CRYPTREC
Cryptography Research and Evaluation Committees

暗号実装委員会活動報告

委員長　本間 尚文

東北大学

目次

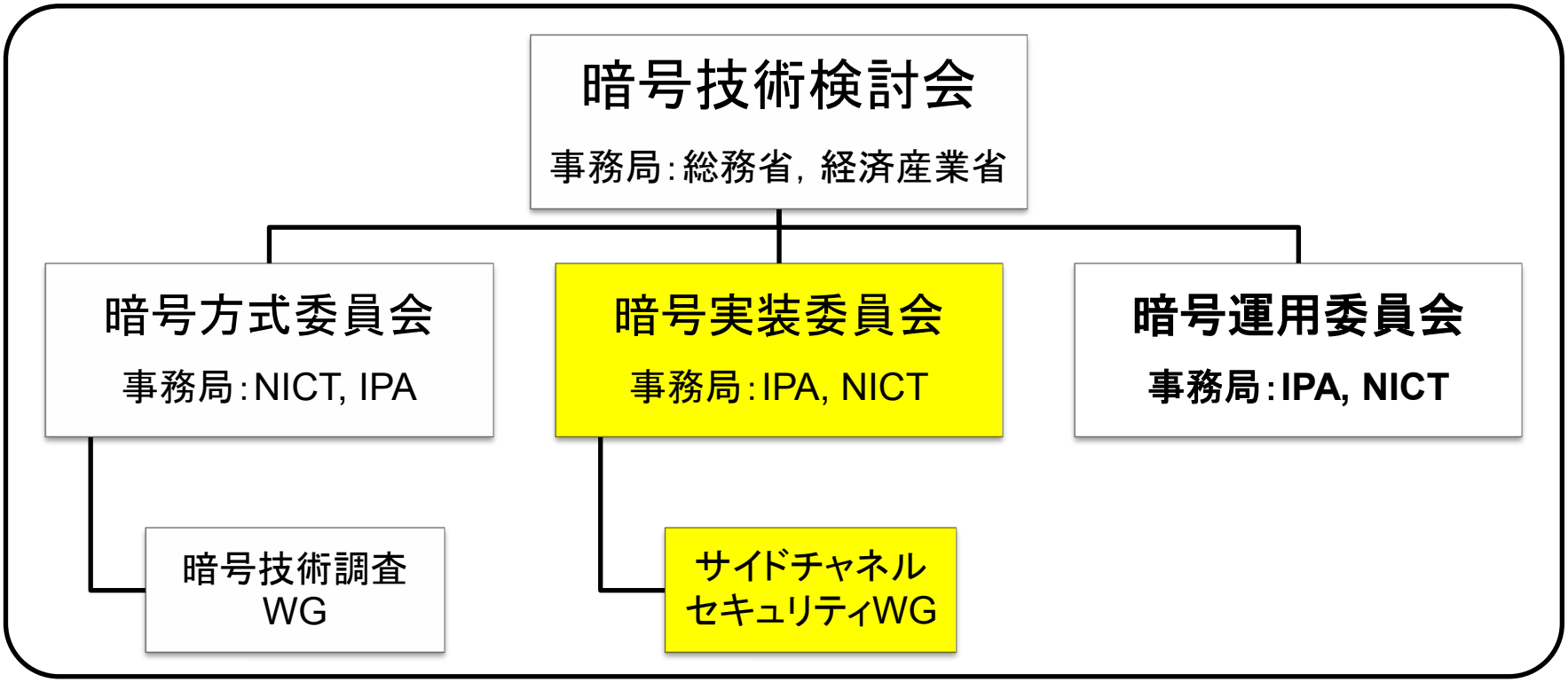
CRYPTREC
Cryptography Research and Evaluation Committees

0. 暗号実装委員会の概要

暗号実装委員会の紹介

2009年度に暗号モジュール委員会を継承する形で新設

電子政府推奨暗号リスト改定のための実装性能評価を実施するとともに，前身の暗号モジュール委員会の業務を引き継ぐ。



CRYPTREC
Cryptography Research and Evaluation Committees

2012年度暗号実装委員会委員

委員長	本間　尚文	東北大学　大学院　情報科学研究科
委員	植村　泰佳	電子商取引安全技術研究組合
委員	大須賀　勝美	NTTエレクトロニクス株式会社　セイフティ・ネットワーク事業部開発部
委員	亀田　繁	日本情報経済社会推進協会　電子署名・認証センター
委員	川村　信一	産業技術総合研究所　セキュアシステム研究部門
委員	﨑山　一男	電気通信大学　大学院　情報理工学研究科
委員	佐藤　恒夫	三菱電機株式会社　情報技術総合研究所
委員	清水　秀夫	株式会社東芝　研究開発センター
委員	高橋 順子	日本電信電話株式会社　NTTセキュアプラットフォーム研究所
委員	高橋　芳夫	株式会社NTTデータ　技術開発本部　セキュリティ技術センタ
委員	角尾　幸保	日本電気株式会社　情報・メディアプロセッシング研究所
委員	鳥居　直哉	株式会社富士通研究所　ソフトウェアシステム研究所
委員	松崎　なつめ	パナソニック株式会社　デジタル・ネットワーク開発センター
委員	松本　勉	横浜国立大学　大学院　環境情報研究院
委員	渡辺　大	株式会社日立製作所　横浜研究所

CRYPTREC
Cryptography Research and Evaluation Committees

2012年度の活動内容

(1) 電子政府推奨暗号改定のための実装性能評価

新規応募暗号技術及び従来の電子政府推奨暗号リスト掲載暗号技術に対するハードウェア実装及びソフトウェア実装の性能評価を完了する。実装は，応募暗号については応募者が，従来の掲載暗号については事務局が開発し，性能は事務局で測定する。また，新規カテゴリのメッセージ認証コード(MAC)については，比較対象として事務局選出のCMACを事務局が実装したものを使用する。

(2)サイドチャネル攻撃対策の有効性確認

新規応募暗号のうち128ビットブロック暗号とストリーム暗号について，応募者が提案するサイドチャネル攻撃対策が有効であるか確認する。この評価はリスト改定における暗号選択には利用されない。

(3)サイドチャネル攻撃等の実験データに関する調査

サイドチャネル解析用プラットフォームの仕様であるSASEBOボード等を用いた評価・解析実験情報の収集と分析を行い，暗号モジュールの安全性・信頼性を評価するための情報を収集する。この活動は，サイドチャネルセキュリティWGにおいて実施する。

(4)国際標準化活動への貢献

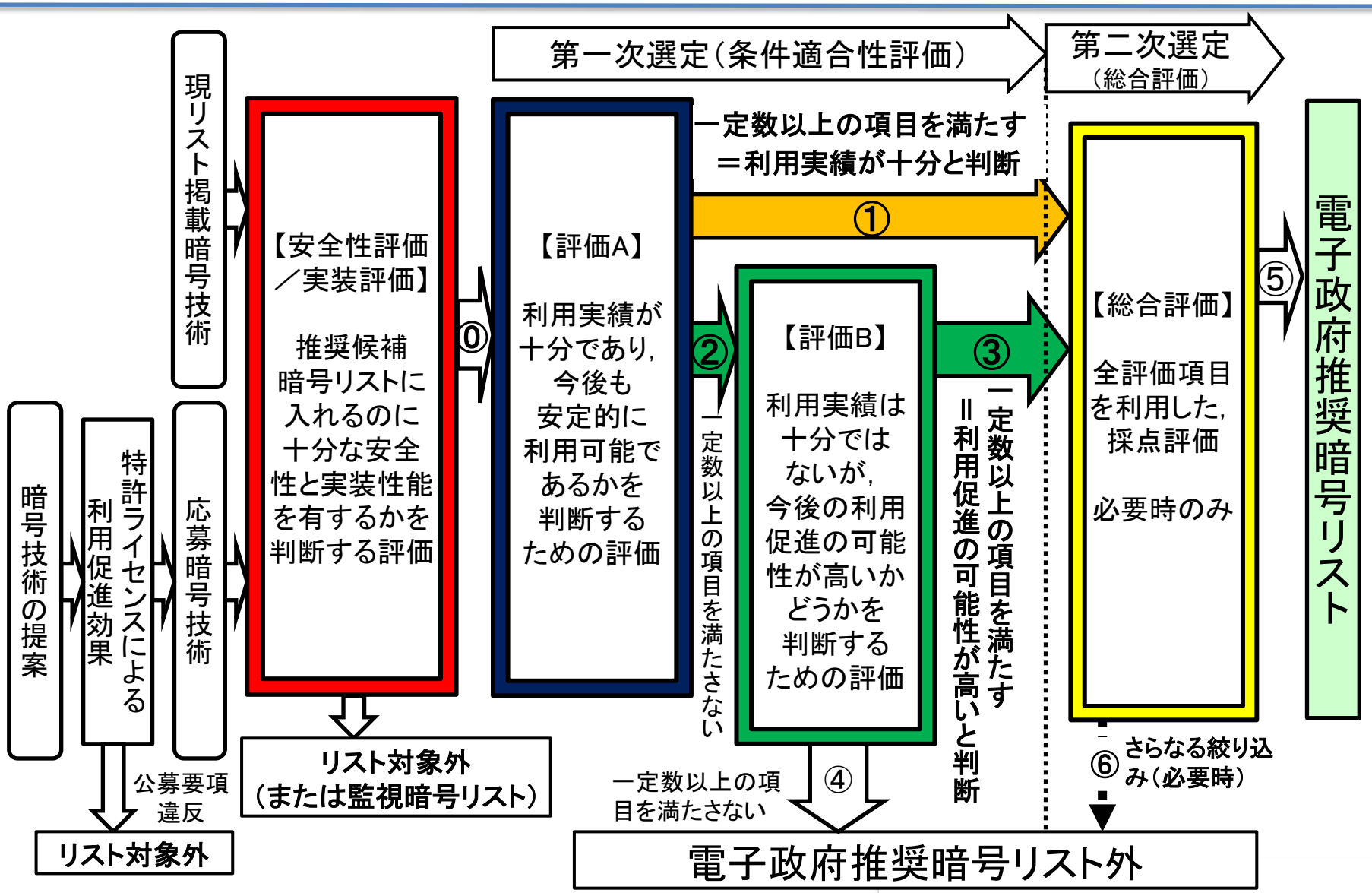
サイドチャネル攻撃に関する調査活動の一環として，暗号モジュールに対するセキュリティ要件及び試験要件の国際標準化に協力する。この活動は，サイドチャネルセキュリティWGにおいて実施する。

2012年度の委員会審議状況

回	開催日時	主な議題
第1回	2012. 7. 5	● 暗号実装委員会活動計画の検討 ● 次期リスト作成に向けた実装性能評価方針の検討 （【安全性評価／実装評価】，【評価B】，【総合評価】）
第2回	2012. 9. 4	● 【安全性評価／実装評価】の判定決定 ● 【評価B】の状況報告（新規応募暗号者に対する質問実施状況）と評価方針決定
第3回	2012. 10. 9	● 【評価B】と【総合評価】の判定決定 ● 実装性能評価結果の情報公開方法に関する検討
合同委員会（三委員長）	2012. 11. 15	● CRYPTREC暗号リスト（案）素案の決定
CRYPTREC暗号リスト発表	2013. 3. 1	● CRYPTREC暗号リスト発表
第4回	2013. 3. 14	● 実装評価データの一部更新 ● サイドチャネル攻撃対策の有効性確認方針の決定 ● 今後の課題検討

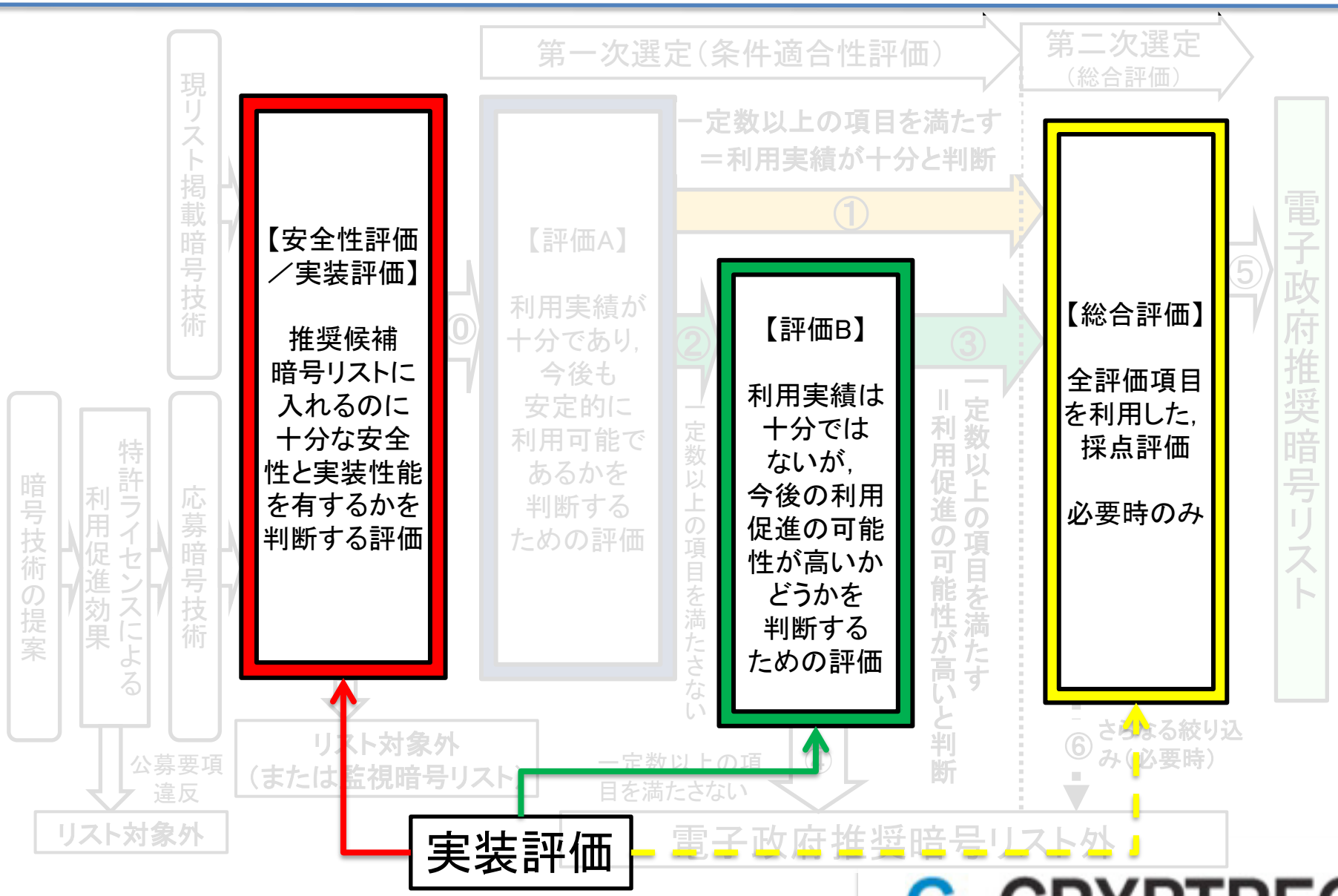
1.【安全性評価・実装評価】における実装性能評価

暗号リスト選定のフレームワーク



CRYPTREC
Cryptography Research and Evaluation Committees

暗号リスト選定のフレームワーク



CRYPTREC
Cryptography Research and Evaluation Committees

【安全性評価・実装性評価】における実装評価の概要

■ 目的

- 推奨候補暗号としての十分な実装性能の有無を判定する。

■ 評価対象暗号の分類（提案者／新旧）

（前）前電子政府推奨暗号リスト掲載暗号

（新）新規応募暗号

（事）事務局選出暗号

■ 判定結果

- 全評価対象暗号を推奨候補暗号としての実装性能を有すると判定した。

公開鍵暗号の判定結果

○は第一次選定（評価A・B）の対象とすることを示す

	カテゴリ	暗号技術名	分類	判定
公開鍵暗号	署名	DSA	（前）	○
		ECDSA	（前）	○
		RSASSA-PKCS-v1_5	（前）	○
		RSA-PSS	（前）	○
	守秘	RSA-OAEP	（前）	○
		RSAES-PKCS1-v1_5	（前）	○
	鍵共有	DH	（前）	○
		ECDH	（前）	○
		PSEC-KEM	（前）	○

共通鍵暗号の判定結果

○は第一次選定（評価A・B）の対象とすることを示す

	カテゴリ	暗号技術名	分類	判定
共通鍵暗号	64ビットブロック暗号	CIPHERUNICORN-E	（前）	○
		Hierocrypt-L1	（前）	○
		MISTY1	（前）	○
		3-key Triple DES	（事）	○
	128ビットブロック暗号	CLEFIA	（新）	○
		AES	（前）	○
		Camellia	（前）	○
		CIPHERUNICORN-A	（前）	○
		Hierocrypt-3	（前）	○
		SC2000	（前）	○
	ストリーム暗号	Enocoro-128v2	（新）	○
		KCipher-2	（新）	○
		MUGI	（前）	○
		MULTI-S01	（前）	○
		128-bit RC4	（前）	○

その他暗号技術の判定結果

○は第一次選定（評価A・B）の対象とすることを示す

	カテゴリ	暗号技術名	分類	判定
その他	ハッシュ関数	RIPEMD-160	（前）	○
		SHA-1	（前）	○
		SHA-256	（前）	○
		SHA-384	（前）	○
		SHA-512	（前）	○
	メッセージ認証コード	PC-MAC-AES	（新）	○
		CBC-MAC	（事）	○
		CMAC	（事）	○
		HMAC	（事）	○
	暗号利用モード	CBC	（事）	○
		CFB	（事）	○
		OFB	（事）	○
		CTR	（事）	○
		GCM	（事）	○
		CCM	（事）	○
	エンティティ認証	ISO/IEC 9798-2	（事）	○
		ISO/IEC 9798-3	（事）	○
		ISO/IEC 9798-4	（事）	○

各分類に対する判定

■ 前推奨暗号リスト暗号の判定 （前）

前回公募・選考時(2000−2002年度)に十分な実装性能を確認済みである。

■ 事務局選出暗号の判定 （事）

ISO/IECや米国NISTなど国際的な規格に採用されており，落とすに足る実装上の問題は報告されていない。

■ 新規応募暗号の判定 （新）

新規応募暗号には現リスト暗号と同等以上の特長（安全性又は実装性）が要求されているため，その実装性能を評価した。

実装評価の結果，応募された全ての暗号が現リスト暗号と同等以上の特長を有することを確認した。

新規応募暗号と比較対象

① 128ビットブロック暗号及びストリーム暗号

- 同じカテゴリの現リスト暗号を比較対象とする。

② メッセージ認証コード

- 事務局選出暗号としてCMACを比較対象とする（ブロック暗号にはAESを使用）。

	評価対象暗号	比較対象暗号	
	新規応募暗号	現リスト暗号	事務局選出暗号
128ビットブロック暗号	CLEFIA	AES Camellia CIPHERUNICORN-A Hierocrypt-3 SC2000	
ストリーム暗号	Enocoro-128v2	MUGI	
	KCipher-2	MULTI-S01*	
メッセージ認証コード	PC-MAC-AES		CMAC (AES)

* ハードウェア実装のみ測定

新規応募暗号評価の基本方針と概要

■ 実装評価の基本方針

- 評価環境は電子政府における利用を念頭に選択する。
- 判定基準は恣意性を排除した説明しやすいものにする。

① 判定基準

評価指標の少なくとも一つにおいて，測定値が比較対象全てに対して優れていれば，優位性ありと判定する。

② 実装評価内容

- ソフトウェア実装評価：Windows PC上での実装性能を評価
- ハードウェア実装評価：FPGA上の実装性能を評価

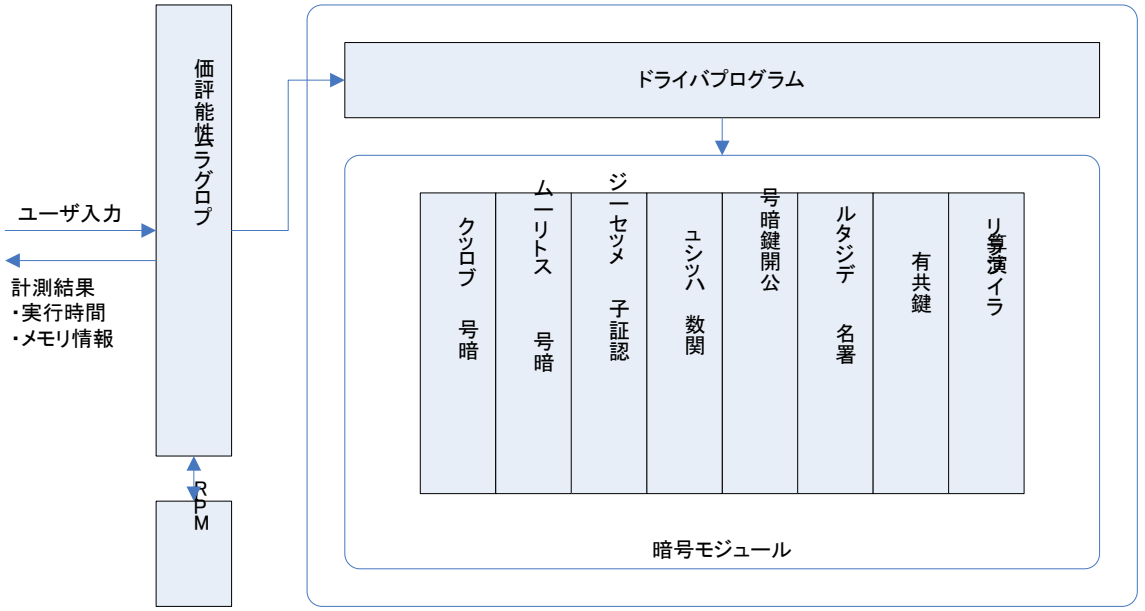
③ 複数の実装を提出した新規応募暗号の扱い

- ハードウェア実装でのリソース利用が最も少ないものを対象とする。
- 安全性パラメータが複数の場合は全てに優位な場合のみ優位性を認める。

ソフトウェア実装測定　－　評価環境

ソフトウェア性能評価ツール *

- ドライバプログラムの機能
  - 入出力ストリーム
  - 測定機能
- 提供される測定項目
  - 実行時間
  - メモリサイズ
- 現リスト暗号（比較対象）
  - 暗号ライブラリとして実装済み
- 新規応募暗号
  - 提供するサンプルコードに基づいて応募者側で実装
  - アセンブリ実装やIntel Compiler利用は不可



評価ツールの全体構成

*2009年度経済産業省委託研究「クラウド環境における暗号技術評価」の一環として開発

CRYPTREC
Cryptography Research and Evaluation Committees

ソフトウェア実装測定　－　実装方法

①　評価対象：新規応募暗号

- 実装者：暗号の応募者
- 経済産業省が2009年度に実施した委託事業「クラウド環境における暗号技術評価」で作成した性能評価ツール向けに実装（サンプルコードを元に設計）

②　比較対象１：現リスト掲載暗号と事務局選出暗号

- 実装者：上記評価ツールの開発者
- 上記評価ツール付属の暗号ライブラリとして実装

③　比較対象２：OpenSSL のAES

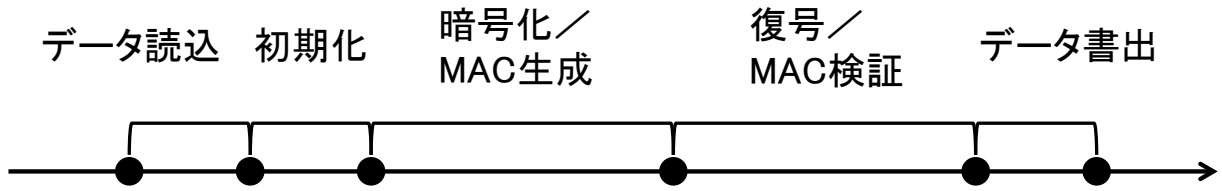
- 実装者：事務局
- OpenSSL提供のソース(1.0.1c内のC言語ソース)を上記評価ツール向けに実装（第三者が確認可能な比較対象として）

ソフトウェア実装測定　－　評価項目

測定の概要

ソフトウェア性能評価ツールを用いて各暗号で処理に要する時間および利用したメモリ量を測定する。

- 処理の概要:



- 出力データ:
  - 初期化時間
  - 暗号化時間（メッセージ認証コードでは，「MAC生成時間」）
  - 復号時間（メッセージ認証コードでは，「MAC検証時間」）
  - データ読込時間＋データ書出時間　（暗号による違いが小さい）
  - プロセスメモリ利用量の平均値
  - プロセスメモリ利用量のピーク値

ハードウェア実装評価　－　概要

①実装環境等（ターゲットディバイス／開発環境）

- Xilinx Virtex-5 LX50　(SASEBO-GII搭載のFPGA)
- ISE WebPACK Version 12.4

②評価環境

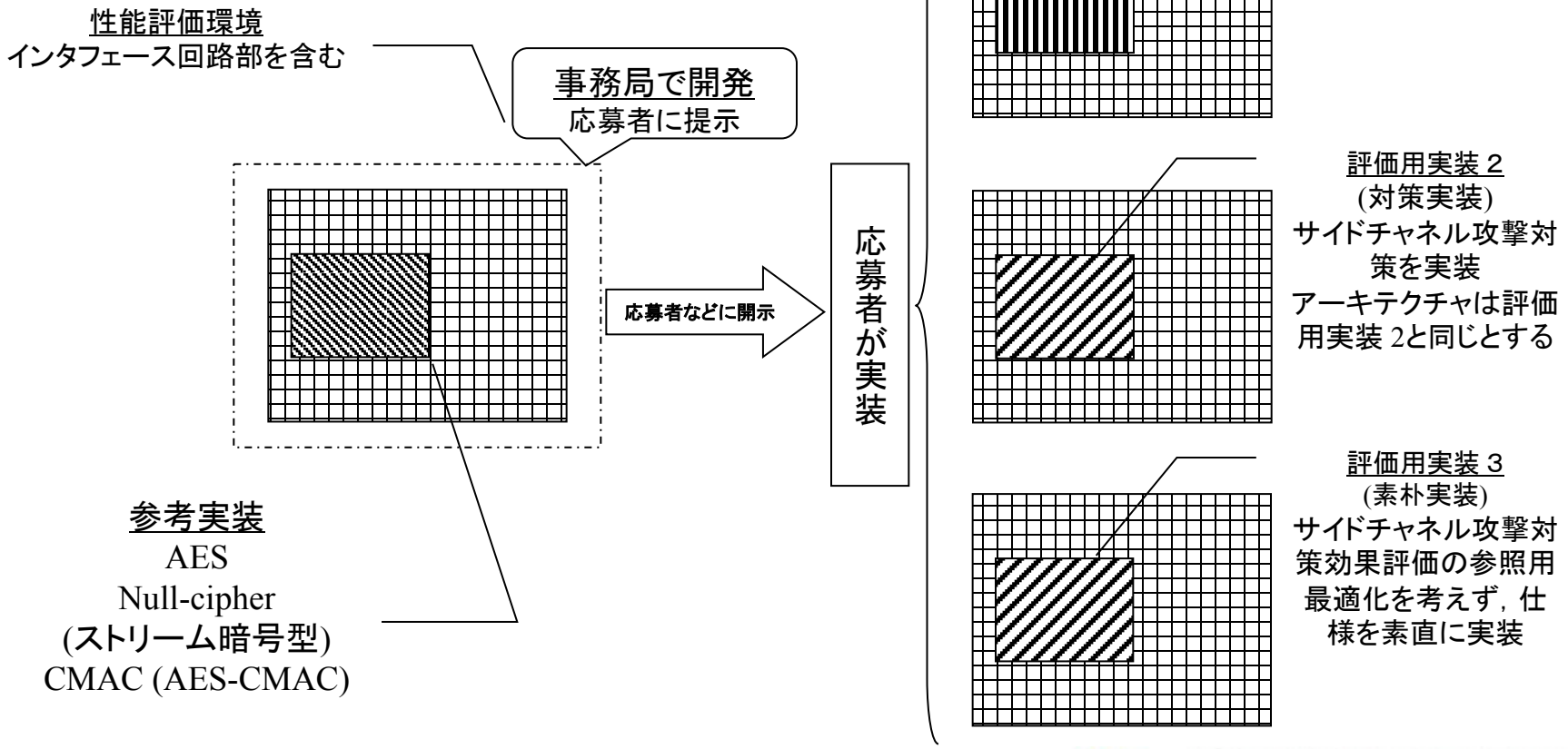
- 産業技術総合研究所（AIST）が開発した，「電子政府推奨暗号用ハードウェア評価環境」等の仕様書，説明書等で説明されている評価環境

③計測項目　（ISE WebPACKのCADサマリ等のデータ）

- 回路規模・処理速度(スライス数，クリティカルパス遅延，クロック数，動作周期)
- 初期化に要するクロック数

ハードウェア実装性能評価 － 評価環境

- 事務局が評価環境（インタフェース回路，参考暗号回路を含む）を提供
- 参考暗号回路を評価対象暗号回路で置換
- 応募暗号は応募者が，現リスト暗号は外部委託による第三者が実装



CRYPTREC
Cryptography Research and Evaluation Committees

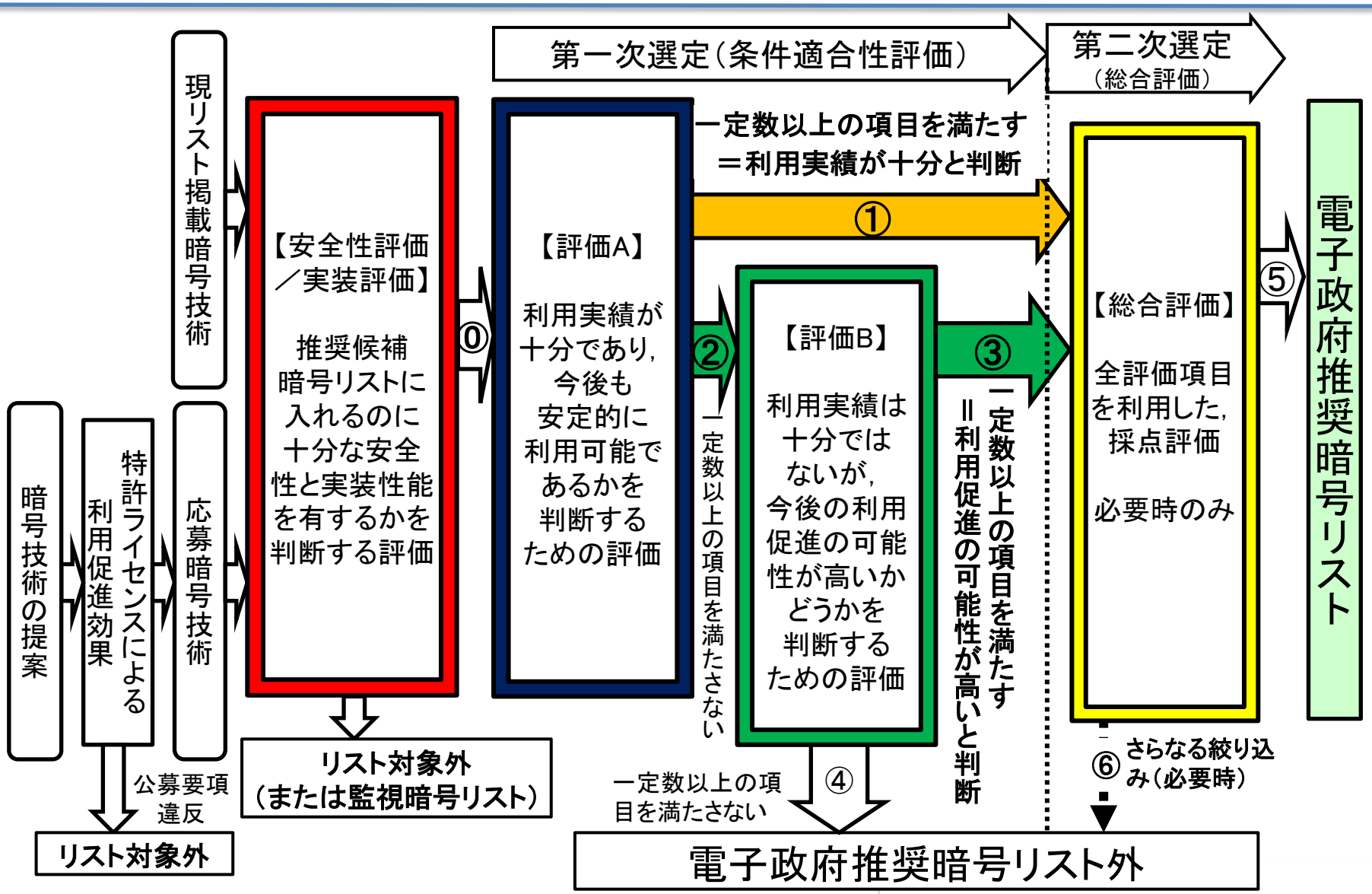
評価結果

- 下記項目において優位性を確認したため，現リスト暗号と同等以上の特長を有すると判定した。
  - 推奨候補暗号リストに追加することを承認した

暗号名	ソフトウェア実装	ハードウェア実装
CLEFIA	初期化時間（16バイト，1536バイト），暗号化速度（16バイト），復号速度（16バイト，1536バイト）	回路効率，規模（LUT-FF pair，LUT）
Enocoro-128v2	初期化時間（全平文長），暗号化速度（16バイト），復号速度（16バイト），メモリ使用量（全平文長）	回路効率，回路規模（LUT-FF pair，LUT，FF）
KCipher-2	初期化時間（全平文長），暗号化速度（全平文長），復号速度（全平文長），メモリ使用量（全平文長）	暗号化速度，回路効率，回路規模（LUT-FF pair，LUT，FF）
PC-MAC-AES	MAC生成速度（全平文長），MAC検証速度（1536バイト，1048576バイト），メモリ使用量（全平文長）	暗号化速度，回路規模（LUT-FF pair），回路効率

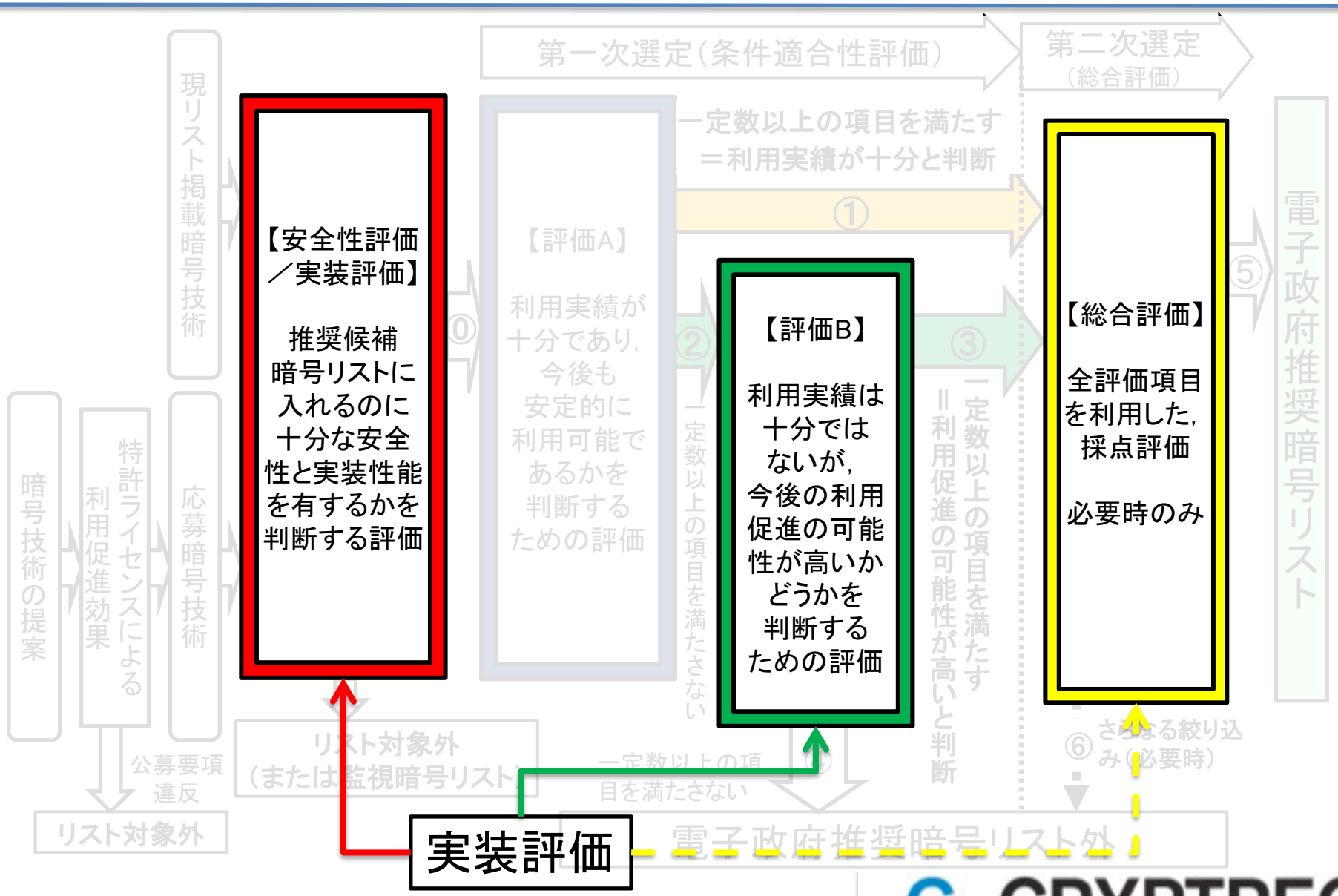
2.【評価B】における実装性能評価

暗号リスト選定のフレームワーク



CRYPTREC
Cryptography Research and Evaluation Committees

暗号リスト選定のフレームワーク



CRYPTREC
Cryptography Research and Evaluation Committees

【評価B】における実装評価の概要

■ 目的

- 評価Bにおける「標準化・規格化の促進を図るハードルの低さ」を判定するための項目の一つ（OR条件）である「市場が認める程度の技術的アドバンテージ」の有無を「実装性能」の面から判定する。

■ 評価対象暗号の分類（提案者／新旧）

（応） 応募された暗号（2000-2001年度，2009年度の公募）

（標） 応募者はなく，事務局が技術的な分類の中で，
標準的なものとして候補に選出した暗号

■ 判定方法

（応）： 技術的な優位性を示す文献・資料から判定

（標）： 標準的なものであることを根拠に一括で判定

各分類に対する判定

■ 応募暗号の判定 （応）

応募者が，同一カテゴリの標準的な暗号技術に対する優位点とそれを示す資料を提出し，その妥当性を審査した。

提出がない場合は，優位性なしと判定した。

■ 応募者がなく，事務局が選出した暗号の判定 （標）

標準的な暗号として比較の基準となるものであるので，それ自体は優位性なしとした。

公開鍵暗号の判定結果（応募暗号）

技術分類	暗号名	回答	比較対象	優位点	分類	判定結果
公開鍵暗号・署名	ECDSA	有	RSA署名	鍵生成時間，署名生成速度	（応）	有
	RSASSA-PKCS-v1_5	無			（応）	無
	RSA-PSS	無			（応）	無
公開鍵暗号・守秘	RSA-OAEP	無			（応）	無
	~~RSAES-PKCS1-v1_5~~ *	無			（応）	無
公開鍵暗号・鍵共有	ECDH	有	DH	鍵生成時間，鍵共有処理	（応）	有
	PSEC-KEM	有	DH	鍵交換速度	（応）	有

* 取消線は暗号方式委員会において推奨候補暗号外と判定された暗号技術。
この判定は第１回暗号技術検討会（2012年8月2日）で承認された。

ブロック暗号の判定結果（応募暗号）

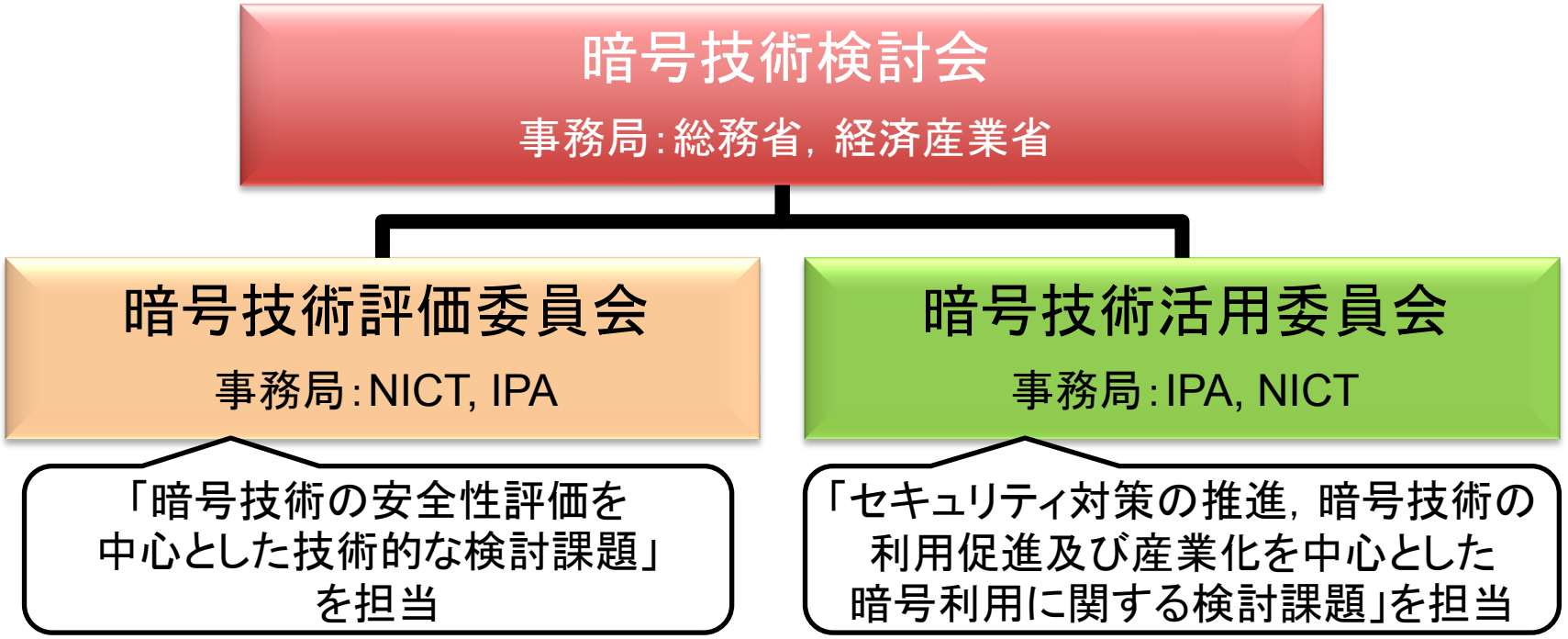
技術分類	暗号名	回答	比較対象	優位点	分類	判定結果
64ビットブロック暗号	CIPHERUNICORN-E	有	TDES	小型実装の実装サイズ	（応）	有
	Hierocrypt-L1	有	MISTY1, TDES	暗号化（復号）速度	（応）	有
	MISTY1	無			（応）	無
128ビットブロック暗号	CLEFIA	有	Camellia	回路効率，小型実装	（応）	有
	Camellia	有	AES	初期化時間(鍵設定，IV設定)，速度，実装サイズ，クリティカルパス遅延，消費電力，回路効率等	（応）	有
	CIPHERUNICORN-A	有	AES	特になし	（応）	無
	Hierocrypt-3	有	AES, Camellia	速度（暗号化，復号）	（応）	有
	SC2000	有	AES	速度，実装環境への対応性，キャッシュメモリの有効活用	（応）	有

ストリーム暗号とMACの判定結果（応募暗号）

技術分類	暗号名	回答	比較対象	優位点	分類	判定結果
ストリーム暗号	Enocoro-128v2	有	ブロック暗号、128ビットストリーム暗号	速度（乱数生成，暗号化），回路規模	（応）	有
	KCipher-2	有	MUGI	速度，初期化時間，内部状態サイズ	（応）	有
	MUGI	有	AES，ストリーム暗号	回路規模，暗号化速度（ハードウェア実装）	（応）	有
	MULTI-S01	有	AES-GCM，AES-CCM	（応募者は速度で優位性があると主張したが，確認できず）	（応）	無
メッセージ認証コード	PC-MAC-AES	有	AESを使用したMAC一般	速度	（応）	有

3. 今後のCRYPTREC活動に向けての課題

CRYPTREC新体制



■暗号技術評価委員会での検討項目

① 新世代暗号に係る調査

② 暗号技術の安全性に係る監視及び評価

③ 暗号技術の安全な利用方法に関する調査

CRYPTREC
Cryptography Research and Evaluation Committees

新体制への引き継ぎ課題

- 実装安全性に関する継続的な動向調査
  - 暗号実装における安全性を維持するため，サイドチャネル攻撃・故障利用攻撃に関する動向調査を継続する必要がある
  - 動向調査の結果をどのように活用するかが課題
- 実装性能評価時の方式の検討
  - 既存暗号と新規応募暗号のフェアな評価方法
    - “一般的な”実装とは？
    - 実装間での最適化の差異の最小化
  - 評価プラットフォームの選定・多様化
    - 今回はWindowsPCでソフトウェア実装評価を行ったが，今後はスマートフォンやタブレット等での利用増が想定される
    - ICカードやRFID等の組込み系を想定した実装評価も必要

レーダーチャートによる測定結果の表示（参考）

【安全性評価・実装評価】における実装性能評価で測定した全項目のデータを参考情報としてレーダーチャートで次頁以降に示す。

ソフトウェア実装測定　－　データに関する注意事項

次の理由から，測定データは評価対象が比較対象と同等以上の性能を有するかの判定のみに使用されるべきである。各暗号（特に比較対象の暗号）の最高性能を示すものではないことに注意されたい。

① 実装方法・開発環境の差異
- 新規応募暗号は応募者，現リスト掲載暗号は評価ツール開発者が実装。
- 現リスト掲載暗号の実装は使用する評価環境向けに最適化されていない。
- 比較対象１のAESはよく知られている高速化手法を使用していない。
  （比較対象２のOpenSSLのAESは使用している）

② 最適化における制約
- MMXなどCPU固有の命令やインラインアセンブラを禁止。

③ 他プロセスの影響
- 他のプロセスの影響を抑えきれない。
- 飛びぬけて大きなクロック数の観測。
  ※　不要プロセスの消去，スタンドアローン動作などの対策は実施

④ 評価ツール自体のオーバーヘッド
- 評価ツール自体がリソースを消費。

ソフトウェア実装測定　－　暗号ごとの特記事項

① AES（外部委託実装）

既存の実装結果と比べ，AESの暗号化速度が相対的に非常に遅い。
原因は通常の高速化手法が利用されていないためと考えられる。

② AES（OpenSSL版）

OpenSSLのソースコードを評価ツールのインターフェイスに合わせて，関数名と変数名を置換した。測定したところ，平文サイズが16バイトでの復号速度が暗号化速度と比較して約1/3と非常に遅かった。
これは，評価ツールでは初期化の際に，暗号化用と復号用の鍵拡大を一括して行う仕様になっていることが，原因の可能性がある。

ハードウェア実装測定 － データに関する注意事項

以下の理由から，測定データは評価対象が比較対象と同等以上の性能を有するかの判定のみに使用されるべきである。

各暗号（特に比較対象の暗号）の最高性能を示すものではないことに注意されたい。

①実装方法・開発環境の差異

- 新規応募暗号は応募者が実装
- 現リスト暗号は評価ツール開発者（第三者）が実装

→ 仕様に忠実な実装であり，最適化はしていない。

② 一種類の実装デバイス（Xilinx Virtex-5 LX50）

- 異なるデバイスへの実装では性能の優劣が逆転する可能性がある。

ハードウェア実装測定　－　暗号ごとの特記事項

①　新規応募暗号

当初，インターフェイス回路(I/F)を含んだ回路を対象としたが，より精度の高い情報を提供するため，本資料では外部委託実装と合わせてI/Fを含まない実装での計測値を採用した。

②　PC-MAC-AES（応募者実装）

AESの暗号コアはCMACのAESコアとは異なる。

③　外部委託実装全般

Virtex-5 を実装したSASEBO-GII ボードでの24MHz 動作を前提に，シンプルなデータパスによる設計を行っている。このため，測定値が各暗号アルゴリズムの絶対的な実装性能を示すものではない。実装環境の制約に応じた最適化により，性能が大きく異なる可能性に留意する必要がある。

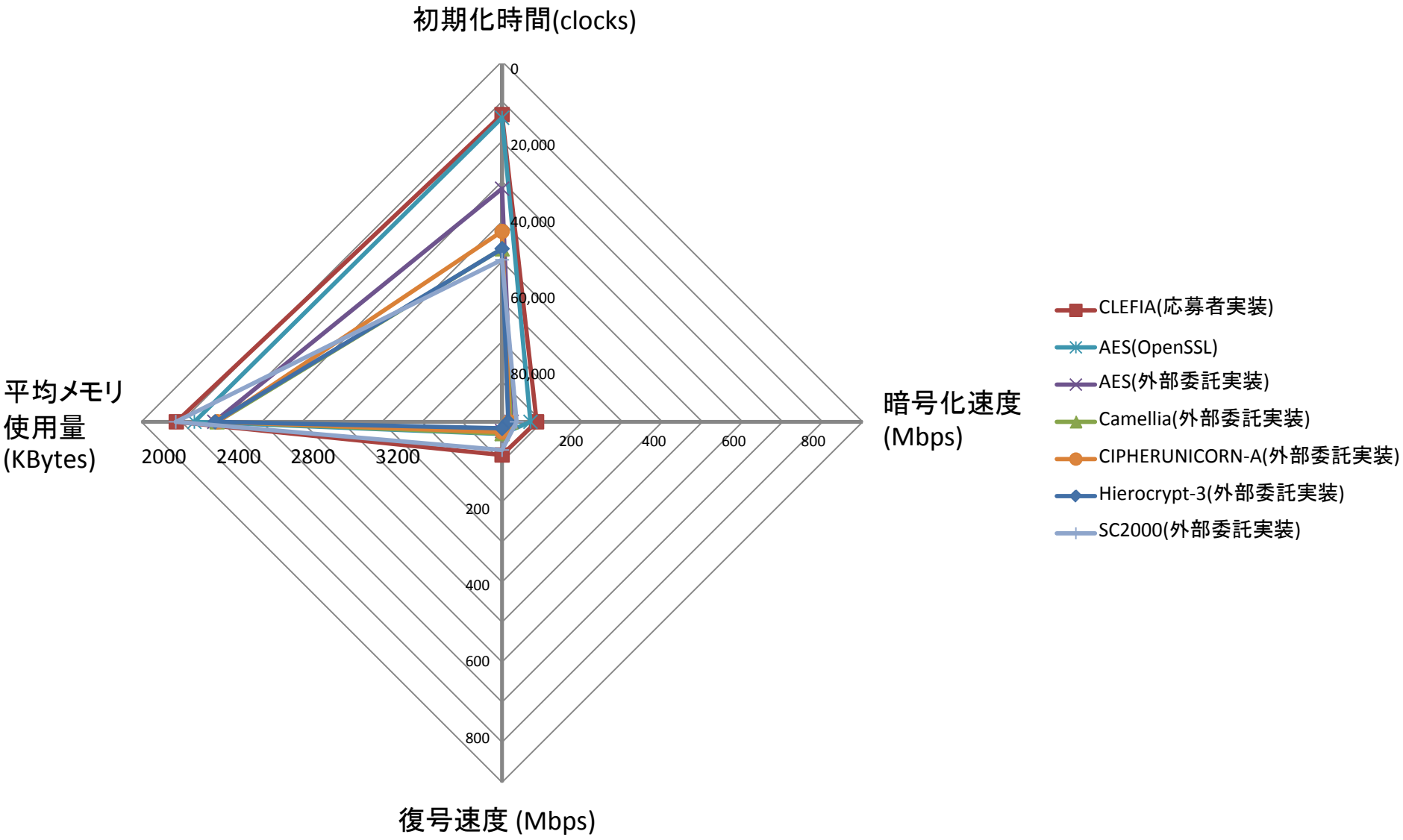
ハードウェア実装測定　－　暗号ごとの特記事項

④　Hierocrypt-3（外部委託実装）

著しく低い性能となっているが，この理由はVirtex-5（Xc5lxff324-3）の制約によるところが大きい。今回は，仕様に忠実に従った結果，線形変換の構成要素のリソースが非常に大きくなり，32ビット入出力処理を4組利用する128ビット処理が実現できなかった。そこで1組を4回繰り返すなどの対応を行ったところ，大幅なスループットの低下を招いた。

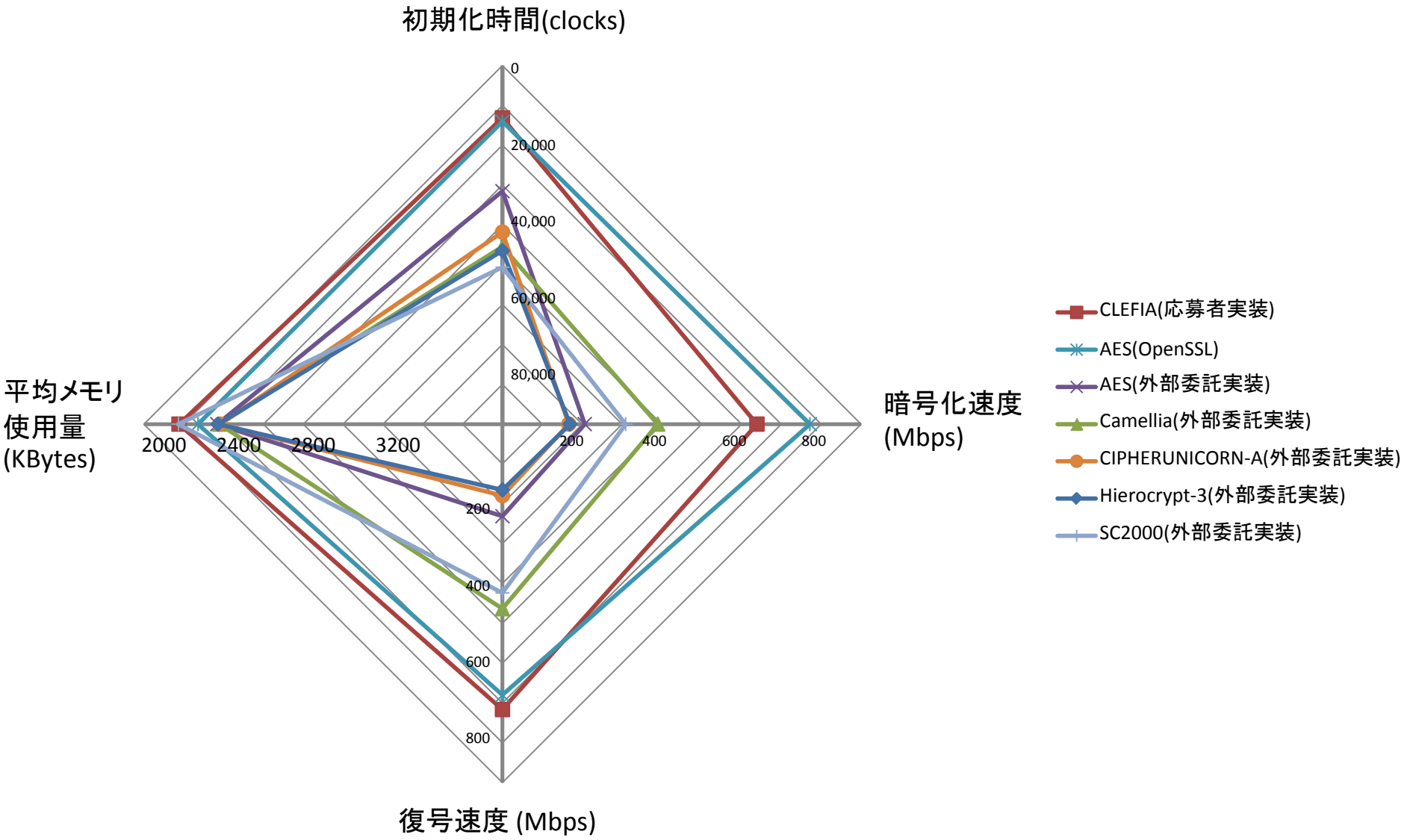
より大きなデバイスをターゲットにデータパスの最適化を行えば，性能の大幅な向上が可能である。また，今回の実装では独立にしているコンポーネントの共有化や実装ノウハウの利用によって，回路規模の大幅な縮小と大幅な性能向上も可能であると考えられる。

ブロック暗号（S/W,平文16バイト）



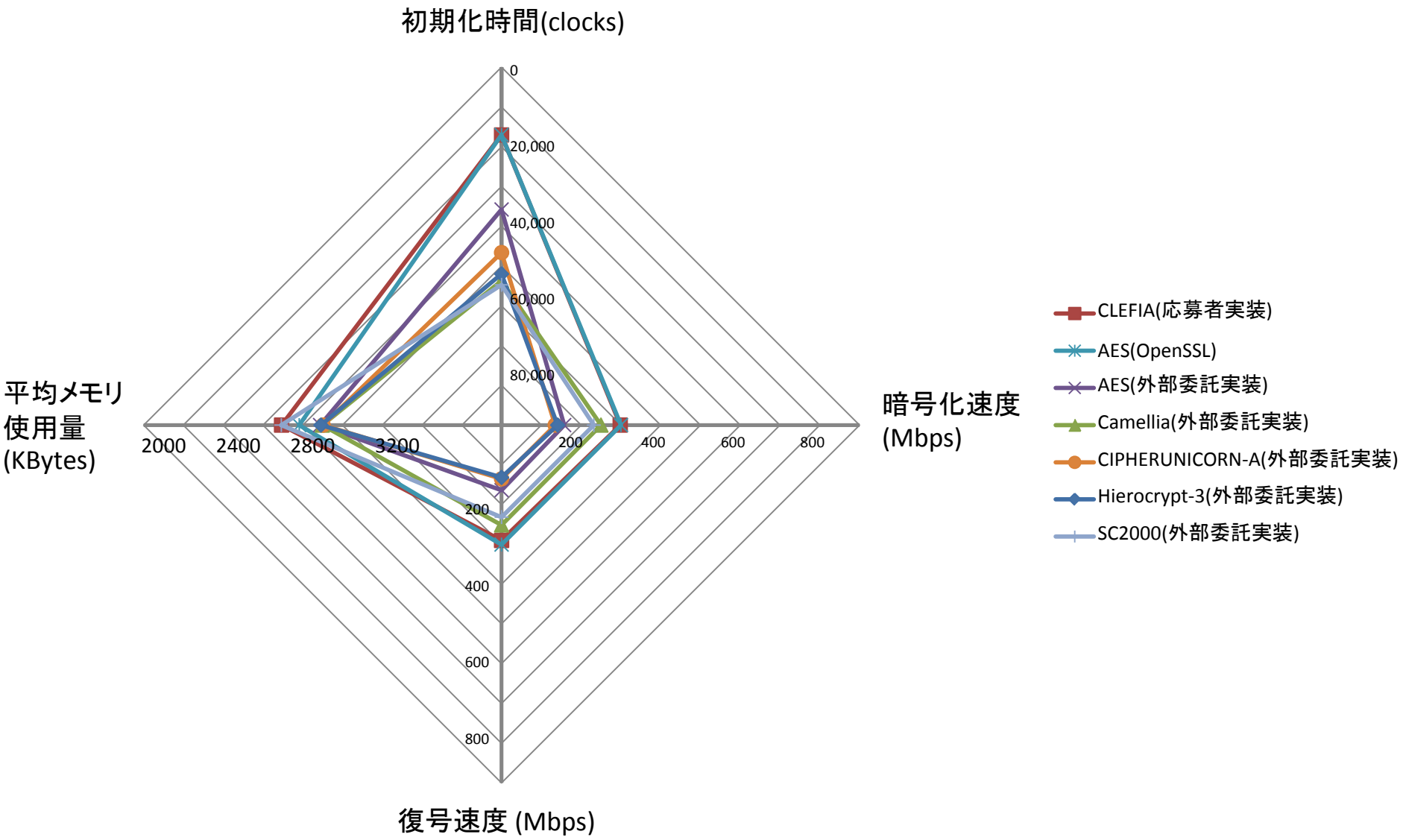
CRYPTREC
Cryptography Research and Evaluation Committees

ブロック暗号（S/W,平文1536バイト）



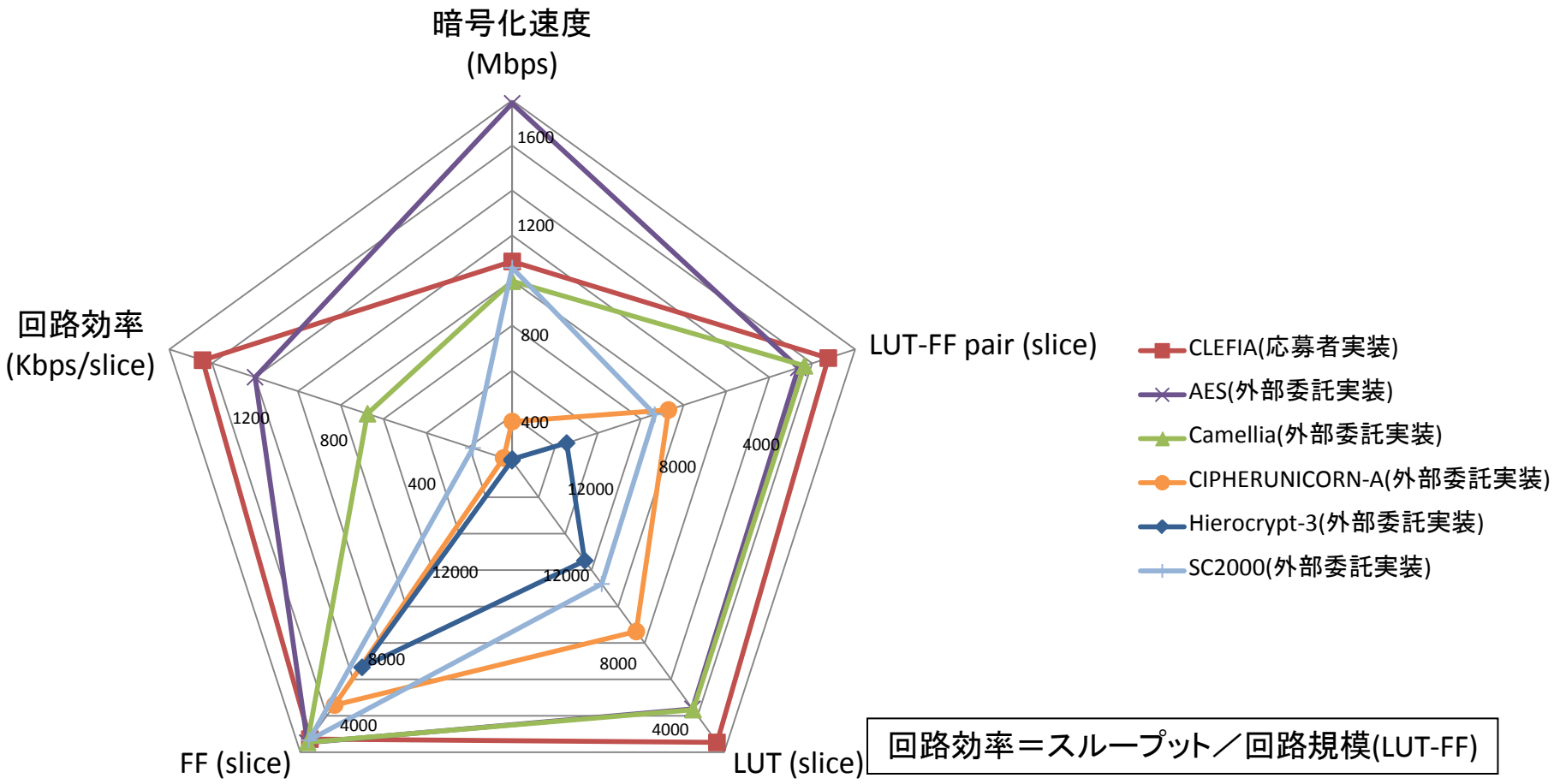
CRYPTREC
Cryptography Research and Evaluation Committees

ブロック暗号（S/W,平文1048576バイト）



CRYPTREC
Cryptography Research and Evaluation Committees

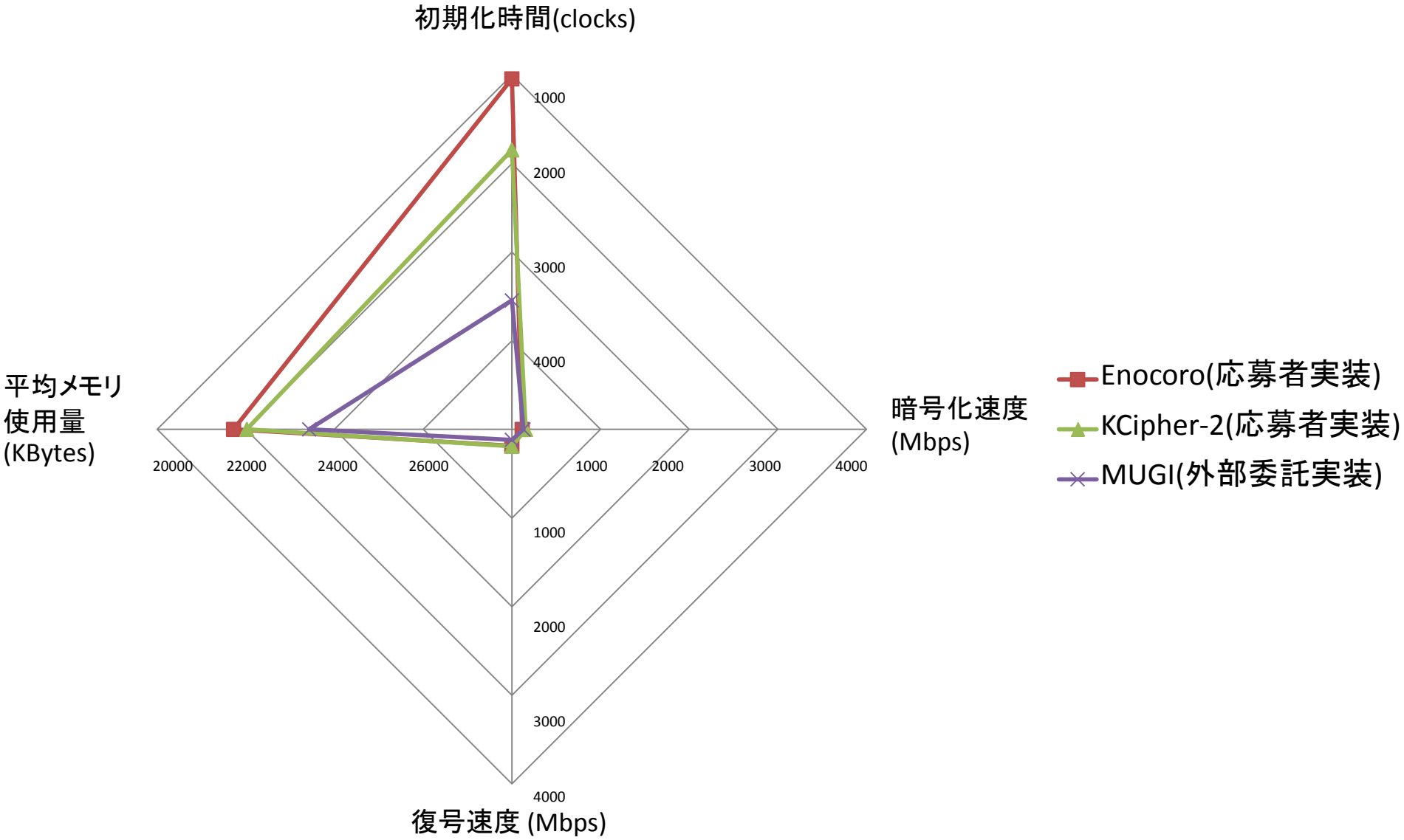
ブロック暗号（H/W）



回路効率＝スループット／回路規模(LUT-FF)

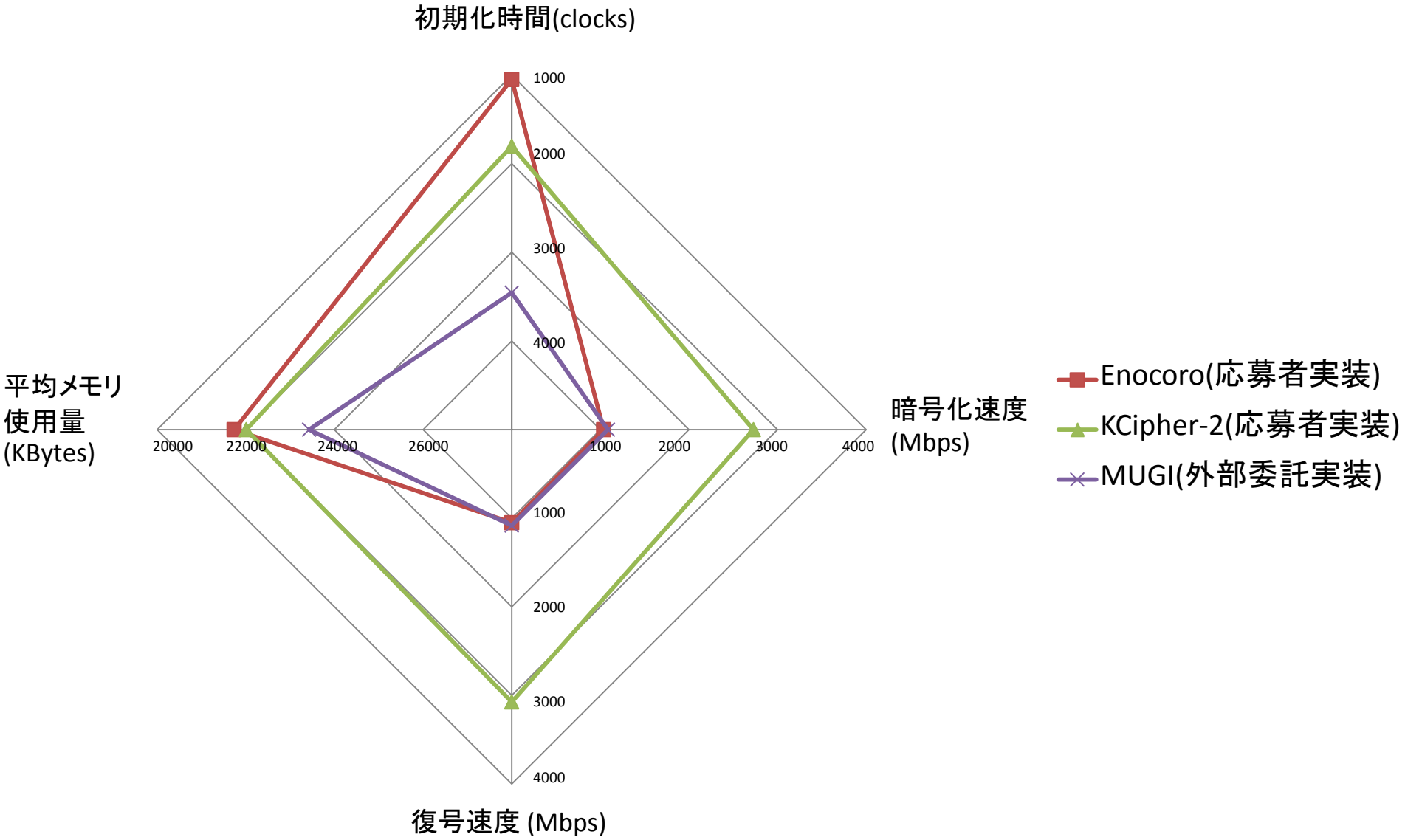
CRYPTREC
Cryptography Research and Evaluation Committees

ストリーム暗号（S/W,平文8バイト）



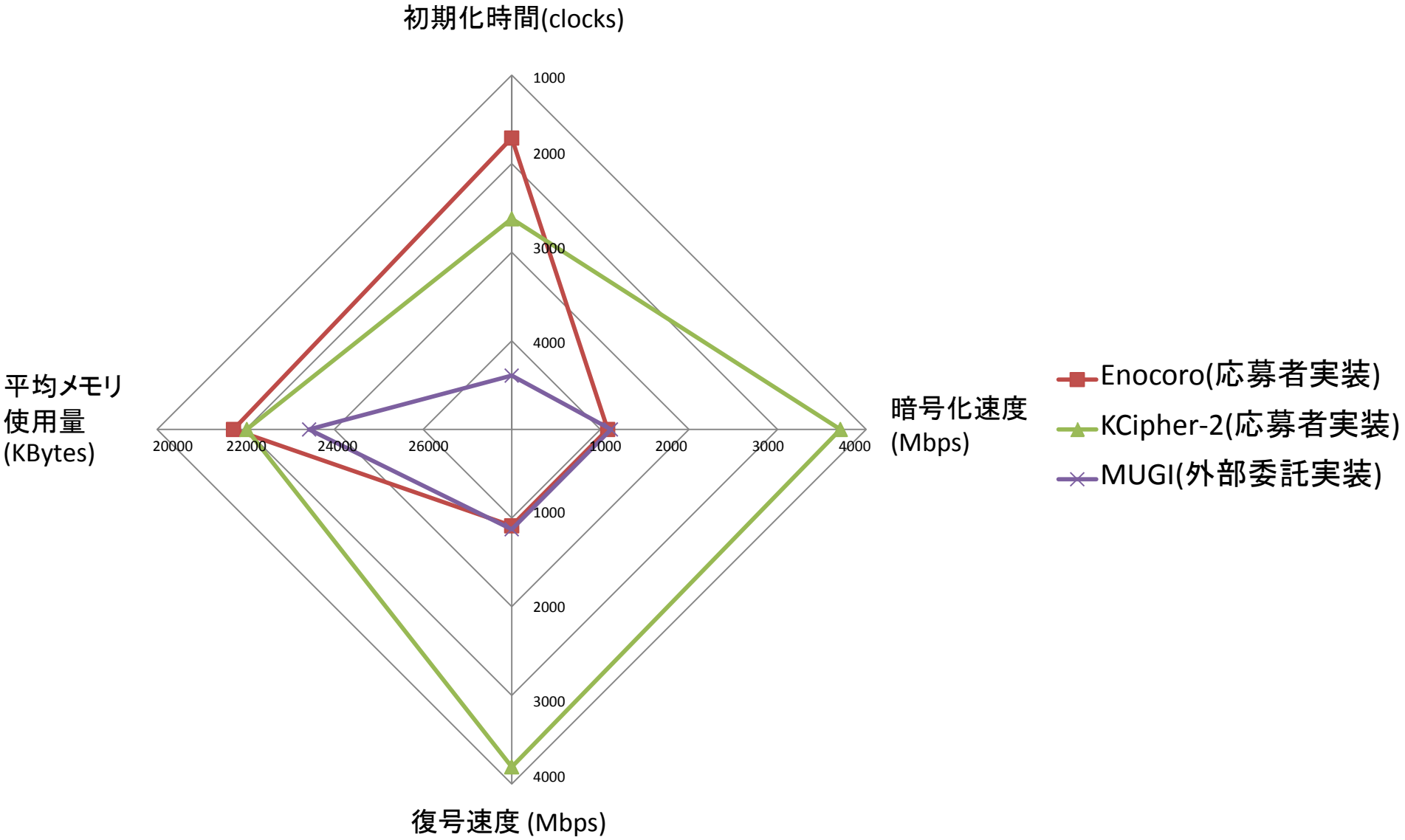
CRYPTREC
Cryptography Research and Evaluation Committees

ストリーム暗号（S/W,平文1536バイト）



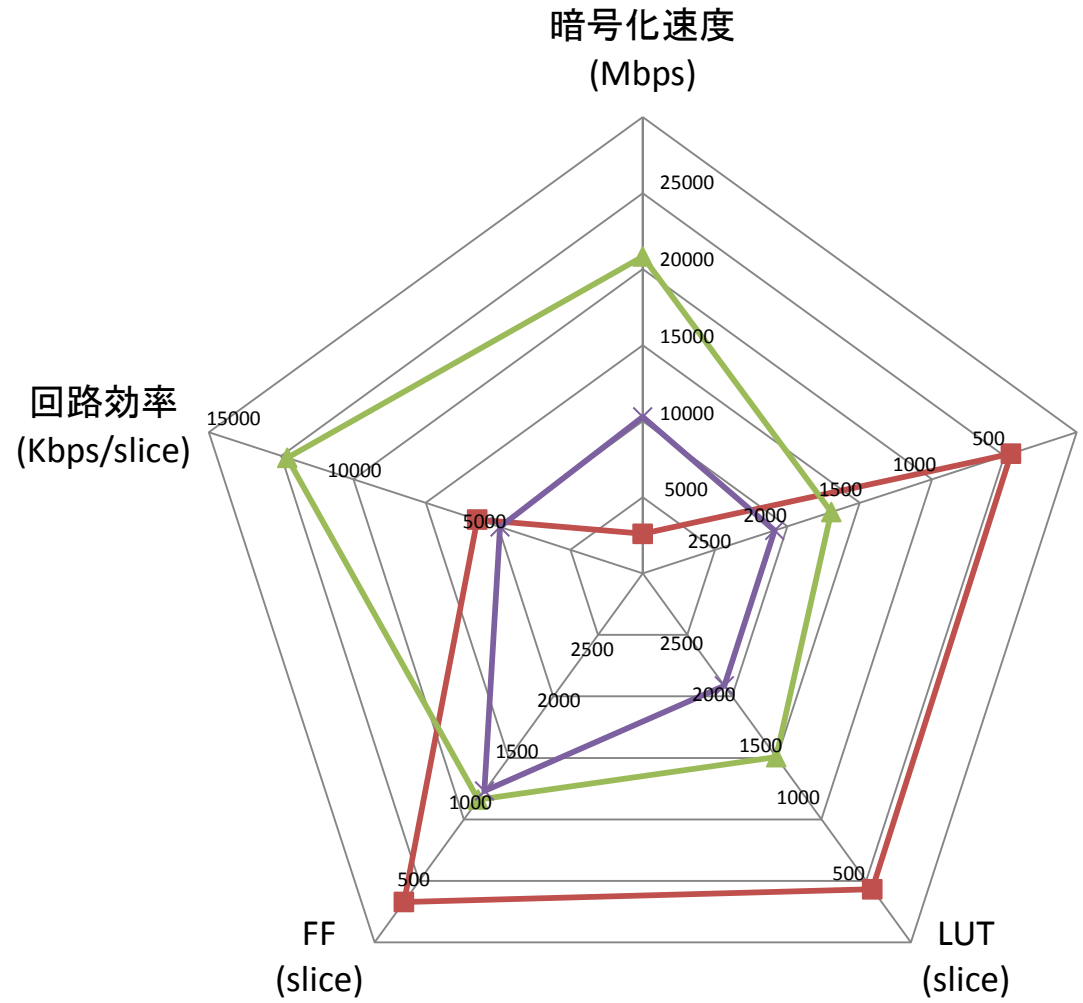
CRYPTREC
Cryptography Research and Evaluation Committees

ストリーム暗号（S/W,平文1048576バイト）



CRYPTREC
Cryptography Research and Evaluation Committees

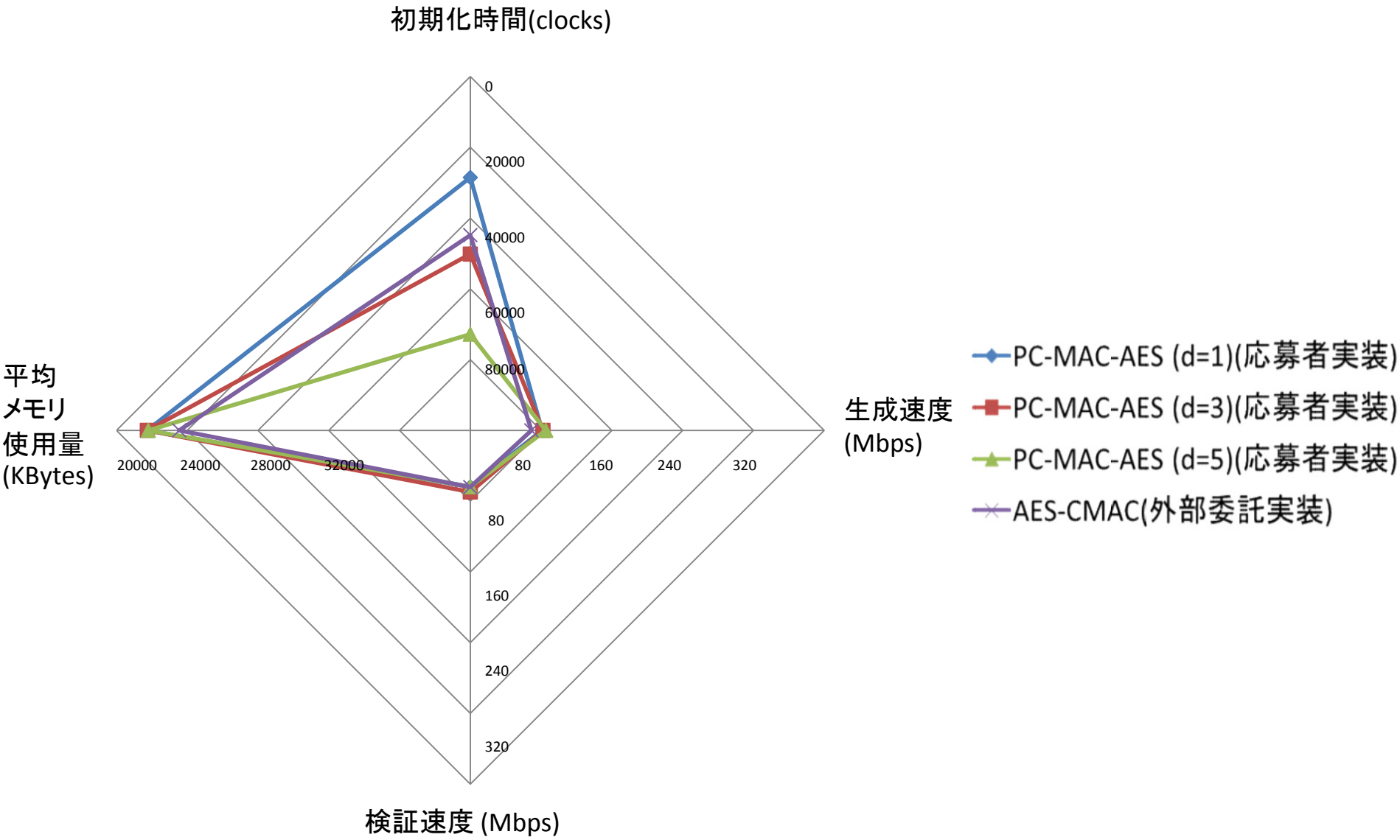
ストリーム暗号（H/W）



回路効率＝スループット／回路規模(LUT-FF)

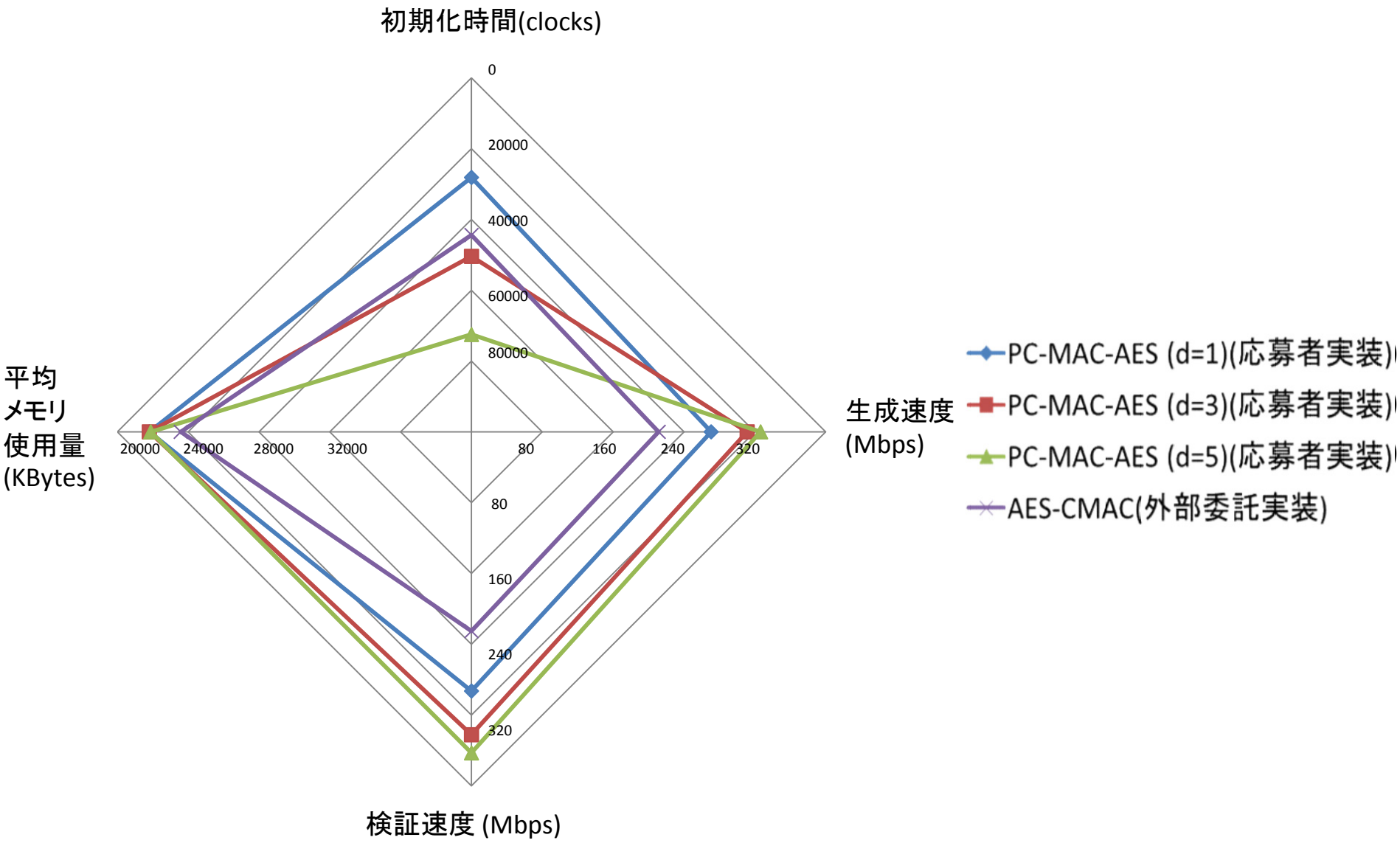
CRYPTREC
Cryptography Research and Evaluation Committees

MAC（S/W,平文16バイト）



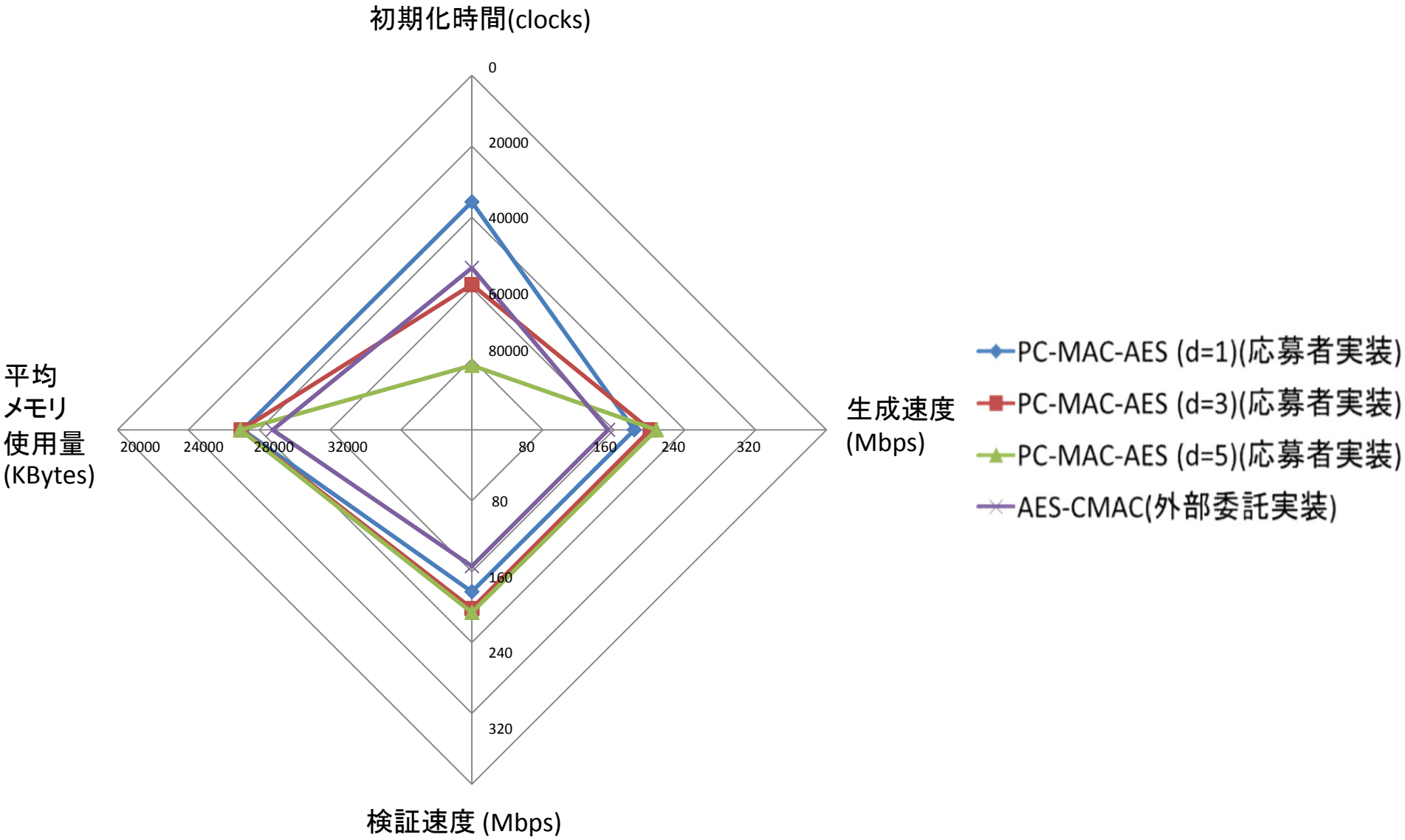
CRYPTREC
Cryptography Research and Evaluation Committees

MAC（S/W,平文1536バイト）



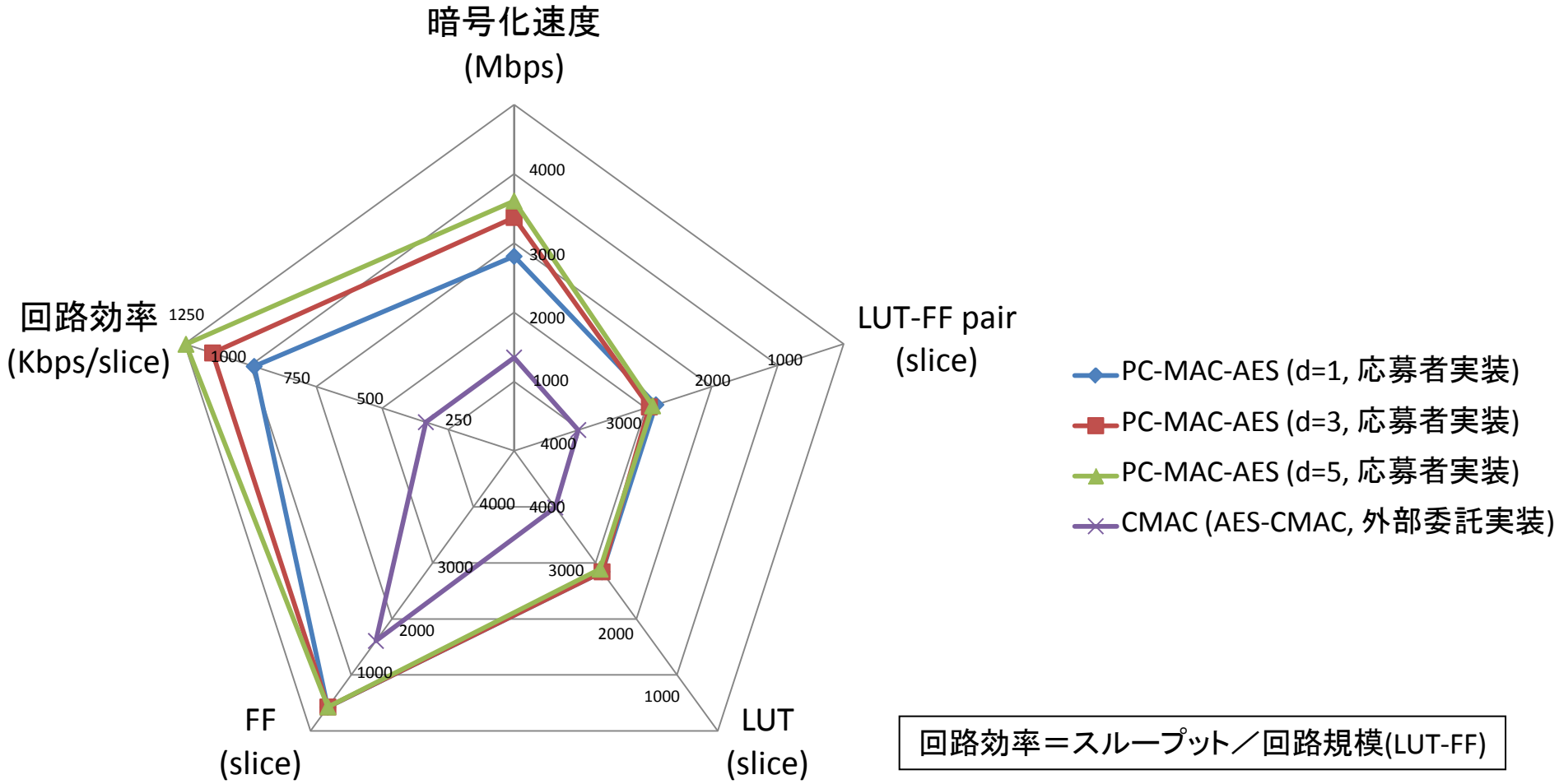
CRYPTREC
Cryptography Research and Evaluation Committees

MAC（S/W,平文1048576バイト）



CRYPTREC
Cryptography Research and Evaluation Committees

MAC（H/W）



回路効率＝スループット／回路規模(LUT-FF)

CRYPTREC
Cryptography Research and Evaluation Committees

サイドチャネル攻撃対策の有効性確認

新規応募暗号に対してサイドチャネル攻撃への対策が可能であることを確認（暗号リストの作成には利用せず）

① 新規応募暗号の共通鍵暗号3件

Enocoro-128v2, KCipher-2, CLEFIA

② SASEBO-GII上のH/W実装に対する電力解析

③ 実装は応募者

- ◆ 2種類（対策・未対策）の実装と関連情報を提出
  - ➢ アーキテクチャは共通
    - – 対策版（対策実装），未対策版（素朴実装）
  - ➢ 攻撃対象と選択関数

④ 事務局が測定・解析

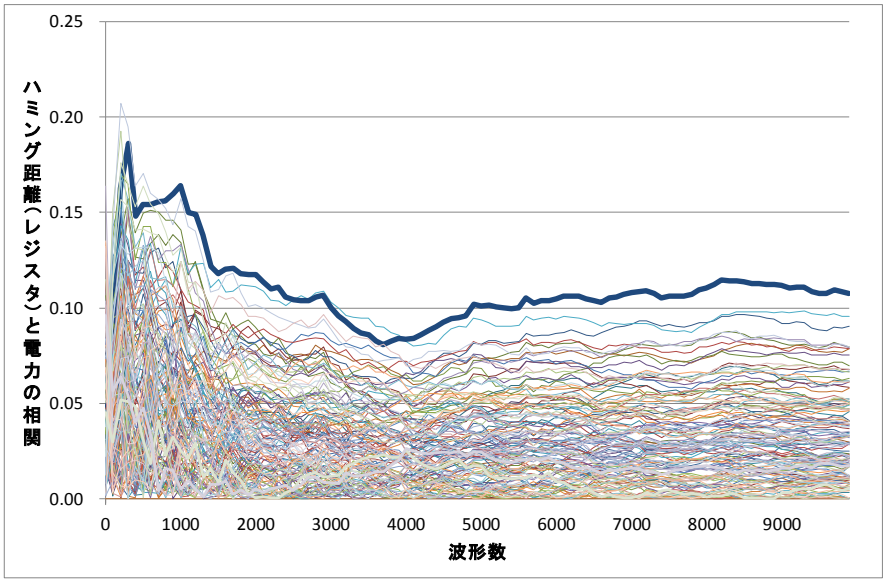
◆対策版が未対策版より攻撃が困難となることを確認する

サイドチャネル攻撃対策の有効性確認

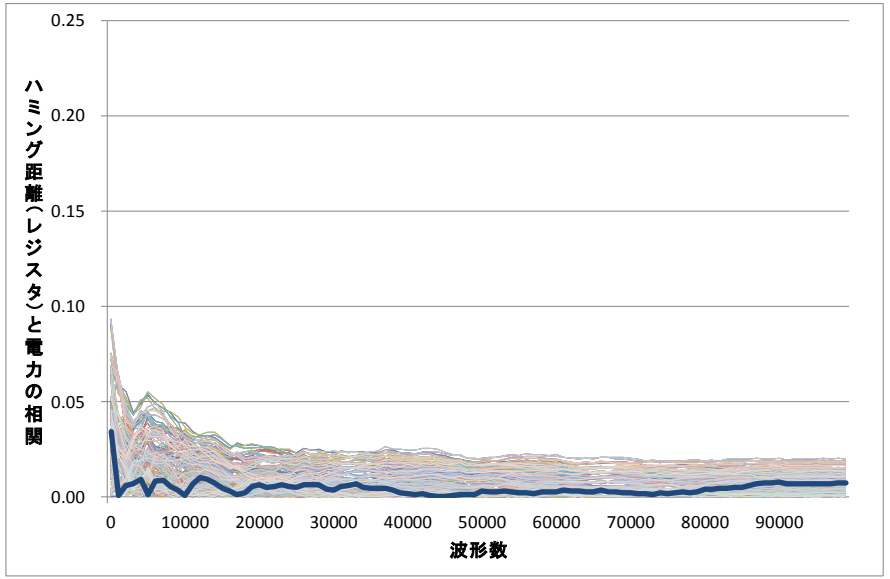
- 攻撃内容
  - ◆応募者により提示された攻撃対象と選択関数を使用
  - ◆相関電力解析(CPA)の適用
    - ハミング距離の使用
    - 未対策版は1万波形，対策版は10万波形を使用

- 結果
  - ◆3件の新規応募暗号全てで対策の有効性を確認

CPAの結果：Enocoro-128v2



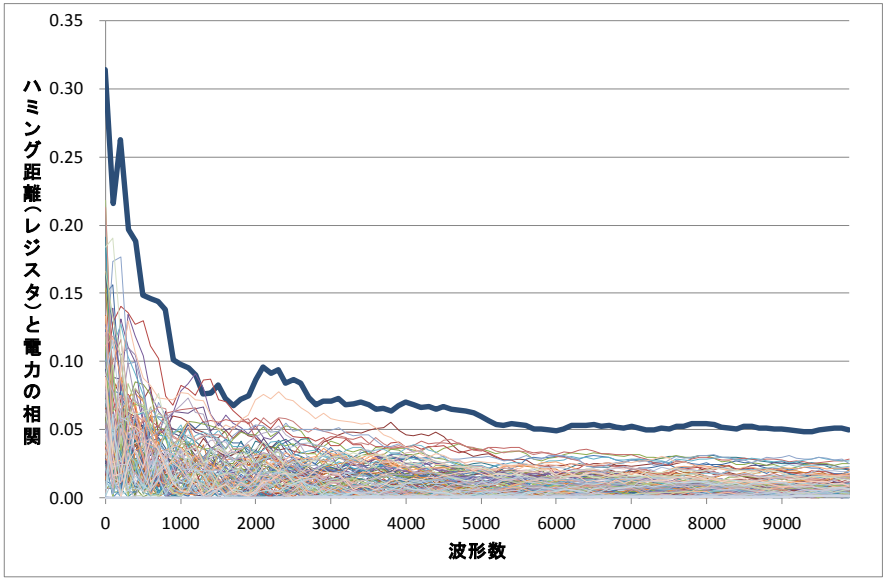
未対策版（素朴実装）



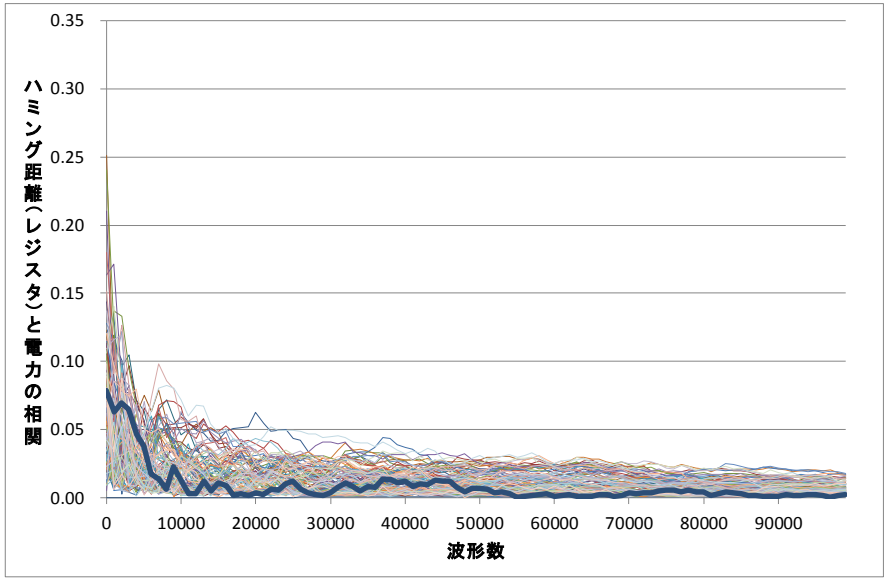
対策版（対策実装）

CRYPTREC
Cryptography Research and Evaluation Committees

CPAの結果：KCipher-2



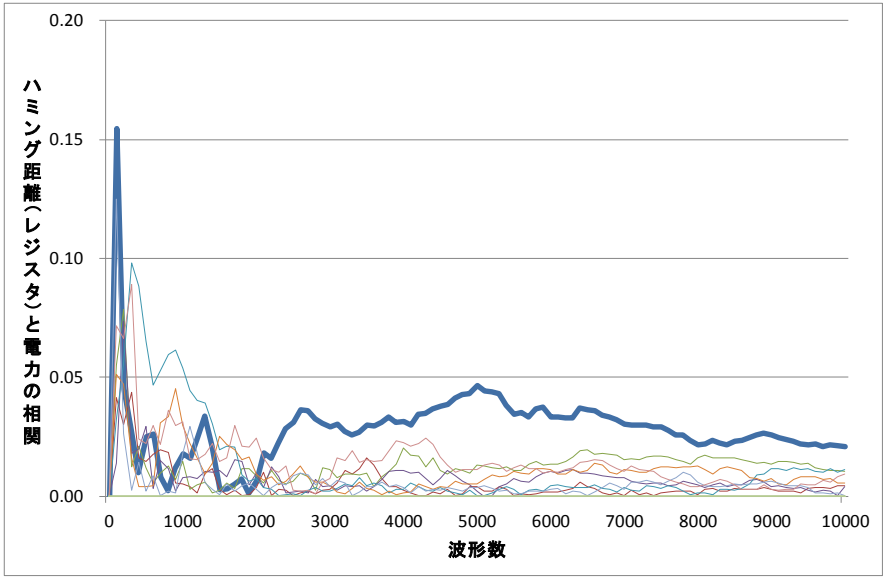
未対策版（素朴実装）



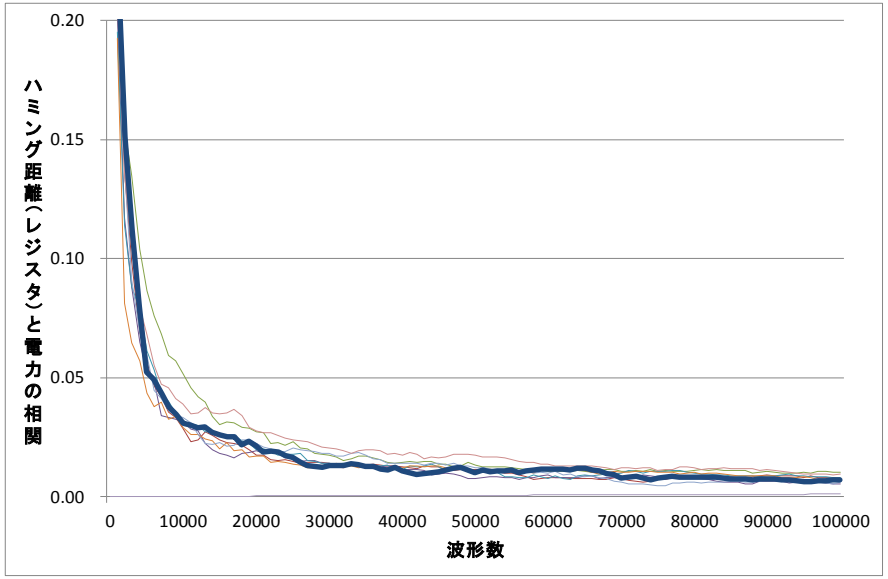
対策版（対策実装）

CRYPTREC
Cryptography Research and Evaluation Committees

CPAの結果：CLEFIA



未対策版（素朴実装）



対策版（対策実装）

CRYPTREC
Cryptography Research and Evaluation Committees