG 今年度活動報告 外部評価についての報告 監視状況報告 暗号技術ガイドライン策定の報告 次年度の検討項目に関する検討

３．２．暗号技術活用委員会

３．２．１．活動の概要

暗号技術活用委員会は、2013 年度から新たに設置された委員会であり、2012 年度まで開催していた暗号運用委員会の全課題及び暗号実装委員会の一部課題を引き継ぎ、CRYPTREC 暗号リスト改定の一環である暗号技術の利用状況に係る調査、暗号技術における国際競争力の向上及び運用面での安全性向上に関する検討を実施する。主要な検討課題は以下のとおりである。

・暗号の普及促進・セキュリティ産業の競争力強化に係る検討（運用ガイドラインの整備、教育啓発資料の作成等）
・暗号技術の利用状況に係る調査及び必要な対策の検討等
・暗号政策の中長期的視点からの取組の検討（暗号人材育成等）

2013 年度は、暗号の普及促進・セキュリティ産業の競争力強化に係る検討、暗号政策の中長期的視点からの取組の検討を行った。以下に、その具体的内容を報告する。

３．２．２．2013 年度の活動内容

暗号の普及促進・セキュリティ産業の競争力強化に係る検討

暗号技術の普及促進・セキュリティ産業の競争力強化についての課題分析を行うに当たって、まずは現状を把握するため、電子政府推奨暗号リストの活用状況や国産暗号に対する考え方等について、関係機関にヒアリングを実施した。

また、暗号の普及促進の具体的な方策について検討するため、暗号技術活用委員会の下に運用ガイドライン WG 及び標準化推進 WG を設置した。

運用ガイドライン WG では、暗号システムを安全に利用できるようにすることを目的とした運用ガイドラインの作成について議論を行い、2013 年度は利用者が多い SSL/TLS について取り上げ、「SSL/TLS サーバ構築ガイドライン」の策定作業を行った。本ガイドラインは、本年 7 月に完成する見込みである。

標準化推進 WG では、各標準化機関に対して、日本から暗号アルゴリズムを提案する際に効率的な提案活動が行えるよう、各標準化機関での活動状況について発表及び意見交換を行い、効率的な提案方法等について情報共有を行った。

暗号政策の中長期的視点からの取組の検討

暗号政策の中長期的視点からの取組である暗号人材育成について、必要な人材像を把握するために、暗号アルゴリズムの選択時の留意点や現状の実務担当者の暗号に関する知識レベル等について、関係機関にヒアリングを行った。

３．２．３．暗号技術活用委員会の開催状況

2013 年度、暗号技術活用委員会は、計 3 回開催された。各回会合の概要は表 3.2 のとおりである。

表 3.2　暗号技術活用委員会の開催

回	年月日	議題
第 1 回	2013 年　9 月 11 日	本年度の活動計画 運用ガイドライン WG 及び標準化推進 WG の活動内容の検討 「暗号政策上の課題の構造」や「暗号と産業競争力の関連性」について分析を行うためのヒアリング内容の検討
第 2 回	2013 年　12 月 13 日	SSL/TLS サーバ構築ガイドラインとりまとめの中間報告 標準化推進 WG の活動についての中間報告 ヒアリングについての中間報告
第 3 回	2014 年　3 月 19 日	ヒアリング調査報告 WG 活動報告 次年度の活動計画

４．今後の CRYPTREC 活動について

電子政府の安全性及び信頼性を確保し国民が安心して電子政府を利用できる環境を整備するため、2014 年度以降も引き続き以下の活動を実施する予定である。

(1) CRYPTREC暗号リストの小改定に関する意思決定（暗号技術検討会が実施予定）
- (a) 推奨候補暗号リストに掲載されている暗号技術の昇格を検討する
- (b) 新規暗号（事務局選出）及び新技術分類の追加（新規暗号公募含む）に関する方針を検討する。
- (c) 内閣官房情報セキュリティセンター等政府関係機関との連絡・調整を実施する。

(2) 暗号技術の安全性評価を中心とした技術的な検討（暗号技術評価委員会が実施予定）
- (a) 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、耐量子計算機暗号等）を実施する。
- (b) 暗号技術の安全性に係る監視及び評価（SHA-3の評価を含む）を実施する。
- (c) 暗号技術の安全な利用方法に関する調査（技術ガイドラインの整備、学術的な安全性の調査・公表等）を実施する。

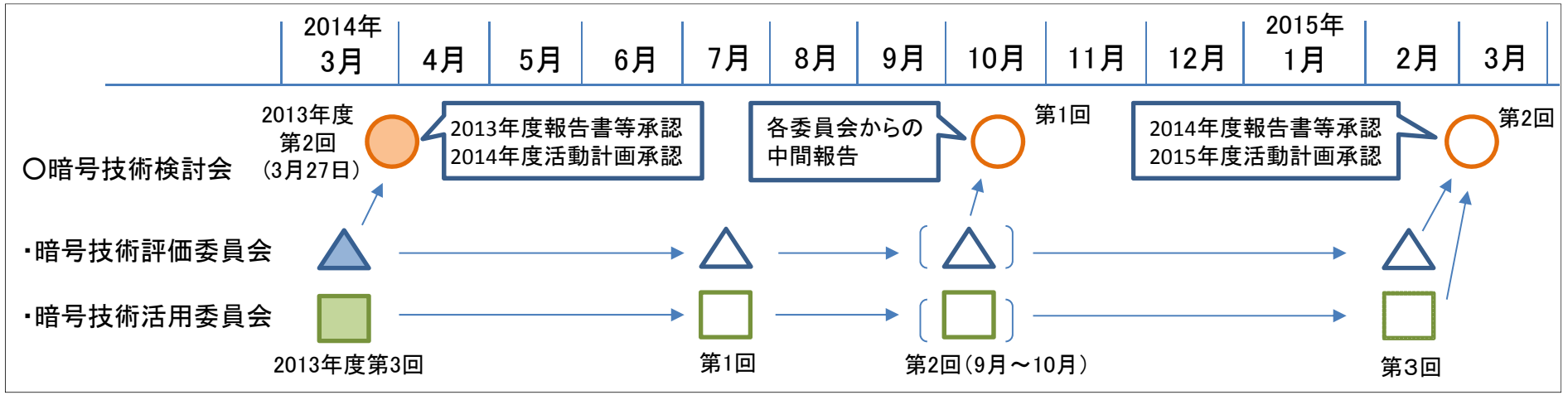
(3) セキュリティ対策の推進、暗号技術の利用促進及び産業化を中心とした暗号利用に関する検討（暗号技術活用委員会が実施予定）
- (a) 暗号の普及促進・セキュリティ産業の競争力強化に係る検討（運用ガイドラインの整備、教育啓発資料の作成等）を実施する。
- (b) 暗号技術の利用状況に係る調査及び必要な対策の検討等を実施する。
- (c) 暗号政策の中長期的視点からの取組の検討（暗号人材育成等）を実施する。

2014年度暗号技術検討会活動計画

資料4

暗号技術検討会及び関連委員会（暗号技術評価委員会及び暗号技術活用委員会）の活動を通じて、電子政府推奨暗号等に関する安全性の監視・評価及び普及促進等を実施。

1. CRYPTREC（暗号技術検討会及び関連委員会）の開催予定



2. 2014年度CRYPTREC体制図及び検討事項

暗号技術検討会

座長：今井 秀樹（東京大学）

（事務局：総務省及び経済産業省）

暗号技術に関する調査・検討

内閣官房情報セキュリティセンター（NISC）

「政府機関の情報セキュリティ対策のための統一基準」等へのインプット

暗号技術評価委員会

委員長：今井 秀樹（東京大学）

（事務局：NICT及びIPA（主担当はNICT））

- 暗号解析評価WG
- 軽量暗号WG

検討事項：暗号技術の安全性に関する監視・評価等

暗号技術活用委員会

委員長：松本　勉（横浜国立大学）

（事務局：NICT及びIPA（主担当はIPA））

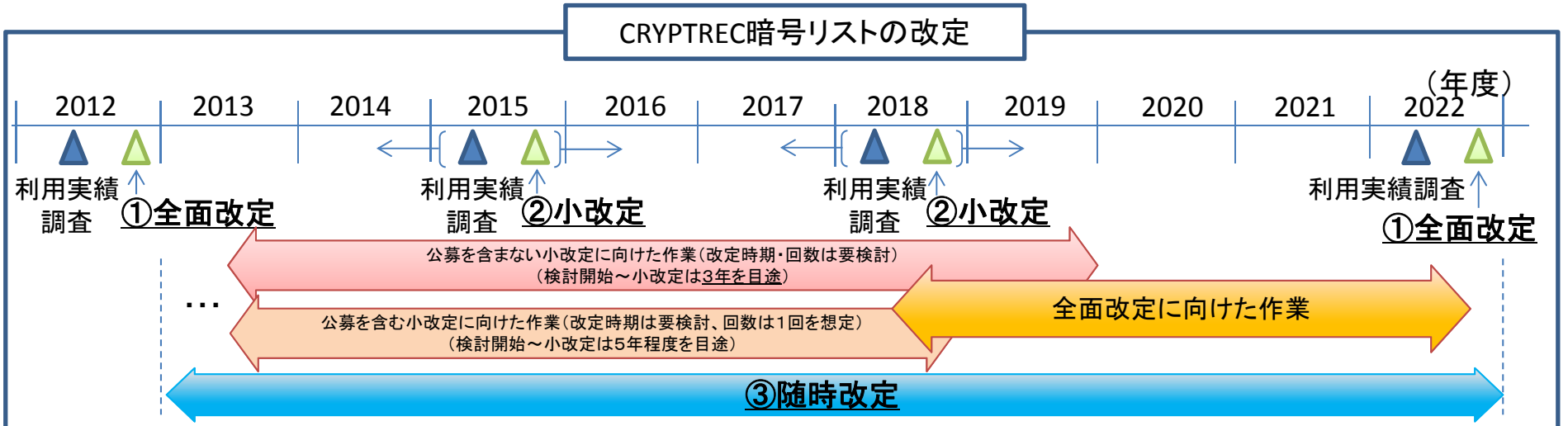
- 標準化推進WG
- 運用ガイドラインWG

検討事項：暗号技術における国際競争力の向上及び運用面での安全性向上等

（参考）長期的な活動方針

CRYPTREC暗号リストに関する検討

（方針） 全面改定は頻繁には行わない（10年程度の運用を想定する）ものの、小改定（推奨候補暗号リストから電子政府推奨暗号リストへの昇格等）は定期的（3年を目途）に見直しをする方向とする。また、運用監視暗号リストへの降格等は随時改定することとする。加えて、各年度で作成する技術的ガイドラインの効果的利用方法も検討する。



各年度で作成する技術的ガイドラインも効果的に利用

①全面改定 ： 以下は、10年を目途に、安全性、実装性能、利用実績（見込み含む）の検討に基づき、全面改定で対応する。
- 既存の技術分類の修正を伴う技術分類見直し、3リスト構成そのものの見直し、新規暗号の全面的公募等

②小改定 ： 以下は、3年を目途に、安全性、実装性能、利用実績（見込み含む）の検討に基づき、小改定で対応する。
- 推奨候補暗号リストへの新規暗号（事務局選出）の追加（現時点ではSHA-3を想定）
- 推奨候補暗号リストから電子政府推奨リストへの昇格
- 推奨候補暗号リストからの製品化されていない暗号の削除

以下は、実施方法及び実施時期等の検討に基づき、小改定で対応する。
- 既存の技術分類の修正を伴わない新技術分類の追加（現時点では軽量暗号（公募を含む）を想定）

③随時改定 ： 以下は、安全性の検討に基づき、随時改定で対応する。
- 電子政府推奨暗号リスト及び推奨候補暗号リストからの運用監視暗号リストへの降格（既存システムへの影響調査要）
- 運用監視暗号リストからの危殆化が進んだ暗号の削除（既存システムへの影響調査要）

資料 5

2014 年度 暗号技術評価委員会活動計画(案)

1. 活動目的

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

2. 活動概要

(1) 暗号技術の安全性及び実装に係る監視及び評価

下記の通り、暗号技術の安全性に係る監視・評価 及び 実装に係る技術の監視・評価を実施する。

① CRYPTREC 暗号等の監視

国際会議等で発表される CRYPTREC 暗号リストの安全性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) に関する監視を行う。報告は、なるべく直近の暗号技術評価委員会で報告することを目標とする。

- 引き続き、仕様書の参照先の変更(ECDSA, ECDH)について検討を行う。

② 電子政府推奨暗号リスト及び推奨候補暗号リストからの運用監視暗号リストへの降格及び 運用監視暗号リストからの危殆化が進んだ暗号の削除

CRYPTREC 暗号リストの安全性に係る監視活動を継続的に行い、急速に危殆化が進んだ暗号技術やその予兆のある暗号技術の安全性について評価を行う。また、リストからの降格や削除、注釈の改訂が必要か検討を行う。

③ CRYPTREC 注意喚起レポートの発行

CRYPTREC 暗号リストの安全性及び実装に係る技術の監視活動を通じて、国際会議等で発表された攻撃等の概要や想定される影響範囲、対処方法について早期に公開することが望ましいと判断された場合、注意喚起レポートを発行する。

④ 推奨候補暗号リストへの新規暗号（事務局選出）の追加

標準化動向に鑑み電子政府システム等での利用が見込まれると判断される暗号技術の追加を検討する。

- 現時点ではハッシュ関数 SHA-3 の検討している。NIST の FIPS Draft が公表されてから安全性評価について検討する。

⑤ 既存の技術分類の修正を伴わない新技術分類の追加

暗号技術調査ワーキンググループにて調査を行い、暗号技術評価委員会は、その調査結果に基づき追加方針等について検討を行う。

(2) 新世代暗号に係る調査

- 引き続き、暗号技術調査ワーキンググループ(暗号解析評価)及び暗号技術調査(軽量暗号) ワーキンググループを設置し、下記の内容について検討を行う
- 暗号技術調査ワーキンググループ(暗号解析評価)

  引き続き、

  (i) Shortest Vector Problem (SVP)

  (ii) Learning with Errors (LWE)

  (iii) Learning Parity with Noise (LPN)

  (iv) Approximate Common Divisor (ACD)

  などの数学的問題を利用した公開鍵暗号技術とパラメータ選択に関する検討を行う。
- 暗号技術調査ワーキンググループ(軽量暗号)

  (a) 軽量暗号に関する検討
  - 軽量暗号が既存暗号に対してアドバンテージをもつエリア
  - 軽量暗号で達成すべき安全性

  (b) 軽量暗号技術に関する現状調査 (サーベイ)
  - 認証暗号：CAESAR プロジェクト提案アルゴリズム等から軽量性に優れた方式を調査
  - ハッシュ関数: SHA-3 の調査

  (c) 今後の活動方針に関する検討
  - 暗号技術ガイドライン (軽量暗号の最新動向) の発行、暗号技術ガイドライン (軽量暗号の詳細評価) の発行、軽量暗号に関する技術公募の実施のいずれがよいか検討を行い、暗号技術評価委員会に提言を行う。

(3) 暗号技術の安全な利用方法に関する調査 (技術ガイドラインの整備、学術的な安全性の調査・公表等)

暗号技術を利用する際の技術面での注意点について必要な検討を行う。

- 具体的な内容については、2014 年度第 1 回暗号技術評価委員会にて検討する。

以上

資料６

2014 年度 暗号技術活用委員会活動計画（案）

今後、暗号に関する様々な課題解決に向けた政策立案等を行う際に役立てるために、2014 年度は、2013 年度の活動内容を継続して実施し、各検討項目における最終報告書を取りまとめる。

1. 暗号の普及促進・セキュリティ産業の競争力強化に係る検討

本委員会では、2013 年度と 2014 年度の 2 年間をかけて、「暗号政策上の課題の構造」や「暗号と産業競争力の関連性」などの課題に対する分析を行い、暗号アルゴリズムの普及促進やセキュリティ産業の競争力強化に向けた障壁が何かを明らかにするとともに、その解決策を取りまとめる活動をしている。

2014 年度は、2013 年度に引き続いて、議論を行ううえで有用な基礎データの収集を上期も継続して実施する。下期には、2013 年度及び 2014 年度上期に収集したデータをもとに、暗号の普及促進・セキュリティ産業の競争力強化に向けた具体的な課題分析や解決策の検討を実施し、報告書に取りまとめる。

2. 暗号政策の中長期的視点からの取組の検討

上記の「暗号の普及促進・セキュリティ産業の競争力強化に係る検討」のなかで、様々なシステムを安全に動かしていくための暗号に関連する人材育成についても一緒に検討していくことにより、CRYPTREC として取り組むべき課題を明らかにし、報告書に取りまとめる。

3. 標準化推進

2013 年度の成果を踏まえ、今後、様々な組織が日本からの暗号アルゴリズムの提案を行う場合に、その成果が効果的に得られるようにするための、有望な標準化提案先の選定、当面必要とされる稼働見積もりや交渉方法、提案活動における課題等を、標準化推進 WG にて引き続き検討し、報告書に取りまとめる。

4. 運用ガイドライン作成・公開

2013 年度にドラフト版を完成させた「SSL/TLS サーバ構築ガイドライン」について、引き続き運用ガイドライン WG にて作業を行い、成果物を暗号技術検討会に報告する。

【参考】2014 年度スケジュール（案）

年 3 回の委員会開催を予定する。

以上

参考資料1

２０１３年度　第１回暗号技術検討会　議事概要

１．日時　平成２５年７月５日（金）　１４：００～１５：３５

２．場所　経済産業省本館４階　商情局第１会議室

３．出席者（敬称略）

構成員：今井 秀樹（座長）、岡本 栄司、岡本 龍明、金子 敏信、国分 明男、武市 博明、近澤 武、中山 靖司、松井 充、松尾 真一郎、松本 勉、松本 泰、向山 友也、渡辺　創

オブザーバ：伊藤 毅志、奥山 剛、亀田 繁、木村 和仙、平 和昌、寶木 和夫、西村 敏信

暗号技術評価委員会事務局：盛合 志帆（独立行政法人情報通信研究機構（ＮＩＣＴ））

暗号技術活用委員会事務局：神田 雅透（独立行政法人情報処理推進機構（ＩＰＡ））

暗号技術検討会事務局：

総務省　吉田 靖、山碕 良志、村上 聡、飯田 恭弘、吉田 丈夫、橋本 直樹

経済産業省　富田 健介、上村 昌博、中谷 順一、室井 佳子

４．配布資料

（資料番号）	（資　料　名）
資料１－１	2013 年度　暗号技術検討会開催要綱（案）
資料１－２	暗号技術検討会の公開について（案）
資料２	2012 年度　暗号技術検討会報告書（案）
資料３	暗号技術評価委員会　活動計画（案）
資料４	暗号技術活用委員会　活動計画（案）
資料５	CRYPTREC の暗号アルゴリズム仕様書について
参考資料１	2012 年度　第３回　暗号技術検討会議事概要
参考資料２	今後の検討課題に関する方針
参考資料３	2013 年度　暗号技術検討会及び関連委員会の体制
参考資料４	2013 年度　暗号技術検討会　構成員・オブザーバ名簿

５．議事概要

１　開会

暗号技術検討会事務局から開会の宣言があり、総務省の吉田政策統括官から開会の挨拶。

参考資料４に基づき、構成員及びオブザーバの交代等の説明（辻井 重男顧問が昨年度をもって勇退、上原 哲太郎構成員が新任、持麾構成員→向山構成員、（内閣官房情報セキュリティセンター）三角氏→奥山氏、（総務省）栗原氏→稲垣氏、濱島氏→増田氏、宮地氏→篠原氏、（財務省）石田氏→郷氏、（法務省）河合氏→佐藤氏、（厚生労働省）代田氏→三富氏、（経済産業省）鈴木氏→辻本氏、（独立行政法人情報処理推進機構）笹岡氏→伊藤氏、（公益財産法人金融情報システムセンター）鈴田氏→西村氏）。上原 哲太郎構成員、太田 和夫構成員、佐々木 良一構成員、本間 尚文構成員は欠席。

２　議事

（１）2013 年度 暗号技術検討会開催要綱等について【承認事項】

資料１及び資料１－２に基づき、2013 年度暗号技術検討会開催要綱及び暗号技術検討会の公開について暗号技術検討会事務局から説明。質疑は以下のとおり。原案どおり承認。座長として今井構成員を選任。

○質疑応答

松本（勉）構成員：資料が速やかに公開されることはよいことである。暗号技術評価委員会、暗号技術活用委員会の各委員会の資料等の公開については、各委員会で定めるのか。

暗号技術検討会事務局：各委員会の初回の会合で決定する。

（２）　2012 年度 暗号技術検討会報告書（案）について【承認事項】

資料２に基づき、2012 年度 暗号技術検討会報告書（案）について暗号技術検討会事務局から説明。質疑等なし。原案どおり承認。

（３）　暗号技術評価委員会 活動計画（案）について【承認事項】

資料３に基づき、暗号技術評価委員会 活動計画（案）について暗号技術評価委員会事務局から説明。質疑は以下のとおり。原案どおり承認。

〇質疑応答

今井座長：注意喚起レポートは委員会で審議せずに発出することもあり得るのか。

暗号技術評価委員会事務局：緊急性を要する場合や次の委員会まで時間が空く場合は電子メールによる審議を経て実施する。

松本（勉）構成員：「リストガイド」から「ガイドライン」となった理由は何か。今後はガイドラインに統一するのか。

暗号技術評価委員会事務局：名称には特段の意図はない。今後はガイドラインに統一する。

松本（勉）構成員：「ガイドライン」だと従うべきという義務的なニュアンスがあるように思うが、本質的には問題ない。

寳木オブザーバ：軽量暗号に関して ISO/IEC の動きが進んでいる。ISO/IEC の活動と関連づけるのか。

暗号技術評価委員会事務局：標準化が進んでいた軽量暗号の ISO/IEC の規格は既に出版されており、新しく軽量ハッシュ関数についてのパートが 10 月から ISO/IEC で標準化が始まることになった。次の ISO/IEC の改定の際に提案できればと考えている。

松本（勉）構成員：更に軽量なものも議論の対象とするのか。

暗号技術評価委員会事務局：そういったものも検討に含めたいと考えているが、WG 委員の意見を聞きながら定義について決定したいと考えている。

（４） 暗号技術活用委員会 活動計画（案）について【承認事項】

資料４に基づき、暗号技術活用委員会 活動計画（案）について暗号技術活用委員会事務局から説明。質疑は以下のとおり。

〇活動計画全般について

暗号技術検討会事務局：小改定のスパンを３年としたので、２年間で調査・検討する方針とした。ただし、２年間も要するのでは遅すぎるという意見もあり得るのではないかとも考えるがどうか。

松本（勉）構成員：スピード感が大事であることは同感であるが、課題抽出から対応まで２年ほどを要する課題もあるのではないか。

暗号技術検討会事務局：じっくり検討する必要があるものと、そうではないものがあると思うので、切り分けないとスピード感がなくなるのではないかということを気にしている。

松本（勉）構成員：その通りであり、その点は留意しておく必要がある。

〇運用ガイドラインについて

岡本（栄）構成員：今までに CRYPTREC で行ってきた内容とは大分異なるように感じる。電子政府推奨暗号リストに入っていても推奨されないものが出るのか。

暗号技術活用委員会事務局：例えば SSL のサイファースイートに含まれており、CRYPTREC 暗号リストに掲載されていてもほとんど製品に実装されていない場合は外れる可能性がある。また、暗号を実装するために複雑なコマンドラインを使用しないと実装できないものを外す、あるコマンドラインで実装しようとすると推奨できない組合せが入ってしまったとしても、対処できる場合は運用上の観点から使用する、といったことはありうる。

岡本（栄）構成員：推奨候補暗号リストや運用監視暗号リストから入ることもあるのか。

暗号技術活用委員会事務局：（使用の要件を付した上で）ありうる。

今井座長：こういったものが出てきた理由は IPA のマニュアルが非常に大きなインパクトを与えたことである。CRYPTREC 暗号リストに掲載しただけではなかなか利用されないという現状がある。ある程度現実に妥協する形となるが、安全性はきちんと確保していくものである。

岡本（栄）構成員：CRYPTREC の活動と分けないと整合性がとれないのではないか。

松本（勉）構成員：一方で、運用ガイドラインが CRYPTREC の活動とリンクしていないと、利用者から見るとばらばらに見えてしまい困るのではないか。したがって CRYPTREC の枠内で行い、しっかりと内容を見ていく方がよいのではないか。

今井座長：電子政府推奨暗号リストの活用を推進するという意味では、こういった方法もあり得るのではないか。まず CRYPTREC の傘の下で実施してみて、その中身を検討会でも確認する方法が良いと思う。その上で議論すれば良いのではないか。ところで、この運用ガイドラインの作成作業での成果について、電子政府推奨暗号リストへのフィードバックは行うのか。

暗号技術活用委員会事務局：対象を SSL/TLS 等に限定することを考えていたため、フィードバックはまでは想定していない。

金子構成員：「運用ガイドライン」という名称が良くない。「SSL/TLS 運用ガイドライン」と限定したらどうか。また、技術ガイドラインと運用

ガイドラインの違いも分かりにくい。さらにベースラインとレッドラインという２つの概念が登場しており、説明を難しくしている。

暗号技術活用委員会事務局：ベースラインとレッドラインは同じ意味で使用している。

暗号技術検討会事務局：事務局内でもガイドラインの違いについて議論があった。今後の進め方としては、両委員会で作成したガイドラインは、相互に関連することから、事前に両委員会で案を作った段階でそれぞれの認識と合致することを確かめながら進め、今井座長のご発言のとおり出来上がったものを CRYPTREC のクレジットで出すべきかどうかについて、この検討会で確認していただく必要があると考えている。

岡本（栄）構成員：SSL/TLS といった限定があるならば、向いていないものがあることも分かるが、やはりリスト上で推奨暗号ではない暗号を、運用ガイドライン上では推奨する可能性があるということに違和感がある。

岡本（龍）構成員：このガイドラインは電子政府を対象としていると考えて良いか。つまり、民生品は対象外と考えて良いか。

暗号技術検討会事務局：そのとおりである。ただ、民間においても参照されればなお良いと考えている。

今井座長：様々な意見があると思うので、この場で言い切れなかった意見は事務局あてメール頂きたい。最終的な判断は座長に一任して頂きたいが、ガイドラインについては、この検討会でチェックする機会は必ず設けるようにする。

（５） CRYPTREC の暗号アルゴリズム仕様書について【承認事項】

資料５に基づき、CRYPTREC の暗号アルゴリズム仕様書の更新について暗号技術評価委員会事務局から説明。以下の質疑を踏まえて軽微な修正を行うこととなるが、ほぼ原案どおり承認。

〇質疑応答

金子構成員：KCipher-2 に日付がついていないのはなぜか。

暗号技術評価委員会事務局：公募提案時に入手した仕様書にリンクさせているため、そのままの名称となっている。

金子構成員：日付は必要ではないのか。

暗号技術評価委員会事務局：入れるようにしたい。

松本（勉）構成員：仕様書がいつの時点のものなのかが分かることが重要であるため、その他の仕様書についても日付を入れるようにすべきではないか。

暗号技術評価委員会事務局：整理して一意に特定できるようにしたい。

松本（勉）構成員：また、リストの改正を踏まえ、JCMVP の方で CRYPTREC の仕様書を改めて引用したいと思ったが、更新されておらず困っているとも聞いている。この仕様書の更新について、対処する必要があるだろう。

暗号技術評価委員会事務局：できれば正式に JCMVP の方から要望の文書が欲しい。

松本（勉）構成員：了解した。仕様書の更新についてのルールを作成することも近々の課題となるだろう。

金子構成員：資料４の４ページ中に、「トレードマーク」とカタカナで書かれている部分があるが、これは正しいのか。

暗号技術評価委員会事務局：RSA 社からの提出された文章のまま引用しているが、確認する。

３　閉会

経済産業省の富田商務情報政策局局長から閉会の挨拶。

暗号技術検討会事務局から、次回暗号技術検討会の時期、場所等の詳細については、別途連絡する旨が説明された。

以上

参考資料２

「CRYPTREC 暗号技術ガイドライン (SSL/TLS における近年の攻撃への対応)」

2014.03.25 版

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

目次

1. 序章

1.1 本ガイドラインの目的

SSL/TLS の運用について、近年、プロトコルの仕組みの脆弱性やソフトウェアの脆弱性を複合的に利用する攻撃がいくつか公開されている。また、プロトコル内で用いる暗号として RC4 を選択することができるが、運用監視暗号リストに位置づけられており、安全性に係る問題のある暗号技術として、互換性維持以外の目的での利用が推奨されていない。さらに、RC4 に対する攻撃が適用できる環境下では SSL/TLS の安全性が保てなくなることが示されている。このような状況を踏まえ、本ガイドラインでは、それら近年示されている攻撃の解説を行うとともに、SSL/TLS を安全に利用するため近年注目されている攻撃に対して推奨される対応を示すことを目的としている。

本文では、プロトコルの仕組みを利用した攻撃として、BEAST、TIME、CRIME、Lucky Thirteen などについて解説するとともに推奨される対応策を示す。また、プロトコル内で用いる暗号として RC4 を用いた場合の実際の攻撃方法、事例を示す。この場合は攻撃を回避する効果的な対応策がないため、RC4 を選択しない利用方法の推奨などを述べている。

1.2 総論

SSL/TLS に関して、 (1) プロトコルの仕組みを利用した攻撃に起因する脆弱性と、 (2) プロトコル内で用いる暗号として RC4 を用いた場合に、RC4 のアルゴリズムの弱さに起因する脆弱性とが指摘されている。

(1) に分類される脆弱性：BEAST は、プロトコルで CBC モードを用いた場合に CBC モードの脆弱性として知られる特性を利用した攻撃である。具体的には、特定のブロックの平文を意図した値に差し替えられる攻撃者が、別のブロックの解読が容易になるという脆弱な性質を利用しており、 SSL/TLS のプロトコルの仕様との複合的事象として、Java アプレット実行環境が脆弱なブラウザにおいて攻撃が発生することが指摘されている。ただし、プロトコルそのものを変更しなくても平文を 1 対 (N-1) の分割を行うことで回避できる可能性が示されている。また、Java アプレットのパッチを当てることでも回避することができるとされている。これらの状況から、この攻撃をもって、 SSL/TLS において、ブロック暗号を利用しないという結論には至らない。 CRIME、TIME、BREACH、Lucky Thirteen は、圧縮データのサイズの差異や、実行時間の差異を利用して暗号解読の攻撃を行う、いわゆる実装攻撃に属する攻撃であるが、これらの攻撃は、一般の実装攻撃への対策と同様の考え方で、圧縮機能の無効化、データや実行時間の平準化やランダム化などの回避策が示されている。その他、圧縮機能を無効化せずに，回避する方法も検討されはじめている。 これらの攻撃を鑑みても SSL/TLS において、ブロック暗号を利用しないという結論には至らない。

(2) に分類される脆弱性： RC4 は、同じデータに対して異なる鍵を用いて生成された暗

号文を複数入手できる Broadcast Setting や同じデータをセッションごとに同じ位置で、異なる鍵で暗号化して送信する Multi-Session Setting の環境が攻撃者に与えられた場合、効率的に攻撃が実現できることが知られている。 SSL/TLS で用いる暗号として RC4 を選択した場合、攻撃者に効率的に RC4 に対する攻撃が適用できる環境を提供してしまうことになる。近年の解析結果では、現実的なコスト、および起こりうる確率で平文が回復できることが示されている。(一例としては、同じメッセージに対して 2^{34} の暗号文が集められた場合、メッセージの先頭から約 1000 T byte を非常に高い確率（0.97）で復元可能であることが示されている［1]）。RC4 の攻撃を適用できる環境として利用されている Broadcast Setting は、BEAST、TIME、CRIME 等の攻撃の中でも利用されており、この攻撃のみで想定している特殊な環境ではない。また、 HTTPS + basic 認証(例：ネットワーク利用者認証、グループ利用の Web ページ）を利用する際に攻撃者に繰り返し re-negotiation をさせられてしまう場合や JavaScript のバグを攻撃者が悪用し、攻撃者のサーバに大量の暗号文を送らされてしまう場合等には、比較的容易に整えられる環境であり、PC 版の Internet Explorer、 Firefox、 Opera、 Safari などのブラウザに対してブロードキャスト状態にするのは十分に実行可能な設定条件であるといえる。ゆえに、RC4 を用いた場合の解析結果は現実的な脅威として配慮すべきである。

SSL/TLS にはいくつかのバージョンが存在する。推奨される設定として、TLS 1.0 より古いバージョンについては、新しいバージョンへアップデートすることが推奨される。TLS 1.0 については、CBC モードを用いた場合の脆弱性がに対してパッチが充てられているため、Java 等のソフトウェアを最新版に更新した上で、CBC モードを選択することが推奨される。TLS 1.1 については、CBC モードを用いた場合の脆弱性が解消されていることから、CBC モードを選択することが推奨される。TLS1.2 については、CBC モード、CCM モード、GCM モードがある為、それらを使うことが推奨される。

1.3 本ガイドラインの構成

2 章に、本文中で取り扱っている技術説明/用語説明を記している。3 章に、プロトコルの仕組みを利用した攻撃を記している。4 章に、RC4 の脆弱性に基づく攻撃を記している。

1.4 注意事項

本ガイドラインは状況の変化に伴い、改訂される場合がある。

2. 技術説明 / 用語説明

SSL/TLS

SSL（Secure Socket Layer）、TLS（Transport Layer Security）は、ネットワーク上のアプリケーションに対して通信相手の認証と暗号化された通信を提供するプロトコル。SSL は Netscape Communications 社が開発し、その仕様を引き継ぐ形で IETF において TLS として標準化されている。

https

アプリケーションにおいて、SSL/TLS を用いて通信を行う際に使われる URI のスキームのこと。

Deflate

可逆データ圧縮アルゴリズムである。SSL などのプロトコル内の圧縮で使われるケースでは 16KB ごとの境界が存在するため、攻撃対象の Cookie の値がちょうどこの境界上に来るようにパディングのサイズを調節することによる 1 バイトずつのブルートフォース攻撃などに利用される。

Cookie

HTTP プロトコルで通信する、ウェブブラウザとウェブクライアントの間で、主に状態管理のために情報を保存するために使われるプロトコル、およびこのプロトコルによって保存される情報そのもの。

3. プロトコルの仕組みを利用した攻撃

3.1 CBC モードの構成を利用した攻撃：BEAST [2]

BEAST は 2011 年に開発された攻撃ツールであり、SSL3.0/TLS1.0 の CBC モードの脆弱性を利用して選択平文攻撃を行い、Cookie（平文）を得る。BEAST の概要は公開されているが、ツールは非公開のため、詳細については不明な部分が多く、以降の説明には一部推測が含まれる。

まず、図 1 に、SSL3.0/TLS1.0 における CBC モードの処理概要を示す。

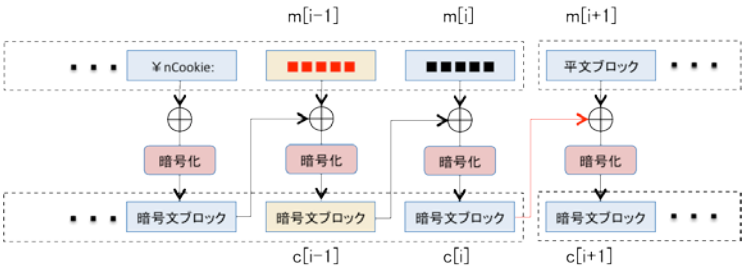


図 1　SSL3.0/TLS1.0 における CBC の概要

ここでのポイントは、初期化ベクトルとして直前の最終暗号文ブロック c[i] を使用している点である。これにより、一つ前の平文ブロック m[i-1]（Cookie に対応）に対して以下の選択平文攻撃が可能となる。

1. 攻撃者は平文 m[i-1] の推測 M[i-1] を生成
2. 次の平文の最初のブロックとして M[i+1]=M[i-1] XOR c[i-1] XOR c[i] を設定
3. 対応する暗号文 C[i+1] と c[i-1] を比較
4. 異なっていれば、1 からやり直し、なお、

C[i+1]=E(M[i+1] XOR c[i])
=E(M[i-1] XOR c[i-1])
=E(m[i-1] XOR c[i-1]), if M[i-1]=m[i-1]
=c[i-1]

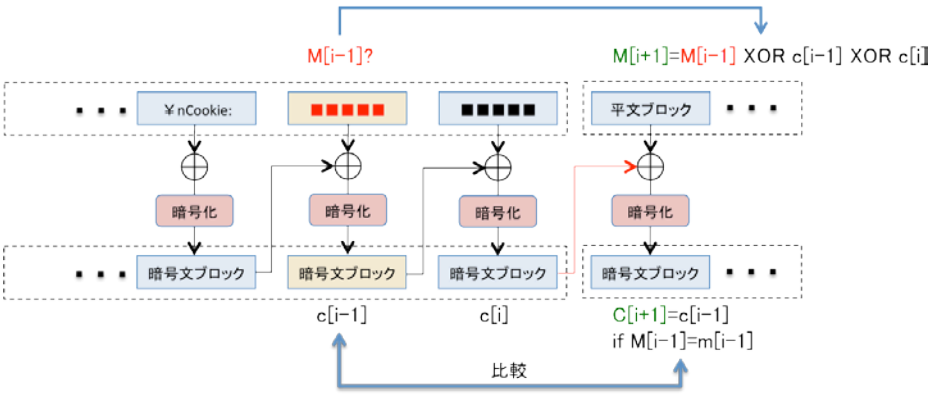


図 2　SSL3.0/TLS1.0 への平文選択攻撃

図 2 の攻撃では、平文ブロックをブロック全体で全数探索しており、特定に（最大）2^{128} 回の平文選択が必要となり脅威は小さい。

それに対して BEAST では攻撃の効率向上のため、ブロック単位ではなくバイト単位で全数探索することで、特定に必要な平文選択を $2^8 \times 16$ と大幅に削減した。具体的には、アクセス先の URL を変更し、図 3 に示すように Cookie の 1 バイト目が平文ブロックの最後となるようにした上で、選択平文攻撃でこの 1 バイトを特定する。そしてさらに、URL を 1 バイト短くすることで、Cookie の 2 バイト目がブロックの最後となるようにし、同様に処理を繰り返し、バイト単位で特定する。これにより、攻撃の効率が飛躍的に向上し、実際に適用可能となった。

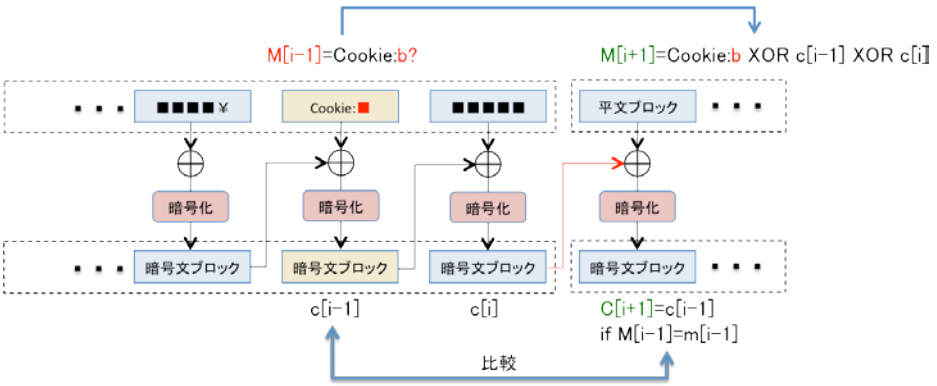


図 3　BEAST におけるバイト単位の平文選択攻撃

BEAST への対策には、TLS1.0 で実施可能な対策と、TLS1.1 以降への移行で実施可能となる対策の 2 種類がある。前者の対策として、セキュリティパッチの適用が挙げられる。現時点のセキュリティパッチ [3]（1/n-1 レコード分割，1/n-1 Record Splitting Patch と呼ばれる）については、その安全性が [4]で評価されており、ある条件下で BEAST 系の平文選択攻撃に対して識別不能性を満たすことが証明されている。ここで条件には、CBC モードでの暗号化の前に平文に付け加えられる MAC（後述の 3.3 節の図 6 参照）の長さがブロ

ック長より短いことが含まれる。よって、ブロック長より長い MAC を生成する Truncated HMAC（RFC6066 [5]）を使う場合には、必ずしも安全性が保証されるわけでは無いため、注意が必要である。一方、後者の TLS1.1 以降で実施可能な対策として、改良された CBC モード（初期化ベクトルに直前のブロックは使わず、リフレッシュする）の使用が挙げられ、さらに TLS1.2 以降であれば、新たに追加された認証付き暗号利用モード(GCM モード、CCM モード)の使用も対策となる。なお、BEAST のデモでは、実装に Java アプレットが使用されているが、その理由は Java アプレットの脆弱性を使用するためと言われている。よって、上述のいずれの対策でも、Java を最新に保つことが不可欠となる。

短期的な対策として共通鍵ブロック暗号の代わりにストリーム暗号 RC4 を使うことが挙げられるが、RC4 の脆弱性が数多く報告されており、長期的な対策としては推奨できない。

3.2 圧縮処理部分の観測に基づく攻撃

3.2.1 CRIME [6]

CRIME（Compression Ratio Info-Leak Mass Exploitation）は、2012 年の Ekoparty において、Rizzo と Duong によって発表された攻撃である。SSL/TLS において、入力データに対する圧縮後のパケット長の違いから平文である Cookie を解読する攻撃である。一般的にデータ圧縮の技術では、頻度が高いデータが多いほど圧縮後のデータ長は短くなる。この性質を利用し、圧縮後のメッセージの長さを参照しながら解読を行う。解読の例を図 4 に示す。

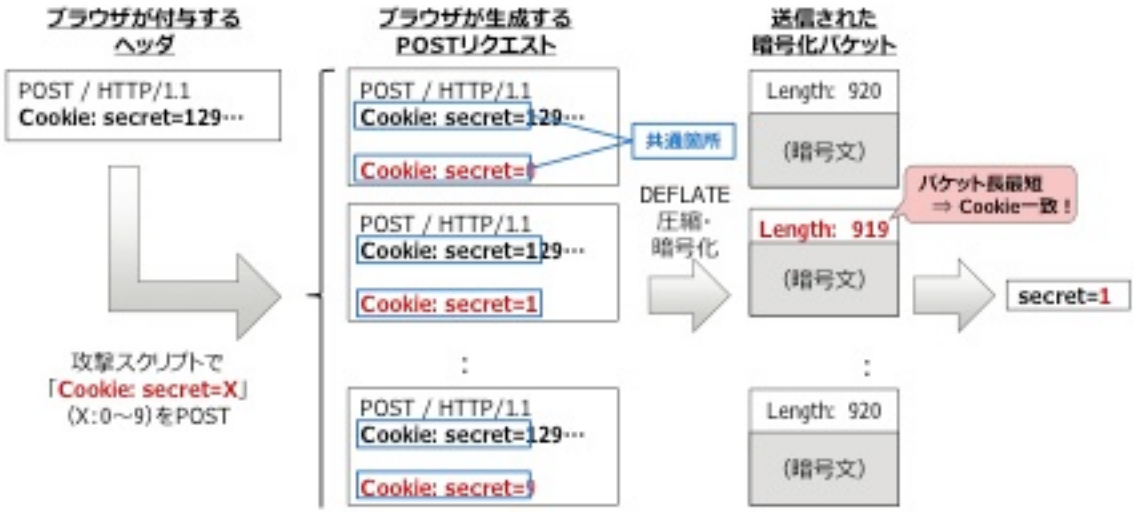


図 4 CRIME の攻撃の流れ

この例では、 Cookie の中に、Secret という属性値がセットされているが、攻撃スクリプトを利用し、secret=X という形で X を 0 から 9 に変化させたデータを SSL/TLS のデー

タとして送る。その結果として圧縮されたデータのパケット長から、secret の値を類推することができる。

この攻撃は、SSL/TLS において使われているデータ圧縮の機能に依存するものであり、SSL/TLS の圧縮機能を使わないことで対応できる。Web ブラウザの Internet Exploler ではもともと圧縮機能に対応していなかったため本攻撃は適用が出来なかった。また、Google Chrome ではバージョン 21.0.1180.89、Firefox ではバージョン 15.0.1、Opera では 12.01、Safari ではバージョン 5.1.7（Windows）5.1.6（MacOS）で圧縮機能が無効化されており、これら以降のバージョンでは本攻撃の影響はない。

また、 Web サーバソフトウエアの Apache2.2 with MOD_SSL ではデフォルトで圧縮機能を利用しており機能の無効化の設定はないが、 Apache2.4 with MOD_SSL ではデフォルトで圧縮機能を利用しているものの無効化も可能となっている。また、 IIS ではもともとすべてのバージョンで圧縮機能が存在せず、 AMAZON ELASTIC LOAD BLANCERS ではデフォルトで圧縮機能は無効となっている。

3.2.2 TIME [7]

TIME（Time Info-leak Made Easy） は 2013 年に Liu らによって発表された攻撃で、CRIME と同様に、 SSL/TLS の圧縮機能を用いて Cookie などの値を解読する攻撃である。 図 5 に攻撃の流れを示す。 CRIME がデータ長を推定に利用したことに対して、TIME ではブラウザにおいての処理時間の差によって攻撃に必要な情報を収集するため、攻撃者による中間者攻撃が必要であった CRIME に比べて、攻撃の実現性が高いことが特徴である。TIME では、HTTP レスポンスの圧縮結果を用いていることが攻撃の原因となっており、圧縮機能の無効化が攻撃を回避する有効な方法である。しかし、現実のアプリケーションにおいては性能上要件により圧縮機能の無効化が受け入れられない場合があり、このような場合においては HTTP レスポンスの圧縮を無効化という対策を講じることは難しいのが現状である。

図 5 TIME の攻撃の流れ

3.2.3 BREACH [8]

BREACH は、2013 年に行われた BlackHat において Prado らによって発表された攻撃である。基本的な考え方は、 CRIME と同様に HTTP リクエストメッセージをコントロールして、圧縮データのデータ長の違いにより暗号文を解読する攻撃である。 CRIME との違いは、 http レスポンスに含まれる情報を奪うことと、 SSL/TLS のデータ圧縮機能を用いるのではなく、アプリケーション層における圧縮機能、例えば Web アプリケーションによる gzip を用いた圧縮においても攻撃が成功するため、SSL/TLS の設定変更では対策にならないという点である。一方で、攻撃成功の条件は限定的であり、 gzip 圧縮の他に、レスポンスの平文にリクエストの情報そのものと、レスポンス自体に CRSF Token などの秘密情報が含まれることが必要である。前述の通り、SSL/TLS の設定変更では対処できないため、 SSL/TLS を用いるアプリケーションでの対応が必要となる。

3.3 MAC-then-Encryption の構成を利用した攻撃：Lucky Thirteen [9]

Lucky Thirteen は 2013 年に発見された TLS が使用する HMAC 付き CBC モード(MAC-then-Encrypt、以下 MEE-CBC-TLS) の脆弱性を利用した中間者攻撃であり [9]、攻撃者は復号処理の処理時間差(ハッシュ関数の計算回数の違い)を特定することで平文を得る。 図 6 に、TLS における MEE-CBC-TLS の処理概要を示す。

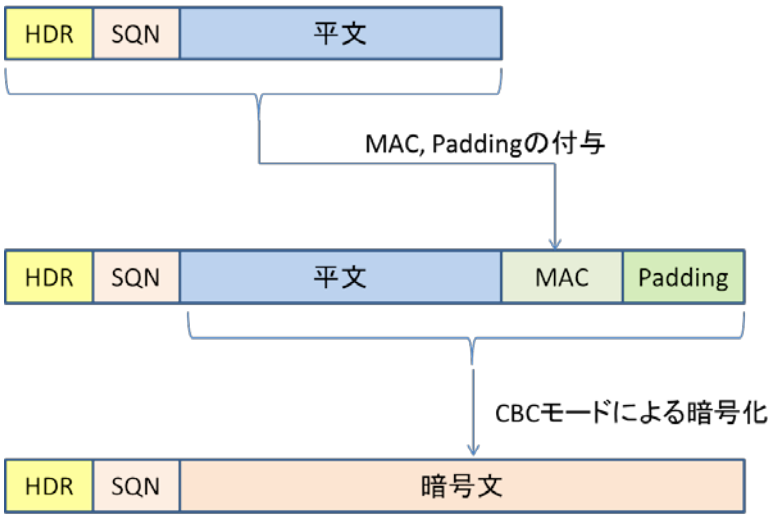


図 6 TLS における MEE-CBC-TLS の概要

ここで MAC の生成に HMAC-SHA1 を用いる場合、ハッシュ対象のデータ長により MAC の生成に用いる SHA-1 の実行回数が異なることが知られている。 SHA-1 の処理回数は[((64+M) +1+8)/64]で表現されるため、具体的には M mod 64 が 55 か 56 になるかで SHA-1 実行回数が変化する。

実際の攻撃は次の通りである。

1. 暗号文を入手する
2. MAC エラーが発生するような攻撃用の暗号文を用意し、サーバに送付する
3. 意図的に MAC エラーを発生させ、エラー発生のタイミング（SHA-1 実行回数の変化）から平文を得る
4. エラー発生箇所を変更し、2、3 を繰り返す

図 6 に示す通り、MAC の対象は平文にヘッダ（HDR）5 byte とシーケンス番号（SQN）8 byte の合計 13 byte を加えたデータとなるため、この 13 byte を加えた平文ブロックのデータ長を変化させる。

また、実際に攻撃を行うためには、攻撃者はネットワーク越しに MEE-CBC-TLS 復号の処理時間差を厳密に測定する必要があるため、実際に攻撃を適用することは難しい。Lucky Thirteen の提案者は、 OpenSSL 及び GnuTLS を使用しているサーバに対して同一セグメント内からの攻撃に成功した実験結果を示している。

Lucky Thirteen に対する対策としては、認証付き暗号利用モード(GCM モード、CCM モード）を利用することである。これは TLS 1.2 以降でサポートされている。

3.4 Renegotiation を利用した攻撃

3.4.1 攻撃方法

Renegotiation を利用した攻撃とは、2009 年に発見された SSL/TLS のハンドシェイクにおいて確立された暗号アルゴリズムと鍵長を更新(Renegotiation)する際の脆弱性を利用した中間者攻撃である [10]。

Renegotiation は、SSL/TLS が確立され暗号通信を行っているセッションを更新して、新たにセッションを確立させる手法である。Renegotiation の概要を図 7 に示す。なお、---は平文データ、===は暗号化データを示す。

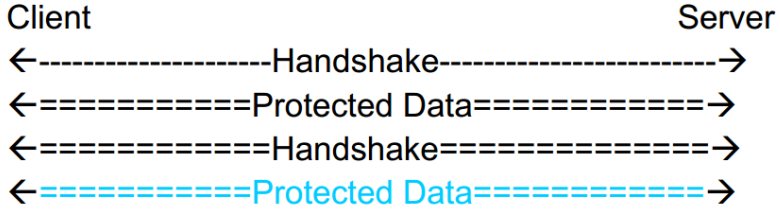


図 7 Renegotiation の概要（[11]より引用）

1. 実際の攻撃は次の通りである。攻撃者はクライアントのハンドシェイクを受信し、パケットを保持しておく
2. 攻撃者とサーバの間で通常のハンドシェイクを行い、サーバと暗号通信を行う
3. 攻撃者は Renegotiation を要求し、クライアントとサーバの間でのハンドシェイクに対して、1 で保持していたパケットをサーバに送信する

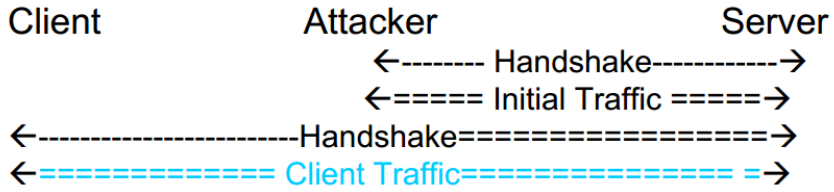


図 8 Renegotiation 攻撃の概要（[11]より引用）

図 8 に示すように、renegotiation されたデータは暗号化されているため、攻撃者が内容を参照することはできないが、サーバはクライアントからのパケットと攻撃者からのパケットを区別することができない。具体的な攻撃としては、サーバ認証のハンドシェイクをクライアント認証(相互認証)に切り替える例が考えられている。

3.4.2 対策方法：RFC5746

Renegotiation の対策として RFC5746 が提案されている。 RFC5746 では TLS 1.2 で定義されている TLS connection state に対して、secure_renegotiation フラグの追加と、client_verity_data と server_verify_data が追加されている。

追加された内容の詳細は次の通りである。これにより、 Renegotiation を安全に行う実装がなされていることをサーバとクライアントの間で共有することが可能となる。

① secure_renegotiation フラグ：セキュアな Renegotiation が使用されているかを示す
② client_verity_data：直前のハンドシェイクにおいてクライアントから送信された Finished メッセージ
③ server_verify_data：直前のハンドシェイクにおいてサーバから送信された Finished メッセージ

また、 SSLv3、 TLS 1.0/TLS 1.1 に対して本対策は適用できないため、 RFC5746 では Cipher Suite に TLS_EMPTY_RENEGOTIATION_INFO_SCSV を追加することでハンドシェイクを中断する方法も提案されている。

なお、これらの実装が行われていない Renegotiation が行われた場合に、正しい相手からのリクエストであるかを安全に確認する手段がないため、この実装が行われていない Renegotiation を拒否することが推奨されている。

4. RC4 の脆弱性に基づく攻撃

4.1 RC4 に対する攻撃

本節では、ストリーム暗号 RC4 において現在までに指摘されている脆弱性について示す。

RC4 は、1987 年に Ronald Rivest によって開発されたストリーム暗号である。1 バイトから 256 バイトの鍵から、鍵スケジューリングアルゴリズム（KSA）により 256 バイトの内部状態を作り出し、内部状態からキーストリーム生成アルゴリズムにより 1 バイト単位のキーストリームを出力する。内部の処理はバイト単位であり、鍵は 1 バイトから 256 バイトの可変長（推奨値は 16 バイト）、内部状態は 256 バイトの配列と、2 つのインデックスからなる。

ストリーム暗号の安全性評価としては、以下の 4 つの攻撃を想定する。

1) 鍵回復攻撃:出力されたキーストリームから、ストリーム暗号に対する入力鍵(の一部)を求める攻撃
2) 内部状態復元攻撃：出力されたキーストリームから、内部状態を推定する攻撃
3) 出力予測攻撃：出力されたキーストリームから、将来出力されるキーストリームを予測する攻撃
4) 識別攻撃：出力されたキーストリームと真性乱数を 1/2 以上の無視できない確率で識別する攻撃

これらの攻撃に対し、それぞれ、入力の鍵長を x とした場合、2^x 以下の計算量で推定ができれば攻撃成功となる

鍵回復攻撃においては、入力の鍵長を推奨値である 128 ビットにした場合、FSE2013 において発表された Sepehrdad らの攻撃により無線 LAN の暗号・認証プロトコルである WEP において、19,800 パケットを収集することで鍵回復攻撃が成立することが示されている。また、弱鍵の性質を用いる Weak Key Attack については、長尾らの攻撃 [12] [13] により、$2^{96.36}$ の計算量、$2^{-18.75}$ の確率で鍵回復攻撃が成立することが示されている。

内部状態回復攻撃においては、 CRYPTO2008 における Maximov らの発表により、2^{241} の計算量で内部状態の復元を行うことが示されている。このため、 RC4 においては、鍵長を 241 ビットよりも長くしても安全性は向上しないことが示されている。

出力予測攻撃においては、 EUROCRYPT2005 の Mantin らの攻撃により、2^{45} バイトのキーストリームから、85%の確率で 1 ビットの出力を予測できることが示されている。

識別攻撃においては、同じく EUROCRYPT2005 の Mantin らの攻撃により、$2^{26.5}$ バイトのキーストリームを用いることで、真性乱数との識別ができることが示されている。また、複数の鍵を用いた場合、 FSE2001 の Mantin らの攻撃により、2^8 バイトのキーストリームを用いることで真性乱数との識別ができることが示されている。このような攻撃

は、4.2 に示すように攻撃環境が整った場合には、RC4 に対する攻撃を適用することにより SSL/TLS のメッセージに対する平文回復攻撃が可能となることが示されている。

4.2 RC4 の攻撃を SSL/TLS に適用した場合の攻撃事例

4.1. に記載のとおり RC4 のアルゴリズム自体の脆弱性は多く示されている。SSL/TLS の中で RC4 を選択した場合、その脆弱性を利用した攻撃が示されている。RC4 の攻撃が適用できる条件として、同じデータに対して異なる鍵を用いて生成された暗号文を複数入手できるような環境下を想定している。そのような環境は比較的容易に得られることが出来る。一例として、図 9 に示すような Broadcast Setting と呼ばれる環境が相当する。Broadcast Setting は、複数のユーザが同じファイルを取得する場合や同じファイル(=平文) を繰り返し送信するような場合に得られる環境である。例えば、ネットワーク利用者の認証やグループ利用の Web ページへのログインなどのように、https の中で basic 認証を行うケースなどで Broadcast Setting の環境は整えることができてしまう。また、OS イメージの配布などの場合でも、Broadcast Setting の環境は準備可能である。その他、図 10 に示す Multi-Session Setting と呼ばれる SSL/TLS で通信を行う際に異なるセッションで同じデータを同じポジションで送信する場合(攻撃対象となるデータ以外の平文は毎回任意のデータで構わない)なども RC4 の攻撃が適用できる条件を満たす。この場合、攻撃対象となるのは、例えば cookie やパスワードといった情報になる。このように RC4 の攻撃が適用できる条件は特殊な利用環境というわけではなく、一般的に存在しうる環境であるといえる。

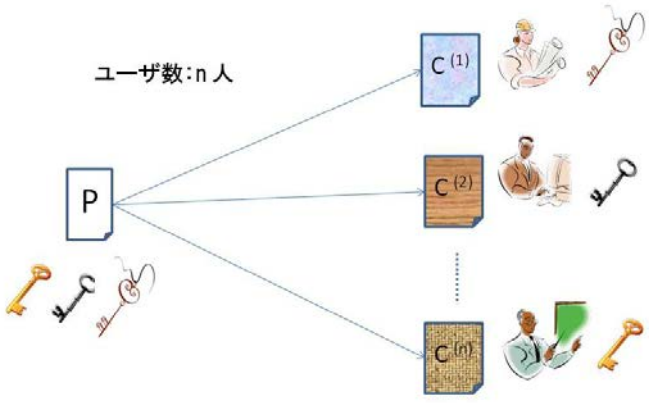


図 9 Broadcast Setting

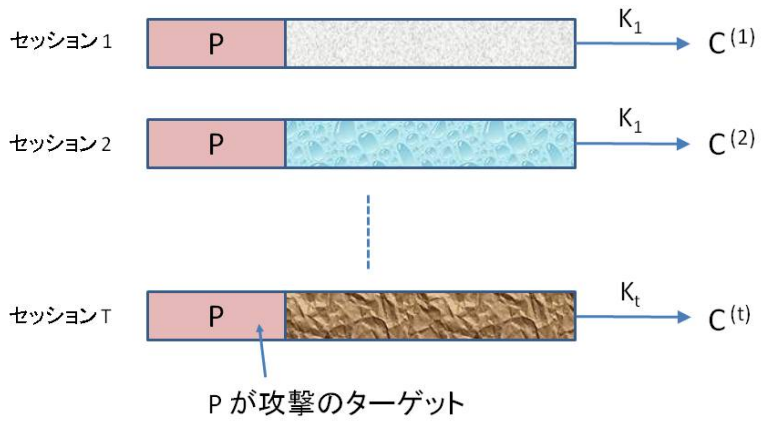


図 10　Multi-Session Setting

近年の結果として [1] [14] では、RC4 の解析を行いキーストリームにおける新しい bias が発見され、それが解析に有効であることを具体的に示されており、RC4 の攻撃が適用できる環境下で、先頭 1000 T バイトの平文を 2^{34} 個の暗号文から 0.97 以上の確率で復元できてしまうことが示されている。さらに [15]では、平文となり得る候補が絞れる場合は、より効率的に解析が行えることが示されている。例えば，平文が PIN code などの場合、入力に使われる文字の種類は 10 種類に限られる。この場合、平文の先頭 257 バイトを 2^{23} の暗号文からランダムに推定する場合よりも高い確率で平文を回復することができる。SSL/TLS の場合、先頭 36 バイトはセッションごとに変化するため、RC4 の解析により、先頭 257 バイトのうち 221 バイトが復元可能となり、入力の種類が限られる場合、より現実的な脅威となることが示されている。

RC4 の攻撃に関しては、 [16] にまとめられている。近年示された強力な攻撃の結果としては、2^{32} の暗号文が集まれば平文の初期 257 byte の任意 byte を確率 0.5 以上で推定が可能であることが示されている [1] [14]。この結果を鑑みても、SSL/TLS で RC4 を用いる場合のリスクがより高くなっているといえる。

[1] [14] などで示されている解析は、RC4 のキーストリームの先頭の n バイト（推奨 n = 768、理想的には n = 3072）を捨てることにより回避することができる。しかしこのような対応をした場合であっても、回避できない攻撃があることが [17] により示されている。具体的には平文の一部(連続した 6 バイト程度) が知られてしまっている場合、同じ平文に対して 2^{34} の暗号文が集められてしまうと，連続した 1 ペタバイトの平文が 0.6 以上の確率で復元されてしまう．また、平文の情報が一切知られていない場合であっても、同じ平

文に対して 2^{35} の暗号文が集められてしまうと，平文のどの位置であっても 1 に近い確率で復元されてしまうことが示されている。

また、 [18] では基本的な攻撃方針としては [1] と同様の手法を用い、成功確率を上げるための最適化を施した解析結果を示している。 具体的には、Broadcast セッティングが実現できるいくつかの具体的な事例を実際に実装し SSL/TLS で RC4 を用いることが現実的な脅威になりうることを示している。事例 1) Java スクリプトの脆弱性を利用し、不正な JavaScript をユーザに使わせることにより、その Java スクリプトを使って大量のターゲットメッセージの Cookie を暗号化して送信させることにより、Broadcast セッティングの環境を実現させる。この不正な Java スクリプトを用いた Broadcast セッティングは、具体的には攻撃者の Web サイトから Java スクリプトマルウェア をダウンロードさせ、その上で https リクエストを大量にリモートサーバに送らせることにより実現できる。事例 2) IMAP(Internet Message Access Protocol；メールサーバ上の電子メールにアクセスし操作するためのプロトコル) で送られるパスワードをターゲットとし、IMAP サーバにアクセスする際に暗号化されたパスワードが送られる仕組みに着目し、暗号化されたパスワードが送られた後に TCP コネクションをリセットし、暗号化されたパスワードを繰り返し送らせることにより Broadcast セッティングを実現させている。具体的に示されている結果として、先頭 256 バイトの bias を実験的に調べ、同じ平文に対して 2^{26} の暗号文を集められると毎回変化する 36 バイトを除いた 40 バイト が 0.5 以上の確率で復元されてしまうことが示されている。 また、同じ平文に対して 2^{32} の暗号文を集められると毎回変化する 36 バイトを除いた 220 バイト が 0.96 以上の確率で復元されてしまうことが示されている。また、ターゲットとなる平文の直前の平文が知られている場合、そのターゲットとなっている平文について、$16 \cdot 2^{30}$ の暗号文を集められるとおおよそ 1 の確率で復元されてしまうことが示されている。

このように、RC4 の攻撃が適用できる条件が整う環境下では、RC4 のアルゴリズムの攻撃は現実的に実現し得るものであり、攻撃者は暗号文を集めれば攻撃を試みることができてしまう。3 章に示された数々の攻撃に対してはそれらを防止する対処策を施すことができる一方、 RC4 の攻撃は対処策がないため、SSL/TLS を運用する選択肢として、RC4 を用いることは、現実的な脅威を招く原因となり得る。

引用文献

[1] T. Isobe, T. Ohigashi, Y. Watanabe, M. Morii, “Full Plaintext Recovery Attack on Broadcast RC4,” FSE, ., 2013.

[2] J. Rizzo and T. Duong, "BEAST: Surprising Crypto Attack against HTTPS, " http://www.ekoparty.org/eng/2011/thai-duong.php.: ekoparty, 2011.

[3] “Bug 665814,” [Online]. Available: https://bugzilla.mozilla.org/show_bug.cgi?id=665814#c59.

[4] 黒川 貴司, 野島 良, 盛合 志帆, “TLS1.0 における CBC モードの安全性について,” 第 31 回暗号と情報セキュリティシンポジウム (SCIS2014), 2014.

[5] “Transport Layer Security (TLS) Extensions: Extension Definitions.,” [Online]. Available: http://tools.ietf.org/ html/rfc6066..

[6] J. Rizzo and T. Duong, “The CRIME Attack,” ekopary, 2012.

[7] T. Be'ery and A. Shulman, “A Perfec Crime? Only TIME Will Tell,” BlackHat, 2013.

[8] Y. Glick, N. Harris and A. Prado, “BREACH: REVIVING THE CRIME ATTACK,” BlackHat, 2013.

[9] N.J. AlFardan and K.G. Paterson, “Lucky Thirteen: Breaking the TLS and DTLS," IEEE Security&Privacy, 2013.

[10] “JVNVU#120541:SSL および TLS プロトコルに脆弱性,” 11 2009. Available: http://jvn.jp/cert/JVNVU120541/.

[11] S. Joe, R. Eric, “TLS Renegotiation Vulnerability,”. Available: http://tools.ietf.org/agenda/76/slides/tls-7.pdf.

[12] A. Nagano, T. Ohigashi, T. Isobe , M. Morii, “New Classes of Weak Keys on RC4 using Predictive State,” Computer Security Symposium 2012 (CSS2012), 2012.

[13] A. Nagano, T. Ohigashi, T. Isobe, M. Morii, “Expanding Weak-Key Space of RC4,” 2013 年暗号と情報セキュリティシンポジウム(SCIS2013), 2013.

[14] T. Isobe, T. Ohigashi, Y. Watanabe and M. Morii, “Comprehensive Analysis of Initial Keystream Biases of RC4,” IEICE Trans. on Fundamentals of Electronics, Comm. and Computer Sciences, 2014.

[15] Y. Watanabe, T. Isobe, T. Ohigashi , M. Morii, “Vulnerability of RC4 in SSL/TLS,” 情報通信システムセキュリティ(ICSS)研究会, ., 2013.

[16] CRYPTREC, “「CRYPTREC Report 2012 暗号方式委員会報告書」,” 2012.

[17] T. Ohigashi, T. Isobe, Y. Watanabe, M. Morii, “How to Recover Any Byte of

Plaintext on RC4," SAC, ., 2013.

[18] N. AlFardan, D. J. Bernstein, K. G. Paterson , J. C. Schuldt, "On the Security of RC4 in TLS," USENIX, ., 2013.

[19] "CVE Details," Available: http://www.cvedetails.com/cve/CVE-2011-3389.

[20] "Mozilla Firefox," Available: https://developer.mozilla.org/en-US/docs/Security_in_Firefox_2.

[21] "Google Chrom," Available: https://code.google.com/p/chromium/issues/detail?id=90392.

[22] "Microsoft Security Bulletin - MS2-006 - Important," Available: http://technet.microsoft.com/en-us/security/bulletin/ms12-006.

[23] "Oracle," Available: http://www.oracle.com/technetwork/topics/security/javacpuoct2011-443431.html.

[24] "List of Browsers Support for Different TLS Version," Available: https://en.wikipedia.org/wiki/Transport_Layer_Security#Web_browsers.

参考資料３

CRYPTREC 暗号技術ガイドライン (SHA-1)

2014 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

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、CRYPTREC 暗号リストの運用監視暗号リストに記載されているハッシュ関数 SHA-1 を利用する際に必要となる情報を示すものである。

1.2. 本書の構成

本書では、2 章で SHA-1 に関する非推奨及び許容事項を、3 章で参考情報を示す。

1.3. 注意事項

本書の内容は2014年3月31日時点の情報に基づき構成されている。従って、今後、CRYPTREC 暗号リストの改定や攻撃方法の研究動向等によって、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。

2. ハッシュ関数 SHA-1 の利用について

2.1. 推奨されない利用範囲

(1)電子署名における署名生成

2012 年度に策定した CRYPTREC 暗号リスト(2013 年 3 月 1 日付) [1]の運用監視暗号リストに記載されている。なお、2008 年 4 月に NISC から「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」 [5]が策定されているため、CRYPTREC 暗号リスト [1]では、RSA-PSS 及び RSASSA-PKCS1-v1_5 には下記の(注 1)が付記されている。

(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)

2.2. 許容される利用範囲

(1) 電子署名における署名検証

2012 年度に策定した CRYPTREC 暗号リスト(2013 年 3 月 1 日付) [1]の運用監視暗号リストに記載されている。なお、一定の検証要件を満たすことにより、電子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 及び XML に対応)が標準化(JIS 及び ISO)されている。

(2) The Keyed-Hash Message Authentication Code (HMAC)

NIST FIPS PUB 198-1[7]の仕様に基づく HMAC が CRYPTREC 暗号リスト [1]に記載されている。安全性について特段の問題点は指摘されていない [8]。

(3) Key Derivation Functions (KDFs)

NIST SP 800-56A、ANS X9.42、SEC 1 v1.0 で使用される KDF の安全性について、特段の問題点は指摘されていない [9,10]。

(4) 擬似乱数生成系

・ 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

の3つの方式が2002年度に策定した改定前の電子政府推奨暗号リスト [2]に記載されている。
また、NIST Special Publication 800-90A [13]にある

・ Hash_DRBG、
・ HMAC_DRBG、
・ CTR_DRBG

の3つの方式が2009年度版リストガイド [14]に記載されている。

(5) パスワード・ハッシングやチェックサムの計算としての利用(hash-only applications)

3. 参考情報

(1)電子署名における署名生成

2002 年度に策定した改定前の電子政府推奨暗号リスト(2003 年 2 月 20 日付) [2]では、ハッシュ関数の SHA-1 は注釈において、『(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。』と規定していた。また、暗号技術監視委員会(当時)は「SHA-1 の安全性に関する見解」(2006 年 6 月 28 日付け) [3,4]において、『電子署名やタイムスタンプのように長期間にわたって利用するシステムでは、新規(更新を含む)に暗号化又は電子署名の付与のアルゴリズムを導入する場合には、256 ビット以上のハッシュ関数の使用を薦める。』と報告していた。

NIST Special Publication 800-131A [6]では、

Digital Signature Process	Use	
Digital Signature Generation	80 bits of security strength: DSA: ((|p| ≥ 1024) and (|q| ≥ 160)) and ((|p| < 2048) OR (|q| < 224)) RSA: 1024 ≤ |n| < 2048 EC: 160 ≤ |n| < 224	Acceptable through 2010 Deprecated from 2011 through 2013 Disallowed after 2013
	≥ 112 bits of security strength: DSA: |p| ≥ 2048 and |q| ≥ 224 RSA: |n| ≥ 2048 EC: |n| ≥ 224	Acceptable

とされている。

(2) 電子署名における署名検証

NIST Special Publication 800-131A [6]では、

Digital Signature Process	Use	
Digital Signature Verification	80 bits of security strength: DSA: ((|p| ≥ 1024) and (|q| ≥ 160)) and ((|p| < 2048) OR (|q| < 224)) RSA: 1024 ≤ |n| < 2048 EC: 160 ≤ |n| < 224	Acceptable through 2010 Legacy-use after 2010
	≥ 112 bits of security strength: DSA: |p| ≥ 2048 and |q| ≥ 224	Acceptable

	RSA: $\|n\| \geq 2048$ EC: $\|n\| \geq 224$	

Acceptable is used to mean that the algorithm and key length is safe to use; no security risk is currently known.

Legacy-use means that the algorithm or key length may be used to process already protected information (e.g., to decrypt ciphertext data or to verify a digital signature), but there may be risk in doing so. Methods for mitigating this risk should be considered.

とされている。

(3) Key Derivation Functions (KDFs)

NIST Special Publication 800-135 Revision 1 [11]を含む、一般的なアプリケーションで利用される KDF については、「2012 年度版リストガイド(KDF に関する調査)」に記載されている [12]。

(4) 擬似乱数生成系

現在、NIST Special Publication 800-90A Revision 1 [15]、800-90B [16]及び800-90C [17]はドラフト版になっている。

なお、NIST Special Publication 800-131A [6]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関する移行指針が下記の通り記載されている。

The use of the RNGs specified in FIPS 186-2, [X9.31] and ANS [X9.62] is **deprecated** from 2011 through December 31, 2015, and disallowed after 2015.

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).

(5) パスワード・ハッシングやチェックサムの計算としての利用(hash-only applications)

NIST Special Publication 800-131A [6]に記載がある。

4. 参考文献

[1] 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

[2] 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

[3] CRYPTREC Report 2005 (第 2 版)[1]、2006 年 5 月 17 日

[4] 暗号技術検討会報告書(2006 年度)[2]、2007 年 3 月

[5] 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[3]、2008 年 4 月 22 日

[6] NIST Special Publication 800-131A[4]、2011 年 1 月

[7] NIST FIPS PUB 198-1[5]、2008 年 7 月

[8] Mihir Bellare, New Proofs for NMAC and HMAC: Security Without Collision-Resistance[6], CRYPTO 2006, LNCS 4117, pp. 602-619, 2006.

[9] CRYPTREC Report 2007, 2008 年 3 月

[10] 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[7]、2008 年 3 月

[11] NIST Special Publication 800-135 Revision 1[8], 2011 年 12 月

[12] CRYPTREC Report 2012[9], 2013 年 3 月

[13] NIST, Special Publication 800-90A[10], 2012 年 1 月

[14] 2009 年度版リストガイド[11]、2010 年 3 月 ([1]で例示したもの、及び、[12]の Hash_DRBG、HMAC_DRBG、CTR_DRBG)

[15] NIST, Draft NIST Special Publication 800-90A Revision 1[12]

[16] NIST, Draft NIST Special Publication 800-90B[13]

[17] NIST, Draft NIST Special Publication 800-90C[14]

---

[1] http://www.cryptrec.go.jp/report/c05_wat_final.pdf
[2] http://www.cryptrec.go.jp/report/c06_kentou_final.pdf
[3] http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf
[4] http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf
[5] http://csrc.nist.gov/publications/fips/fips198-1/FIPS-198-1_final.pdf
[6] https://eprint.iacr.org/2006/043
[7] http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf
[8] http://csrc.nist.gov/publications/nistpubs/800-135-rev1/sp800-135-rev1.pdf
[9] http://www.cryptrec.go.jp/report/c12_sch_web.pdf
[10] http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf
[11] http://www.cryptrec.go.jp/report/c09_guide_final.pdf
[12] http://csrc.nist.gov/publications/drafts/800-90/draft_sp800_90a_rev1.pdf
[13] http://csrc.nist.gov/publications/drafts/800-90/draft-sp800-90b.pdf

参考資料４

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		名称
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)	3-key Triple DES(注3)
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256
		SHA-384
		SHA-512
暗号利用モード	秘匿モード	CBC
		CFB
		CTR
		OFB
	認証付き秘匿モード	CCM
		GCM(注4)
メッセージ認証コード		CMAC
		HMAC
エンティティ認証		ISO/IEC 9798-2
		ISO/IEC 9798-3

[1] 総務省政策統括官（情報通信担当）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）　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。

（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。

（注4）　初期化ベクトル長は 96 ビットを推奨する。

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		名称
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		該当なし
暗号利用モード	秘匿モード	該当なし
	認証付き秘匿モード	該当なし
メッセージ認証コード		PC-MAC-AES
エンティティ認証		ISO/IEC 9798-4

（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） 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。

（注7） 平文サイズは 64 ビットの倍数に限る。

[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		名称
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	該当なし
	128 ビットブロック暗号	該当なし
	ストリーム暗号	128-bit RC4(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	該当なし
メッセージ認証コード		CBC-MAC(注11)
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） 128-bit RC4 は、SSL （TLS 1.0 以上）に限定して利用すること。

（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。

[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。

参考資料５

2013 年度　暗号技術検討会　構成員・オブザーバ名簿

2014.3.27 現在

（構成員）

○今井　秀樹	中央大学　理工学部電気電子情報通信工学科　教授
上原　哲太郎	立命館大学　情報理工学部情報システム学科　教授
太田　和夫	電気通信大学　電気通信学部情報通信工学科　教授
岡本　栄司	筑波大学大学院　システム情報工学研究科　教授
岡本　龍明	日本電信電話株式会社　セキュアプラットフォーム研究所 岡本特別研究室　室長（社団法人電気通信事業者協会代表兼務）
金子　敏信	東京理科大学　理工学部電気電子情報工学科　教授
国分　明男	一般財団法人ニューメディア開発協会　顧問・首席研究員
佐々木　良一	東京電機大学　未来科学部情報メディア学科　教授
武市　博明	一般社団法人情報通信ネットワーク産業協会　常務理事
近澤　　武	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 グループリーダー（ISO/IEC JTC 1/SC27/WG2 Convenor（国際主査））
中山　靖司	日本銀行　金融研究所情報技術研究センター　企画役
本間　尚文	東北大学大学院　情報科学研究科　准教授
松井　　充	三菱電機株式会社　情報技術総合研究所　情報セキュリティ技術部長
松尾　真一郎	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 セキュリティアーキテクチャ研究室　室長（ISO/IEC JTC1 SC27/WG2（国内小委員会主査））
松本　　勉	横浜国立大学　大学院環境情報研究院　教授
松本　　泰	セコム株式会社　IS 研究所 コミュニケーションプラットフォームディビジョン　マネージャー
向山　友也	社団法人テレコムサービス協会　技術・サービス委員会　委員長
渡辺　　創	ISO/IEC JTC1 SC27　国内委員会　委員長

○：座長

（オブザーバ）

奥山　　剛	内閣官房情報セキュリティセンター内閣企画官
佐藤　正明	警察庁情報通信局情報管理課長
稲垣　　浩	総務省行政管理局行政情報システム企画課情報システム企画官
増田　直樹	総務省自治行政局地域政策課地域情報政策室長
篠原　俊博	総務省自治行政局住民制度課長
野口　宣大	法務省民事局商事課長
大村　周一郎	外務省大臣官房情報通信課長
郷　　敦	財務省大臣官房文書課業務企画室長
田中　正幸	文部科学省大臣官房政策課情報化推進室長
三富　則江	厚生労働省大臣官房統計情報部情報システム課長
辻本　崇紀	経済産業省産業技術環境局基準認証ユニット情報電子標準化推進室長
木村　和仙	防衛省運用企画局情報通信・研究課サイバー攻撃対処・情報保証企画室長
平　　和昌	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長
寶木　和夫	独立行政法人産業技術総合研究所セキュアシステム研究部門 副研究部門長
伊藤　毅志	独立行政法人情報処理推進機構セキュリティセンター長
亀田　　繁	一般財団法人日本情報経済社会推進協会電子署名・認証センター長
西村　敏信	公益財団法人金融情報システムセンター監査安全部長

（五十音順、敬称略）