CRYPTREC
Cryptography Research and Evaluation Commitees

暗号技術調査WG(軽量暗号)
活動報告

主査　本間 尚文
東北大学

目次

- 軽量暗号WGについて
- CRYPTRECで扱う軽量暗号のスコープ
- 軽量暗号の優位点と留意点
- 軽量暗号に関する現状調査
- 軽量暗号のアプリケーションに関するヒアリング
- 軽量ブロック暗号の実装詳細評価
- 今後の活動方針に対する提言

軽量暗号WG　活動目的と活動概要

CRYPTREC
Cryptography Research and Evaluation Commitees

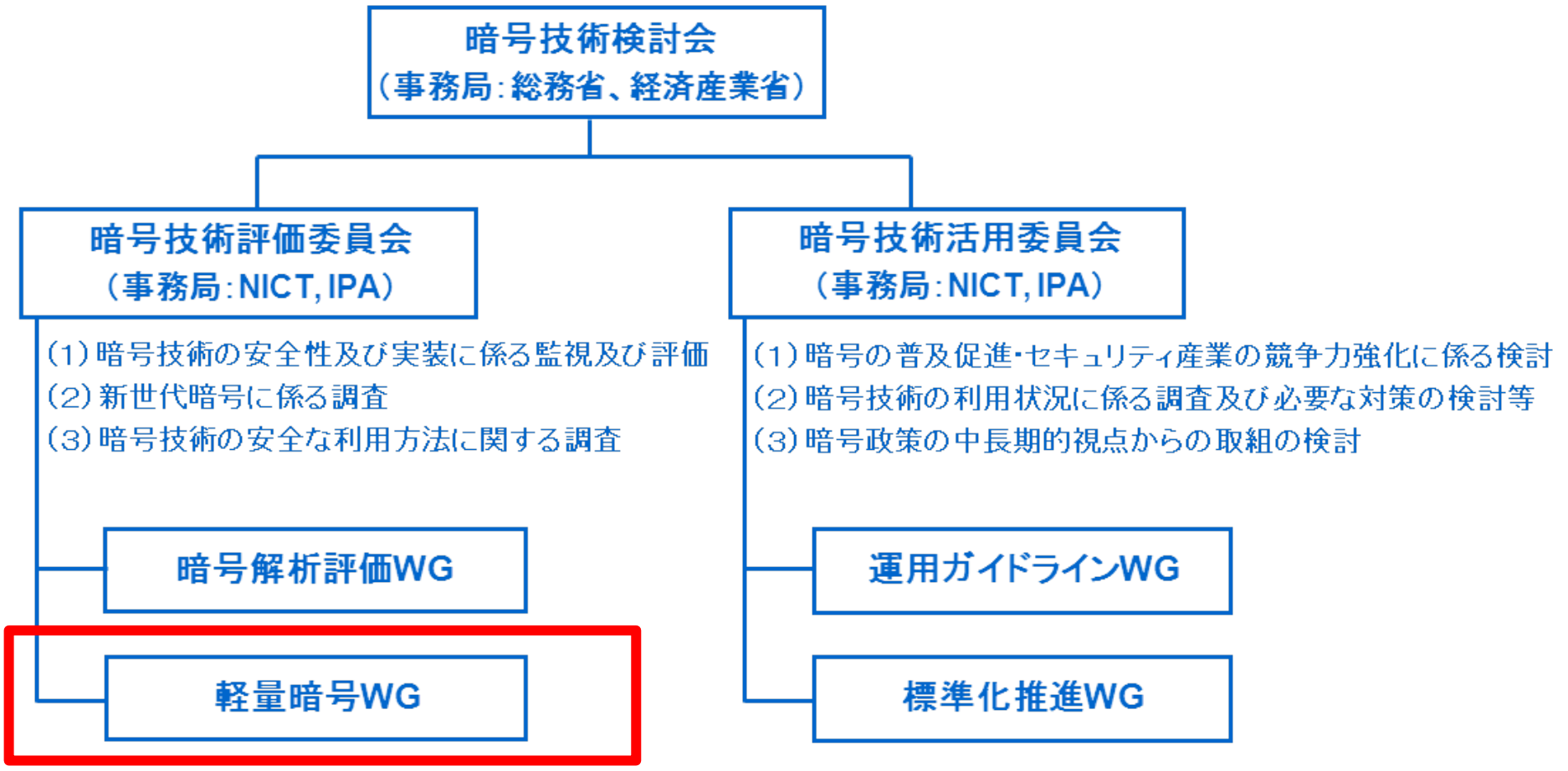
- 活動目的
  - 軽量暗号WGは、軽量暗号技術が求められるサービスにおいて、電子政府のみならず利用者が適切な暗号方式を選択でき、容易に調達できることをめざして設置された。

- 活動概要
  - 軽量暗号技術に関する検討
  - 軽量暗号技術に関する現状調査（サーベイ）
  - アプリケーションに関する調査
  - 実装評価
  - 今後の活動方針に関する議論

軽量暗号WGの位置づけ

CRYPTREC
Cryptography Research and Evaluation Commitees

CRYPTREC体制図



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

軽量暗号WG　委員構成

CRYPTREC
Cryptography Research and Evaluation Commitees

主査	本間　尚文	国立大学法人東北大学
委員	青木　和麻呂	日本電信電話株式会社
委員	岩田　哲	国立大学法人名古屋大学
委員	小川　一人	NHK放送技術研究所
委員	崎山　一男	国立大学法人電気通信大学
委員	渋谷　香士	ソニー株式会社
委員	鈴木　大輔	三菱電機株式会社
委員	成吉　雄一郎	ルネサスエレクトロニクス株式会社
委員	峯松　一彦	日本電気株式会社
委員	三宅　秀享	株式会社東芝
委員	渡辺　大	株式会社日立製作所

CRYPTRECで扱う軽量暗号のスコープ

CRYPTREC Cryptography Research and Evaluation Commitees

- 「実装性能と安全性のトレードオフを勘案した上で、従来の暗号技術に対して特定の性能指標で優位性（軽量性）を持つように設計された暗号技術」をスコープとし、用途が想定される代表的な性能指標に対して優位性を主張する暗号を主な対象とする。

軽量暗号の用途が想定される代表的な性能指標

性能指標		アプリケーションの例
ハードウェア実装	回路規模（消費電力、コスト）	RFID、低コストセンサー
	消費電力量	医療機器、バッテリ駆動デバイス
	レイテンシ（リアルタイム性能）	メモリ暗号化、車載機器、産業向けI/Oデバイス制御
ソフトウェア実装	メモリサイズ（ROM/RAM）	家電機器、センサー、車載機器

軽量暗号技術の優位点と留意点

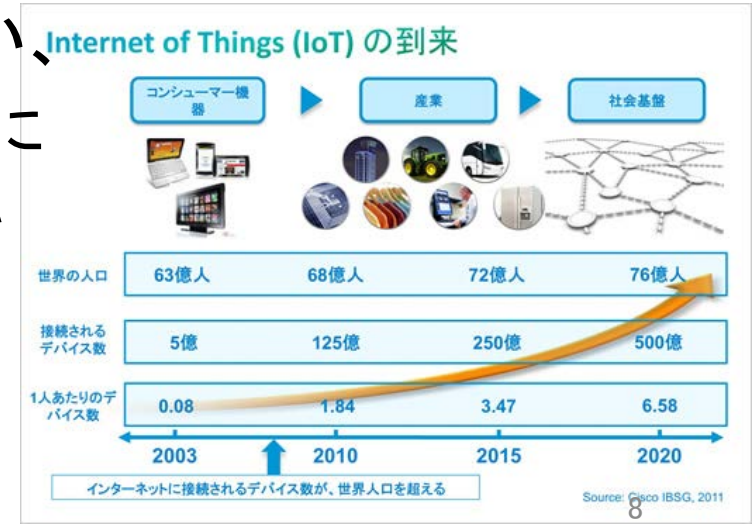
CRYPTREC
Cryptography Research and Evaluation Commitees

- 既存暗号に対して優位性をもつ分野

回路規模	・軽量暗号とAESの差(数kgate)は、50μm角クラスの小さなチップや180nmなど古いプロセスではcriticalで、暗号機能の搭載可否に影響を与えうる。
消費電力量	・回路規模が小さいほど消費電力(量)は小さくなる傾向。軽量暗号により消費電力(量)に関する設計条件を緩和できる効果が期待できる。
レイテンシ	・AESの2倍の応答速度をおよそ1/10の回路規模で実現できる軽量暗号が存在(20kgateで10ns以下での演算が可能)。産業向けI/Oデバイス制御などμsオーダーのリアルタイム性が求められる用途で活用可能。
メモリサイズ	・AESのおよそ1/4のROMサイズで実装可能な軽量暗号が存在。軽量暗号なら追加できるケースやチップ単価を下げられるケースあり。

軽量暗号技術の優位点と留意点

- 既存暗号に対して優位性をもつ分野
  - 2020年、センサー1兆個、IoT機器500億個がつながる時代に、ローエンドマイコンを搭載する機器に暗号技術が必要になることが予想される。
  - 自動運転の実用化、工場やプラントがクラウドとシームレスにつながる時代に、現時点で暗号技術が利用されていない領域にも利用が広がることが予想される。
  - 現時点で暗号技術を搭載していない、想定すらしていない機器やシステムにおいて、将来的に実装面での制約を緩和する効果を期待できる。



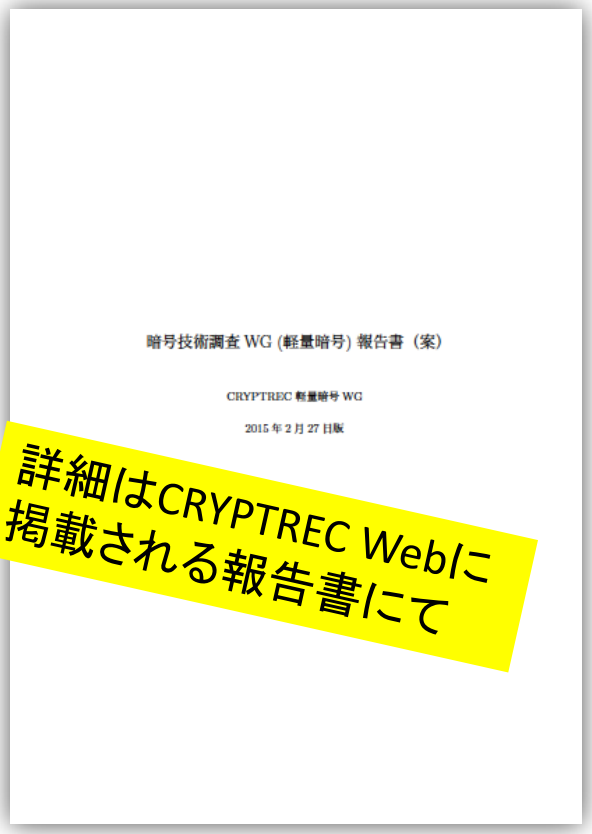
http://cisco-inspire.jp/issues/0010/cover_story.html 参照

軽量暗号技術の優位点と留意点

- 軽量暗号で達成可能な安全性
  - 電子政府推奨暗号リストおよび推奨候補暗号リストに掲載されている暗号技術は、安全性、実装性能が確認された方式。
    - カテゴリ毎に想定されている利用範囲で安全性の問題が生じない、実装性能では実装環境ごとの差が少ないバランスのとれた方式。
  - 軽量暗号は特定の性能指標で優位性をもつように設計されており、上記暗号技術より安全性が低くなる傾向にある。
    - 例えば、64ビットブロック暗号では同じ鍵で2^{32}ブロック(32GB)以上のデータを処理すると、高い確率で無作為に選んだビット列と区別できる。
    - 一つの鍵で処理するデータを減らしたり、上記を回避できるCENCのようなモードを利用するなどの対策法もある。
  - 電子政府推奨暗号でもリスクなしの運用は困難であり、軽量暗号でも利用に応じたリスクを考慮しながらの運用が必要。

軽量暗号技術に関する現状調査

- 軽量暗号アルゴリズム
  - ブロック暗号
  - ストリーム暗号
  - ハッシュ関数
  - MAC
  - 認証暗号
- 軽量暗号に関わる新しい技術動向
  - 低レイテンシ暗号
  - サイドチャネル攻撃耐性
  - CAESARプロジェクト
  - 軽量暗号の活用事例および標準化動向



軽量暗号のアプリケーションに関するヒアリング

- 2013年度第2回軽量暗号WG（2013.12.26）にて
  下記の方々に講演を頂き、議論を行った。

- 「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
    - 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。
- 「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
    - 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ありとのコメント。

軽量ブロック暗号の実装詳細評価

CRYPTREC
Cryptography Research and Evaluation Commitees

- 目的
  - 文献調査では評価環境や実装者が異なり、アルゴリズム間の比較が困難であることから、同一プラットフォーム上で、統一的な実装ポリシーにより評価を行う。
- 評価対象アルゴリズム
  - AES, Camellia, CLEFIA, PRESENT, LED, Piccolo, TWINE, PRINCE
- 実装環境および測定指標
  - 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、回路遅延、消費電力、ピーク電流、リーク電力
  - 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

軽量ブロック暗号の実装詳細評価

- 評価結果概要
  - ハードウェア実装
    - 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。
    - 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。
    - 小さい、速いという単一指標だけだと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ような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。
  - ソフトウェア実装
    - 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ROM200バイト以下、RAM32バイト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。

今後の活動方針に対する提言

CRYPTREC
Cryptography Research and Evaluation Commitees

2015年度以降の活動方針案：概要、目的、期待される効果

A) 暗号技術ガイドライン（軽量暗号の最新動向）の作成

- 軽量暗号の最新技術動向をまとめた技術レポート
- 軽量暗号の利用促進

B) 暗号技術ガイドライン（軽量暗号の詳細評価）の作成

- 軽量暗号の安全性と実装性能を統一的に評価した技術レポート
- 軽量暗号を選択・利用する際の技術的判断材料として活用
- 軽量暗号の利用促進
- 第三者評価レポートとして活用

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・選定
- 電子政府システム等での最適な方式の選択と調達

A) B)のハイブリッド案で軽量暗号に関する暗号技術ガイドラインを作成する。

今後の活動方針に対する提言

CRYPTREC
Cryptography Research and Evaluation Commitees

提言に対する根拠

- 軽量暗号は、特定の性能指標における優位性が認められ、次世代のネットワークサービスでの活用が期待される一方、電子政府推奨暗号リスト掲載の暗号技術ほど高い安全性を保証していない方式もあり、利用において留意すべき点がある。
- 軽量暗号を選択・利用する際の技術的判断に資することや今後の利用促進をはかることを目的として暗号技術ガイドラインを発行することが有効と考えられる。
- 軽量暗号も分野が広く、詳細評価が望ましい分野と既存文献調査で十分と思われる分野がある。

⇒A)とB)のハイブリッドで軽量暗号に関するガイドラインを作成

おわりに

- 軽量WGでの２年間の調査・検討結果をまとめ、CRYPTRECでの今後の活動方針について提言を行った。
- IoT等の次世代ネットワークサービスにおいて軽量暗号の活用が期待されることから、方式を選択・利用する際の技術的判断に資すること、今後の利用促進をはかることを目的として、暗号技術ガイドラインを作成する。

- 本WGでの調査・検討内容詳細は、4月以降にCRYPTREC Webページで公開される報告書をご覧下さい。