実装性能評価結果

目次

1. はじめに

- 【安全性評価・実装評価】の目的
  推奨候補暗号としての十分な安全性・実装性能の有無を判定する。

- 評価対象暗号の分類
  （現）現リスト掲載暗号
  （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。

  以下、判定結果を示した後、評価及び判定について記す。

2. 公開鍵暗号の判定結果

〇は第一次選定（評価A・B）の対象とすることを示す

技術分類	暗号技術名	分類	判定
署名	DSA	現	〇
	ECDSA	現	〇
	RSASSA-PKCS-v1_5	現	〇
	RSA-PSS	現	〇
守秘	RSA-OAEP	現	〇
	RSAES-PKCS1-v1_5	現	〇
鍵共有	DH	現	〇
	ECDH	現	〇
	PSEC-KEM	現	〇

2. 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

技術分類	暗号技術名	分類	判定
64ビットブロック暗号	CIPHERUNICORN-E	現	○
	Hierocrypt-L1	現	○
	MISTY1	現	○
	3-key Triple DES	現	○
128ビットブロック暗号	**CLEFIA**	新	○
	AES	現	○
	Camellia	現	○
	CIPHERUNICORN-A	現	○
	Hierocrypt-3	現	○
	SC2000	現	○
ストリーム暗号	**Enocoro-128v2**	新	○
	KCipher-2	新	○
	MUGI	現	○
	MULTI-S01	現	○
	128-bit RC4	現	○

2. 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

技術分類	暗号技術名	分類	判定
ハッシュ関数	RIPEMD-160	現	○
	SHA-1	現	○
	SHA-256	現	○
	SHA-384	現	○
	SHA-512	現	○
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	○

3. 各分類に対する判定

- 現リスト掲載暗号の判定（現）
  前回公募・選考時(2000-2002年度)に十分な実装性能を確認済み。

- 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、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）
  公募要項で現リスト掲載暗号に対する同等以上の特長（安全性又は実装性）が要求されており、実装性能で検証する必要があった。
  実装評価を実施した結果、全暗号についてこの条件を満たすことが確認できた。以下で具体的内容について示す。

4. 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
同じ技術分類の現リスト掲載暗号を比較対象とする。

② メッセージ認証コード
事務局選出暗号の代表としてCMAC（ブロック暗号にAESを使用）を比較対象とする。

技術分類	評価対象暗号	比較対象暗号	
	新規応募暗号	現リスト掲載暗号	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

5. 新規応募暗号評価の基本方針と概要

実装評価は次の基本方針に従って実施した。

A)　評価環境は電子政府における利用を念頭に選択する。

B)　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

- 個々の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

A) ソフトウェア実装評価

- 独自のWindows PCを対象とする評価ツールを利用する。
- 評価は高速実装を対象とする。

B) ハードウェア実装評価

- 独自のFPGAを対象とする評価環境を利用する。
- 評価は高速実装を対象とする。
- サイドチャネル攻撃対策可能性も同環境で評価するが、本判定の対象外。

③ 複数の実装を提出した暗号の扱い

- ハードウェア実装でのROM,RAMの利用が最も少ないものを対象とする。
- 安全性パラメータの違う複数の実装では、全実装が揃って優位な場合のみ優位性を認める。

6. ソフトウェア実装評価　－　評価方法

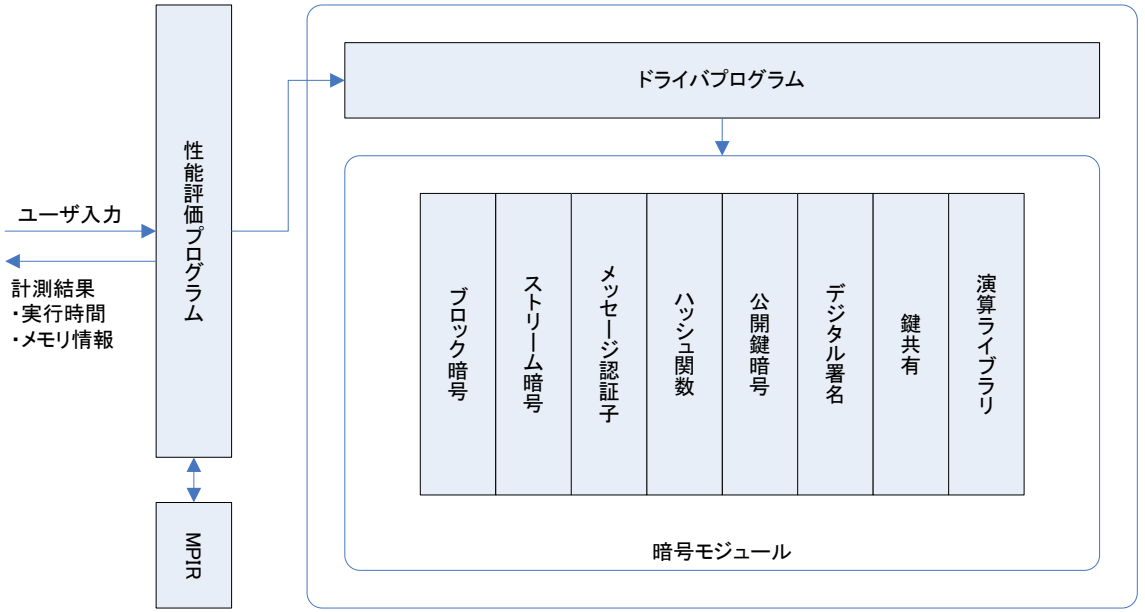
ソフトウェア性能評価ツール＊

・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
　・実行クロック数
　・メモリサイズ

現リスト掲載暗号（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



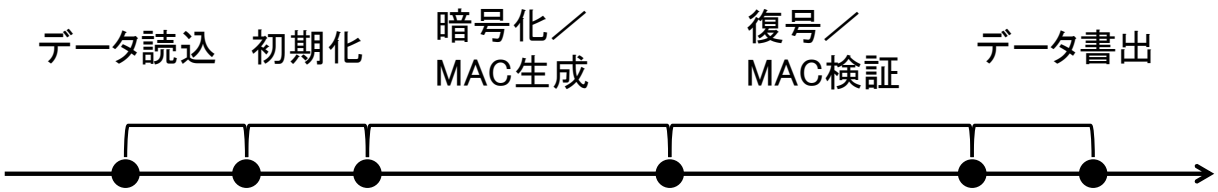
評価ツールの全体構成

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

6. ソフトウェア実装測定　－　評価方法

測定の概要

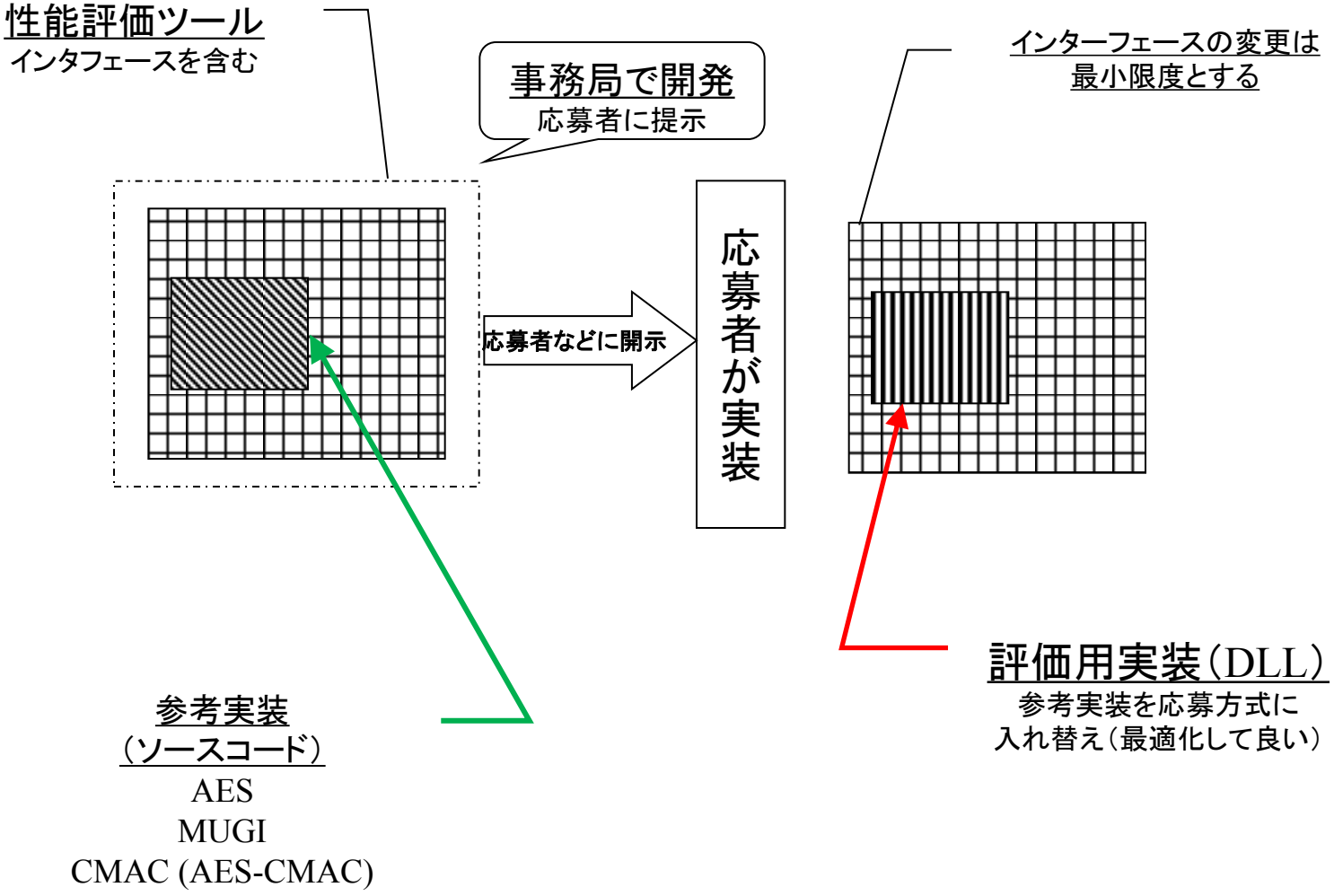
このツールでは、暗号モジュールで各イベントに掛かったクロック数を測定する。



具体的には上図に示すように、データ読込、初期化、暗号化(MAC生成)、復号(MAC検証)、データ書出に掛る時間を測定し、次の測定値を出力する。

- 初期化時間
- 暗号化速度 （メッセージ認証コードでは、「MAC生成速度」）
- 復号速度　 （メッセージ認証コードでは、「MAC検証速度」）
- 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

6. ソフトウェア実装測定　－　応募者の実装方法



6. ソフトウェア実装測定　－　データを読む際の注意事項

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、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。

6. ソフトウェア実装測定　－　データの測定法

128回測定した最小値を3回集め、その平均値を測定値とする

最小値を採用した理由
- 他プロセスの影響が小さいと考えられるため。

128回を3回とした理由
- 前回の公募・評価時（2000-2年度）では、128回の平均値を3個表示した。

6. 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たので、同手法が利用されているOpenSSLのソースコードを利用した実装も比較対象に加えた。

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き換えた。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おり、暗号化開始時に拡大鍵がキャッシュヒットするのに対し、復号開始時には拡大鍵がキャッシュヒットせず、ハードディスクから呼び出すオーバーヘッドが生じるためと推定できる。
この推定は、暗号化と復号の拡大鍵が共通であるFeistel型のブロック暗号で、暗号化と復号の速度に大きな差が見られないことと整合する。

7. ハードウェア実装評価　ー　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）
- 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)
- 状態の初期化に掛かるクロック数

7. ハードウェア実装性評価　ーデータを読む際の注意事項

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
  → 十分な最適化を行ったと想定される。

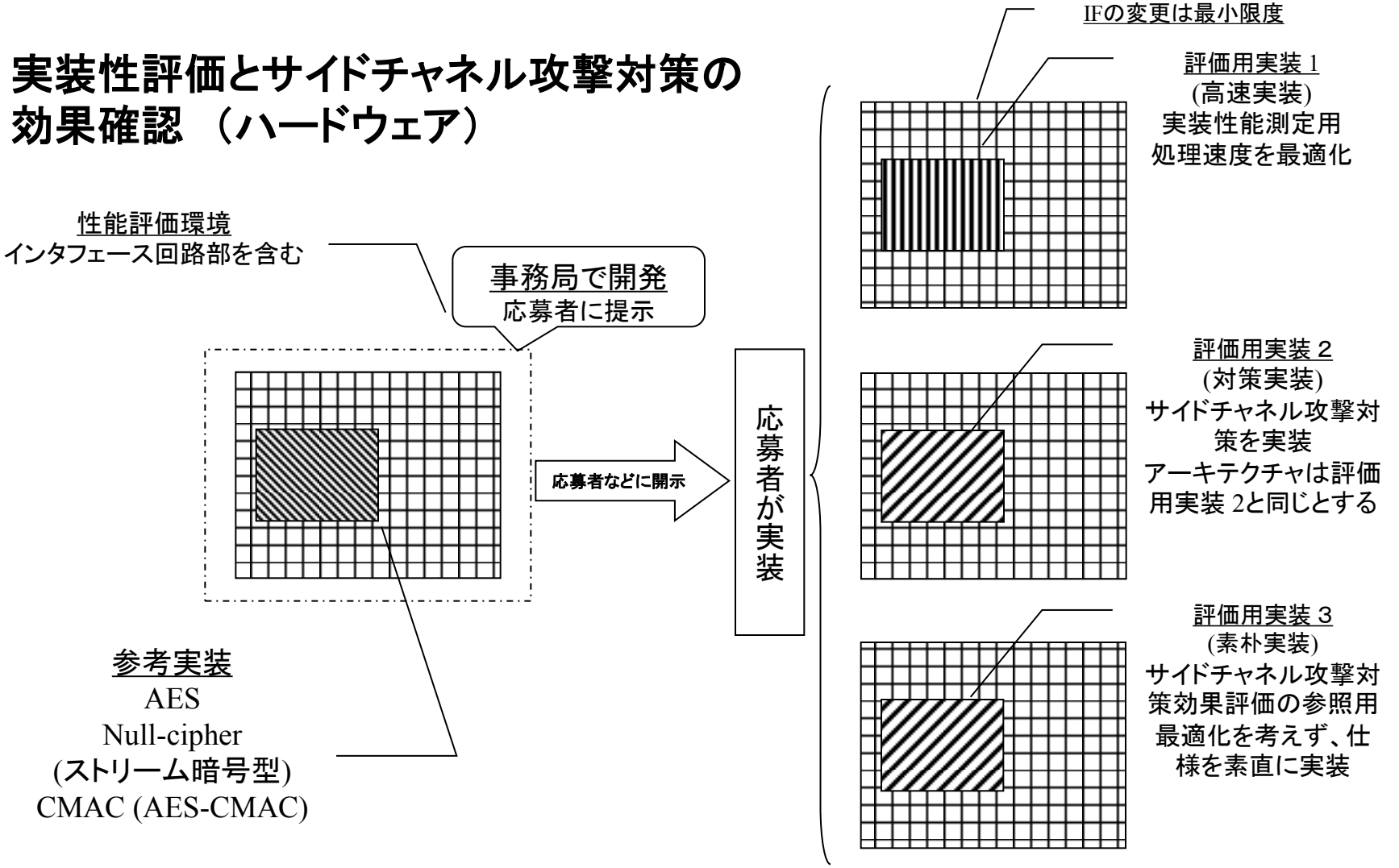
- 現リスト掲載暗号は評価ツール開発者（第三者）が実装
  → 仕様に忠実な実装であり、特別な最適化は実施していない。

② ー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。

7. ハードウェア実装性能評価 ー 応募者による実装開発

実装性評価とサイドチャネル攻撃対策の効果確認 （ハードウェア）



サイドチャネル攻撃対策は本評価の対象外

7. ハードウェア実装測定　－　暗号ごとの特記事項

① CLEFIA（応募者実装）
高速実装は次の3種類が提出された。
A） S-boxと4x4行列をLUTで実装
B） S-boxをROMで実装(256 bytes ＊ 8 = 2 Kbytes)、4x4行列はLUT
C） S-boxと4x4行列を合成してROMで実装(1 Kbites ＊ 8 = 8Kbytes)
性能比較にはA)を利用した。

② Enocoro-128v2（応募者実装）
特になし。

③ KCipher-2（応募者実装）
S-boxはROMで実装した。

④ PC-MAC-AES（応募者実装）
デフォルトオプションを使った結果、144KBのブロックRAMが使用された。

⑤ 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く、実装するデバイスや求められる回路規模や動作速度などの様々な制約に応じた最適化により、性能が大きく異なって示される可能性に留意する必要がある。

7. ハードウェア実装測定　－　暗号ごとの特記事項

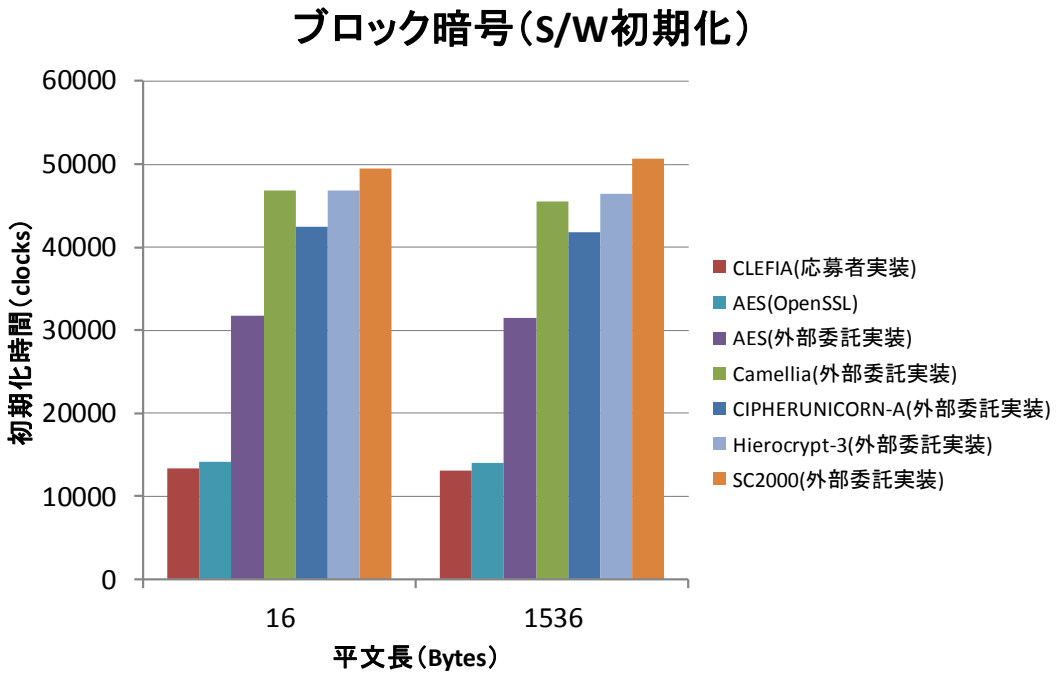
⑥　Hierocrypt-3（外部委託実装）
著しく低い性能となっているが、この理由はVirtex-5（Xc5lxff324-3）の制約によるところが大きい。今回は、実装ノウハウの利用は最小限に留め、仕様に忠実に従った結果、線形変換の構成要素のリソースが非常に大きくなり、32ビット入出力処理を4組利用する128ビット処理が実現できなかった。そこで1組を4回繰り返すなどの対応を行ったところ、大幅なスループットの低下を招いた。より大きなデバイスをターゲットにデータパスの最適化を行えば、性能の大幅な向上が可能である。また、今回の実装では独立にしているコンポーネントの共有化や実装ノウハウの利用によって、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。

8. 評価結果

新規応募暗号が比較対象暗号より優れていると認められた評価項目とそれを裏付けるデータの一例（棒グラフ）を次以降に示す。

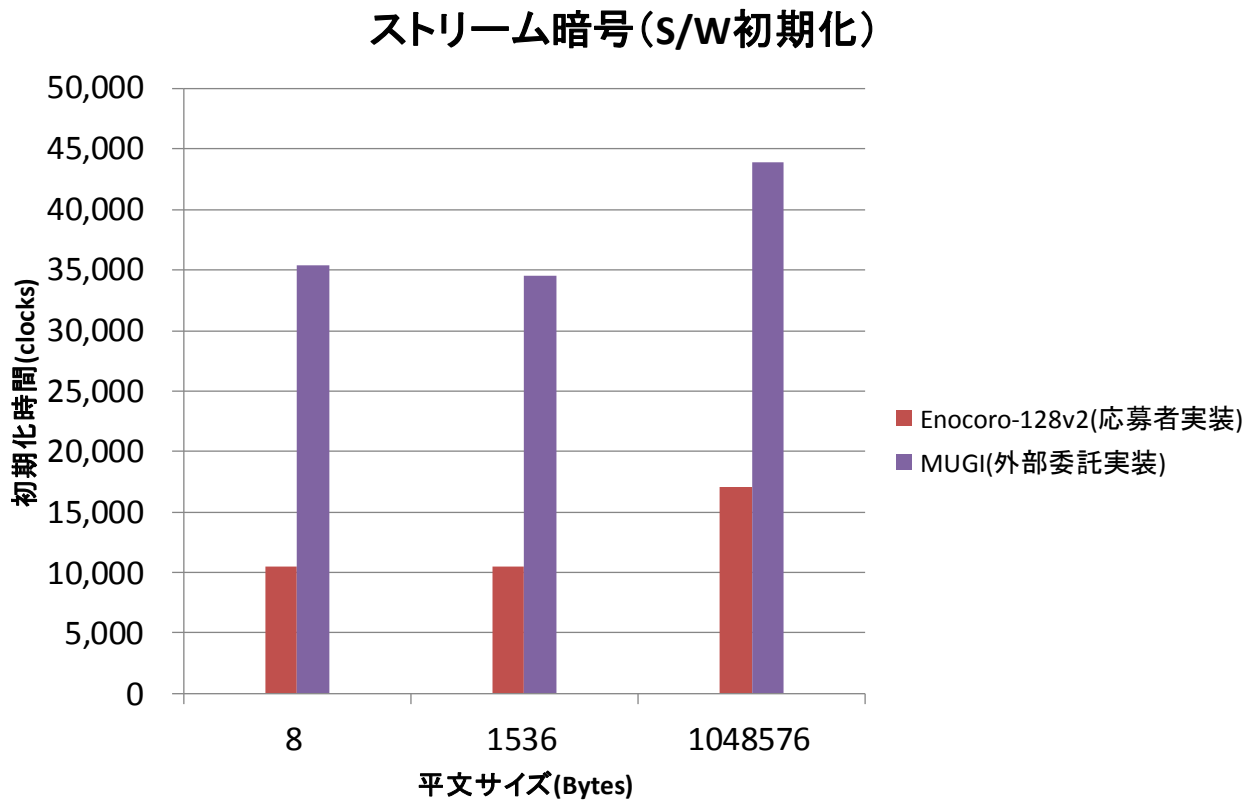
優位性が認められる項目（CLEFIA）

ソフトウェア実装：
　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)
ハードウェア実装：
　回路規模（LUT-FF pair）



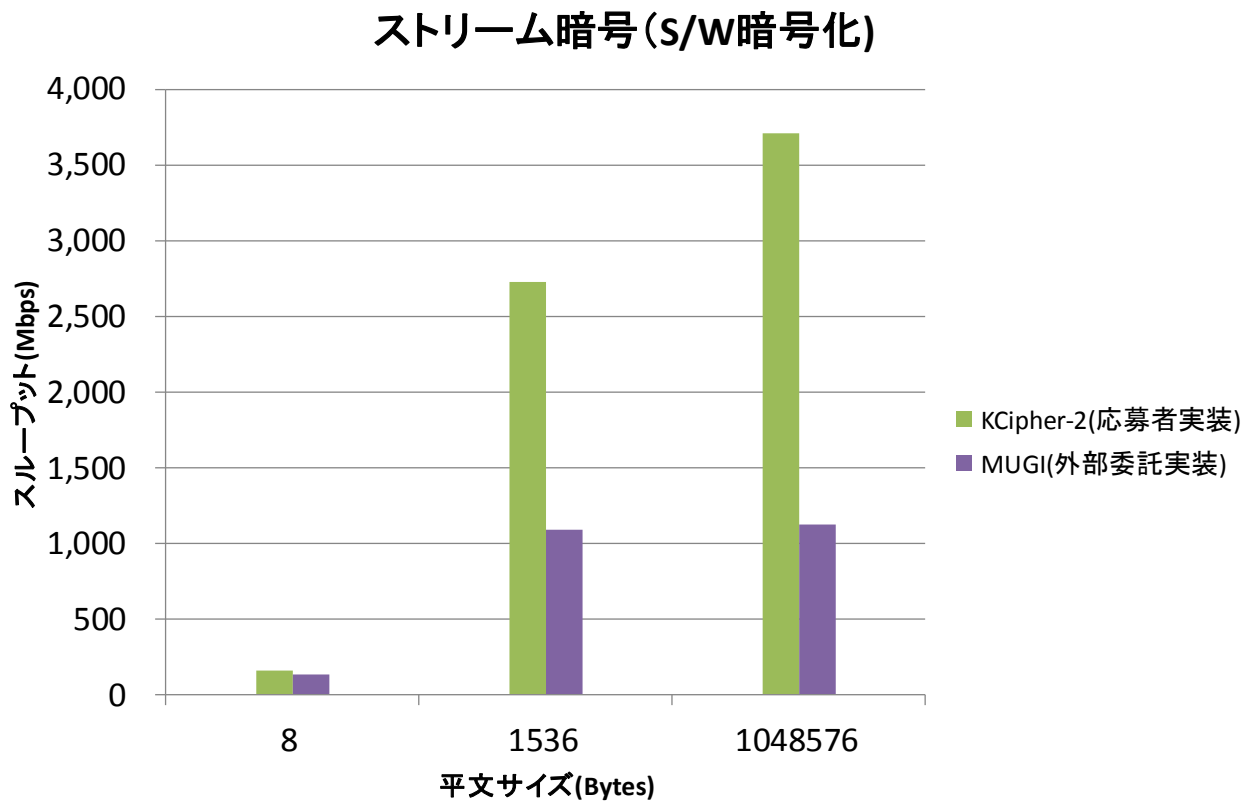
優位性が認められる項目（Enocoro-128v2）

ソフトウェア実装：
　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）
ハードウェア実装：
　回路規模（LUT-FF pair）



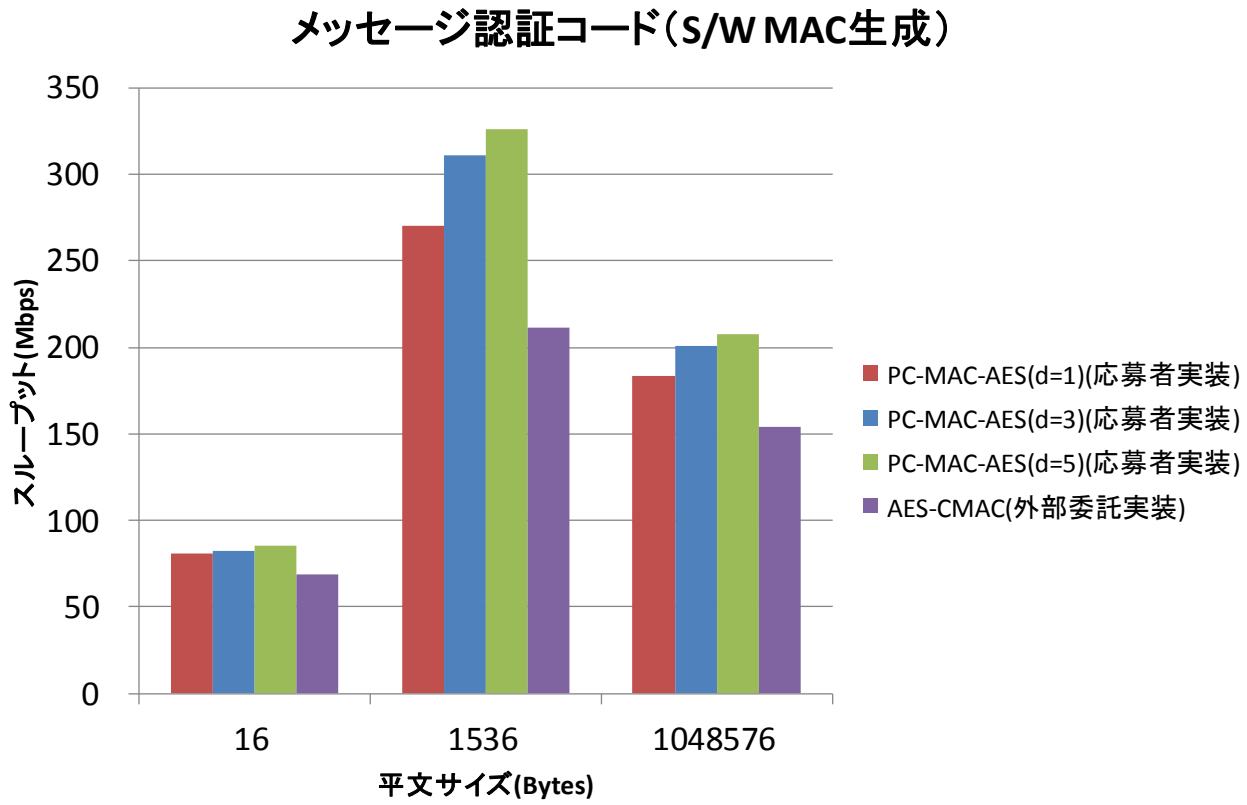
優位性が認められる項目（KCipher-2）

ソフトウェア実装：
　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）
ハードウェア実装：
　暗号化スループット，回路効率



優位性が認められる項目（PC-MAC-AES）

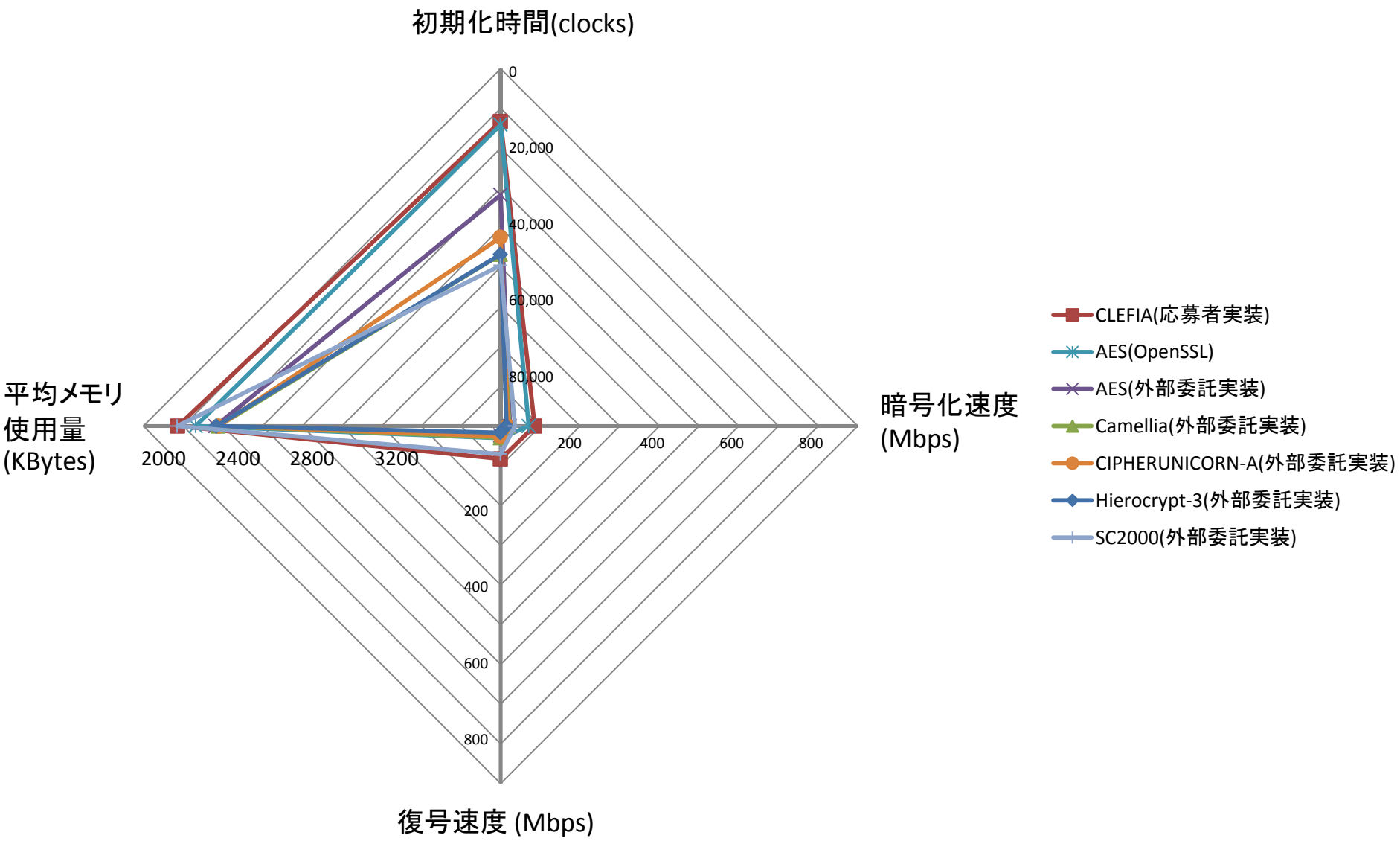
ソフトウェア実装：
　MAC生成速度（全平文長），
　MAC検証速度(1536バイト, 1048576バイト)，メモリ使用量（全平文長）
ハードウェア実装：
　暗号化スループット，回路規模（LUT-FF pair），回路効率



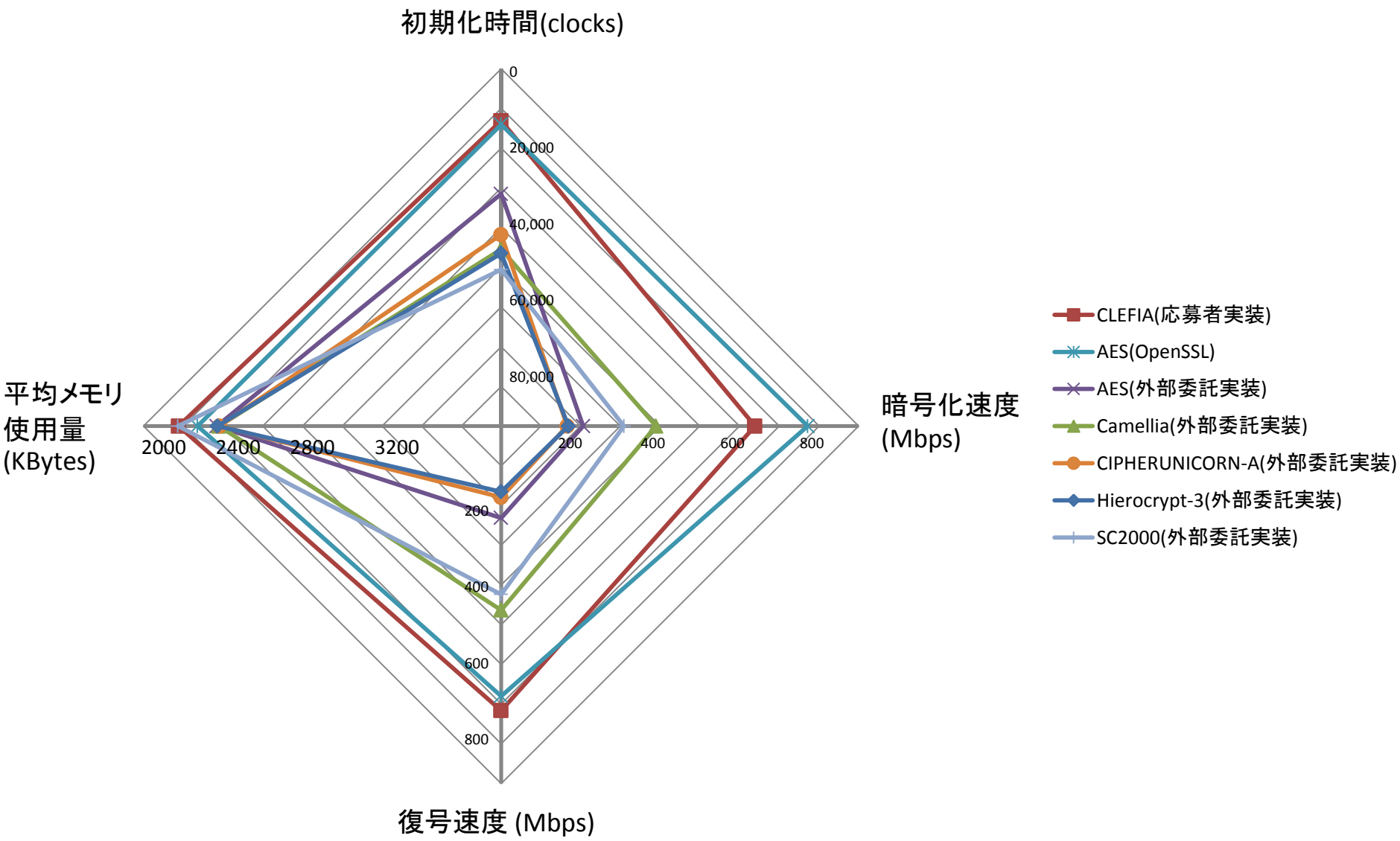
9. レーダーチャートによる測定結果の表示（参考）

今回測定した全項目のデータをレーダーチャートで次以降に示す。

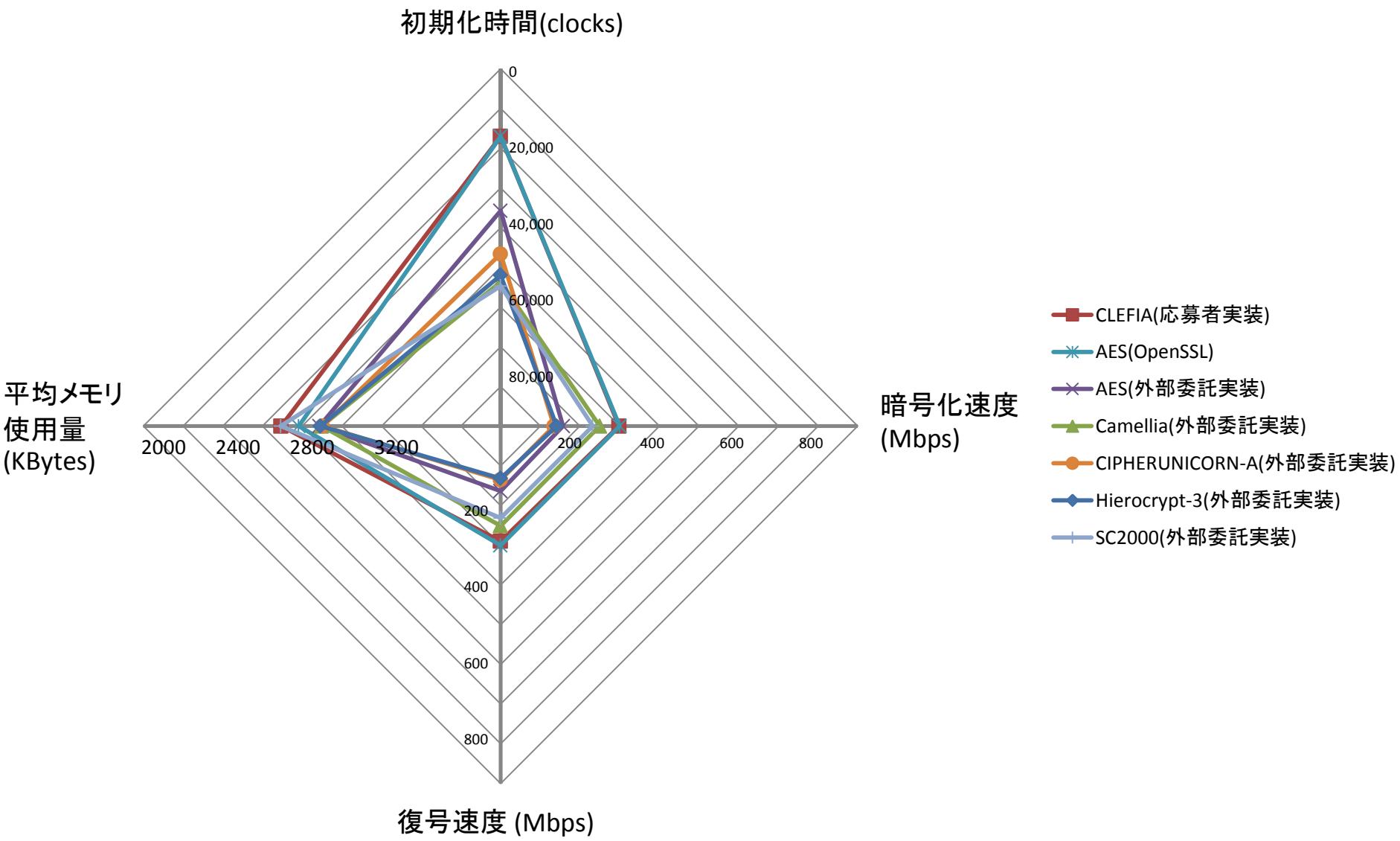
ブロック暗号（S/W, 平文16バイト）



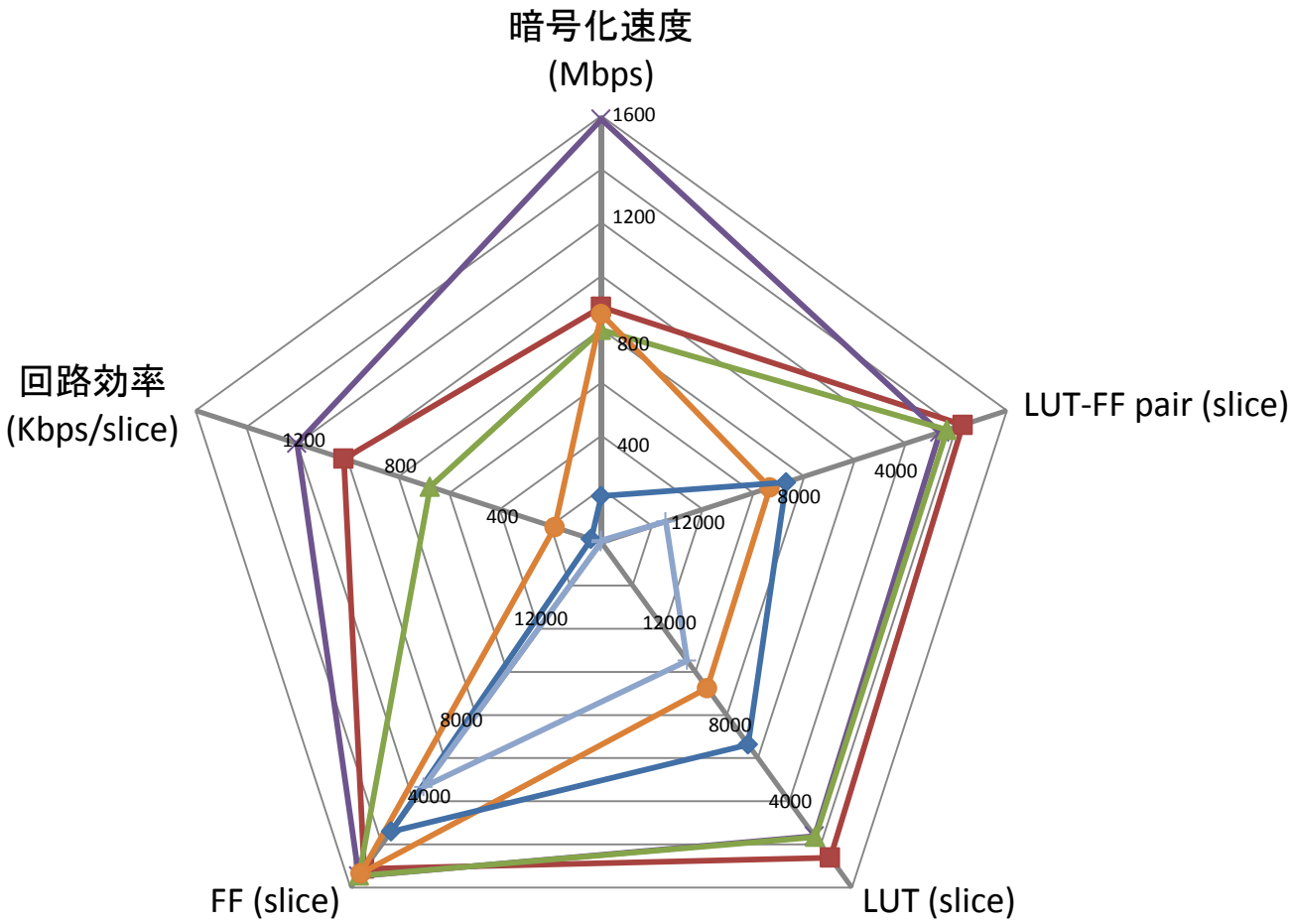
ブロック暗号（S/W, 平文1536バイト）



ブロック暗号（S/W, 平文1048576バイト）

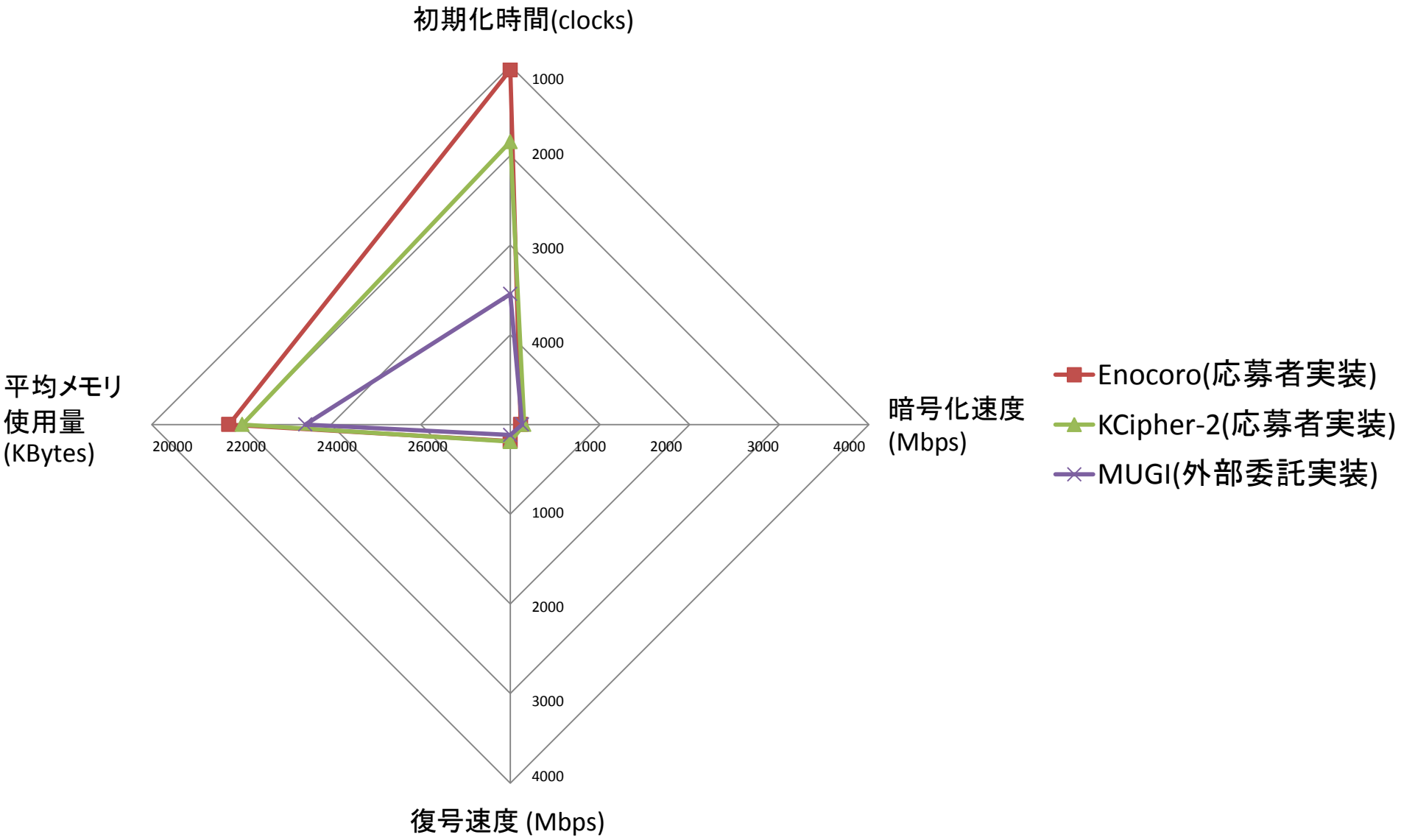


ブロック暗号（H/W）

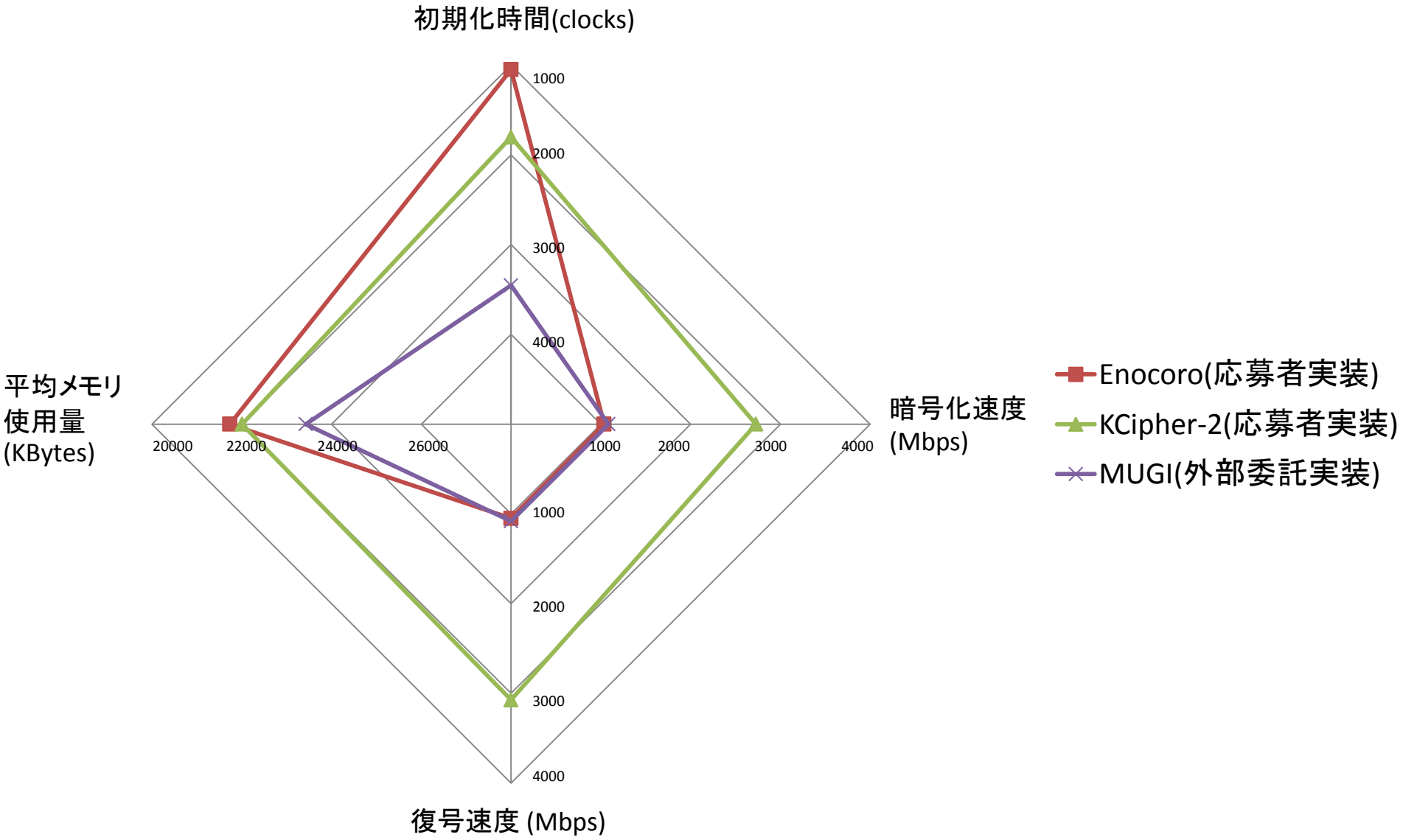


回路効率＝スループット／回路規模(LUT-FF)

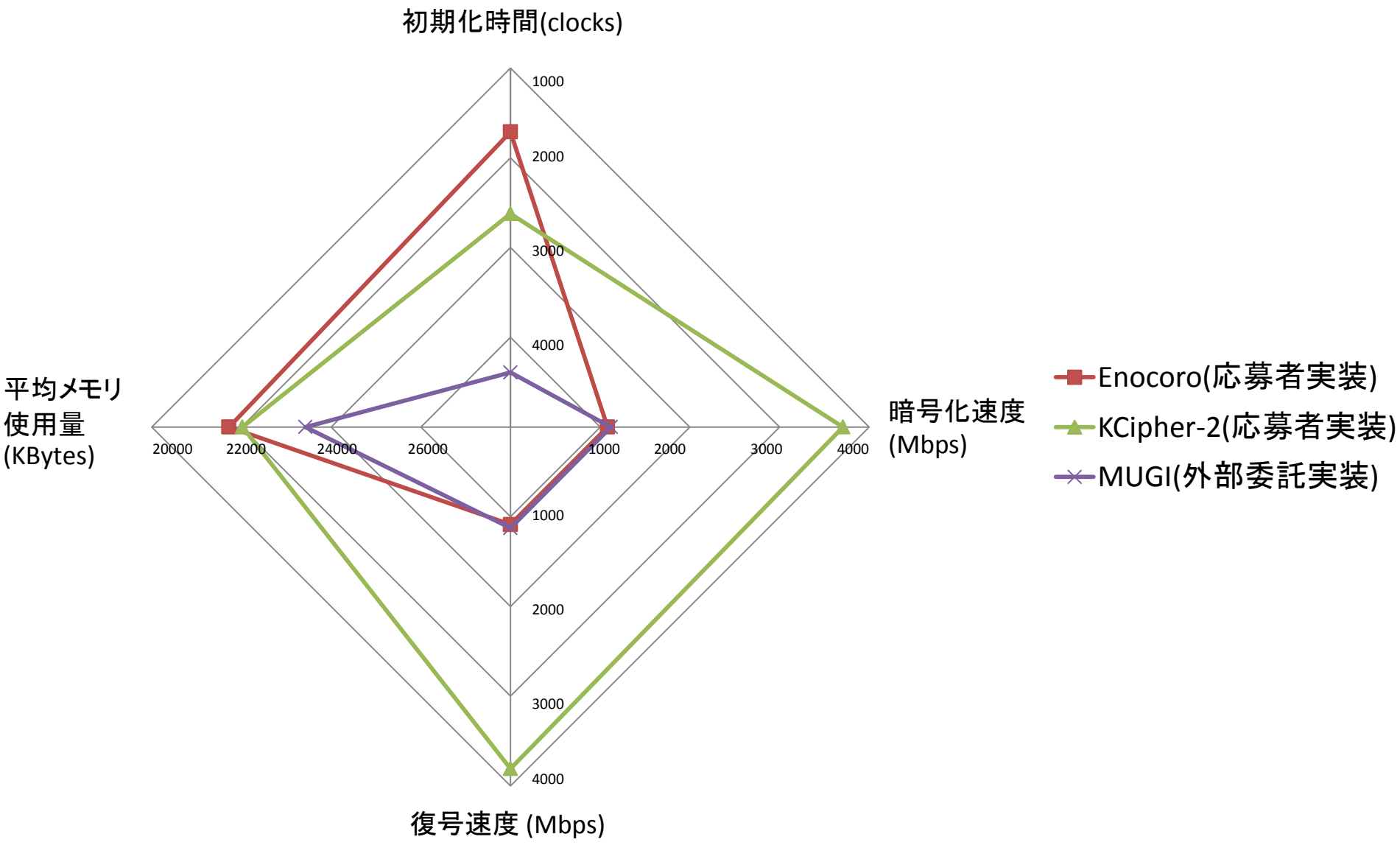
ストリーム暗号（S/W, 平文8バイト）



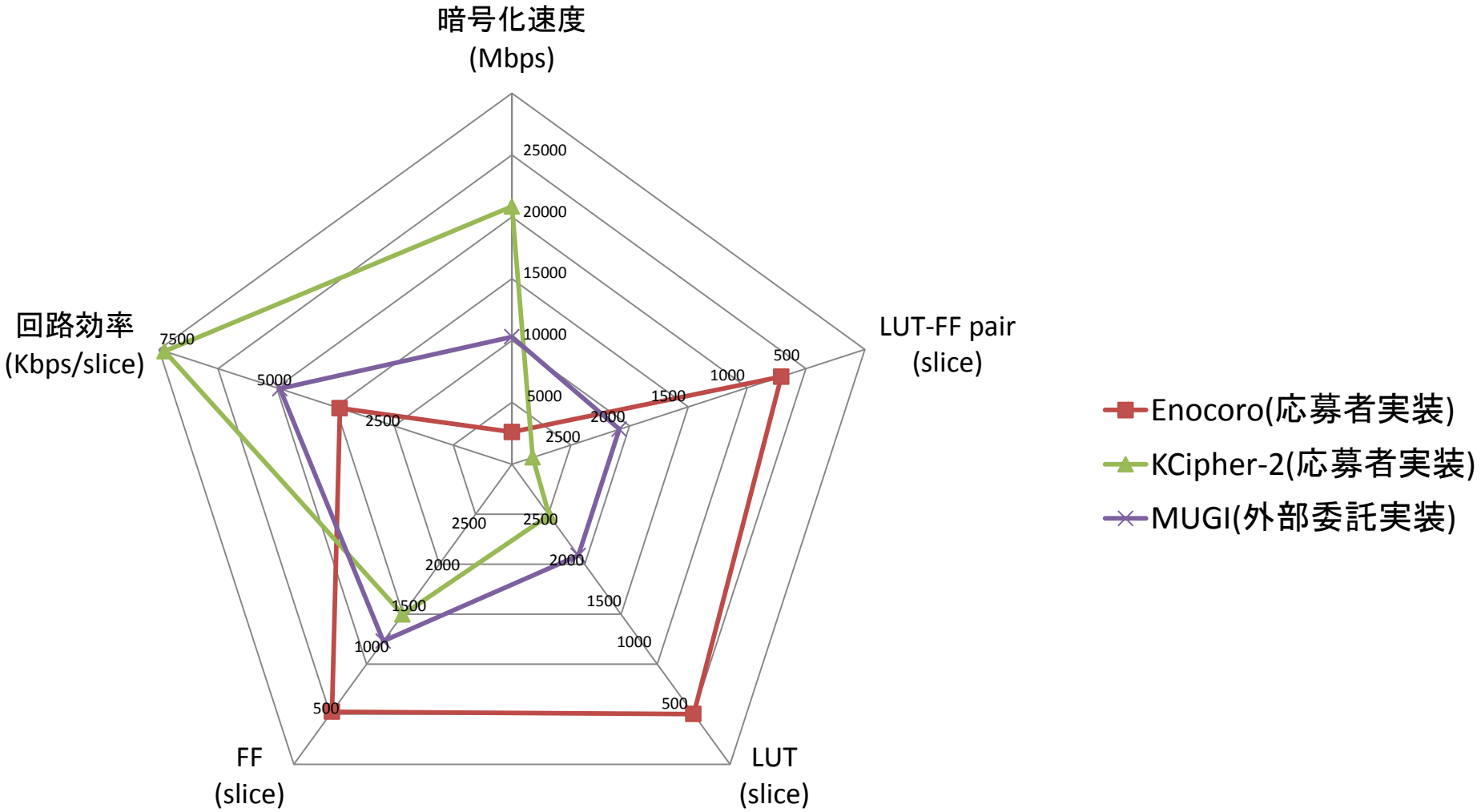
ストリーム暗号（S/W, 平文1536バイト）



ストリーム暗号（S/W, 平文1048576バイト）

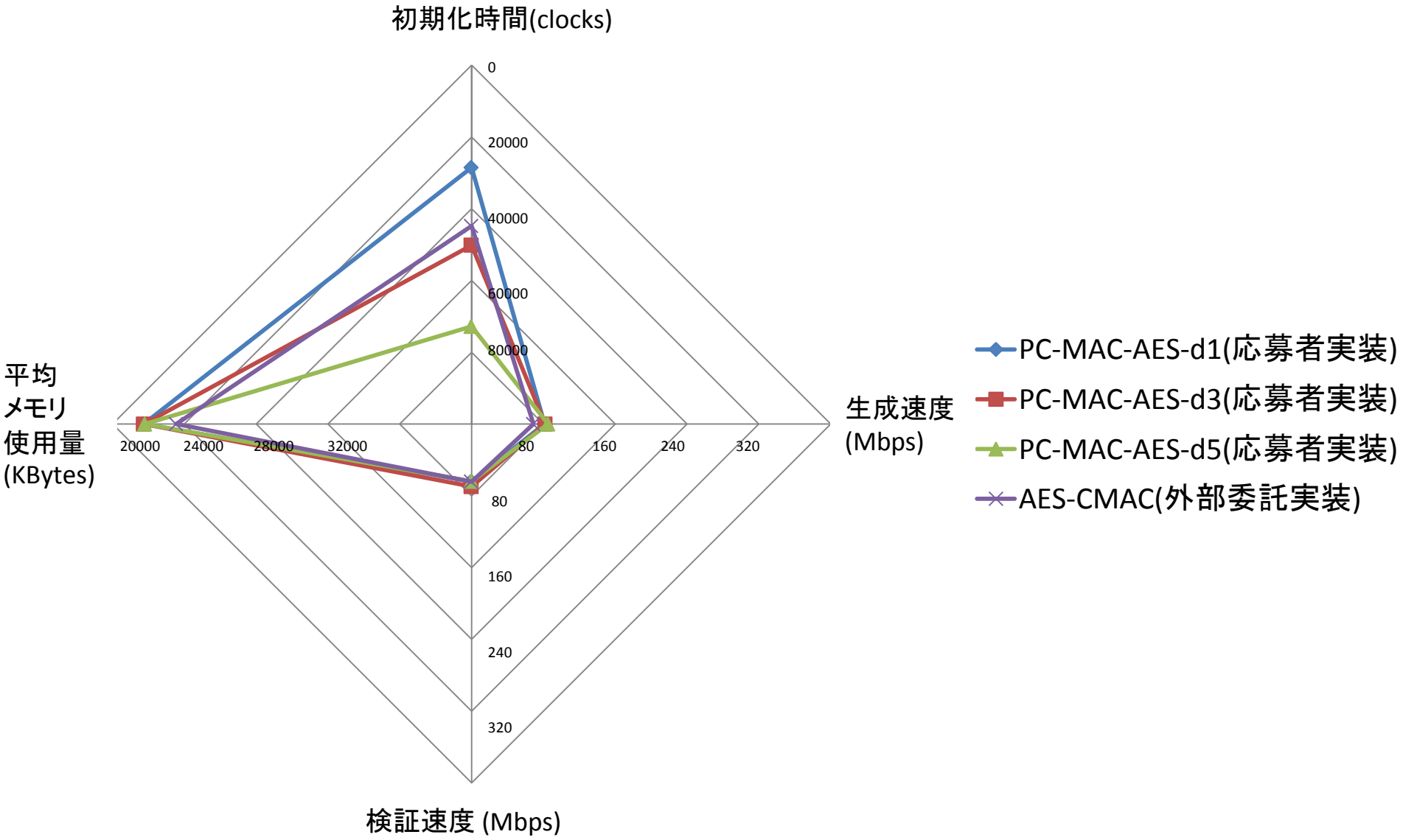


ストリーム暗号（H/W）

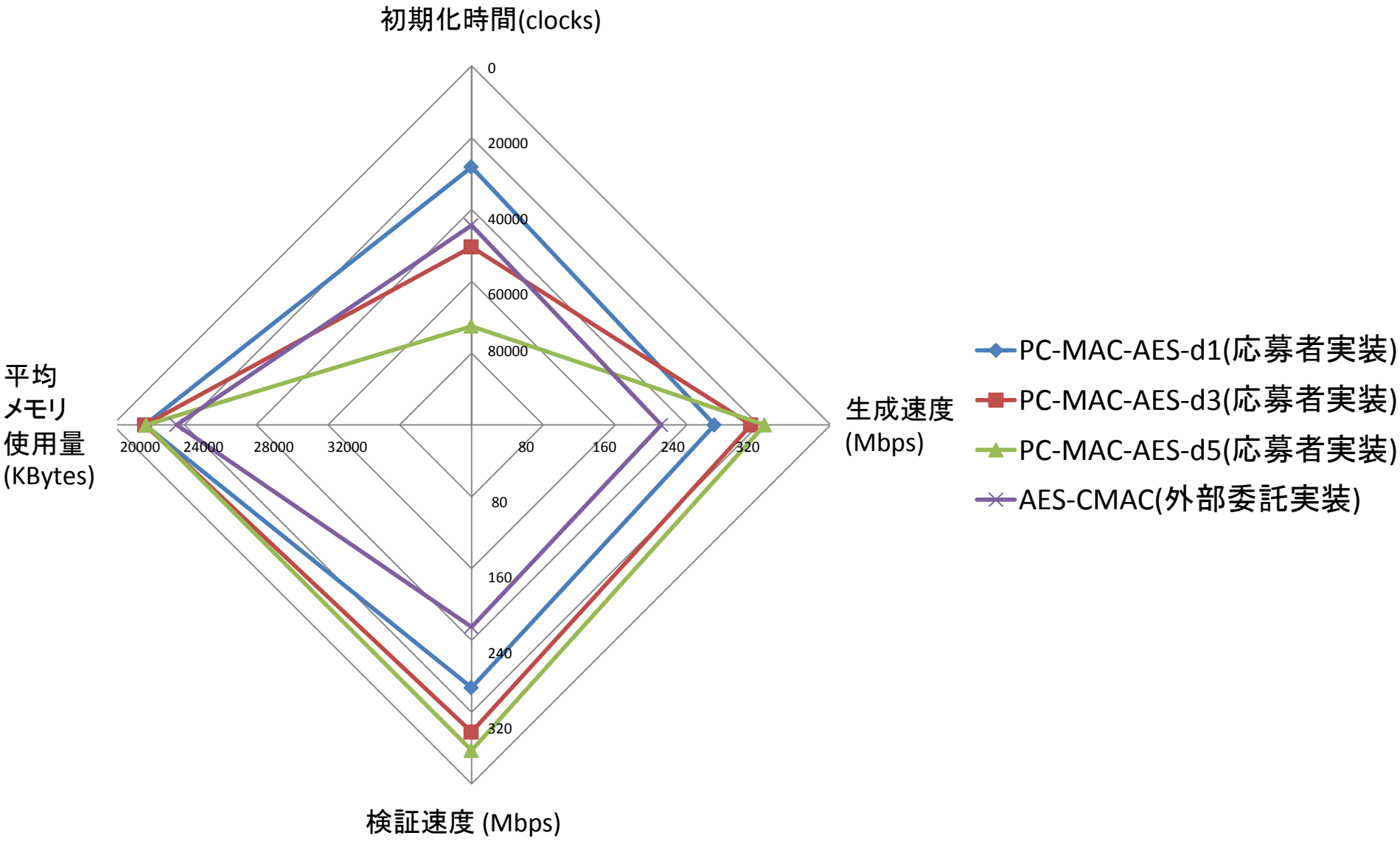


回路効率＝スループット／回路規模(LUT-FF)

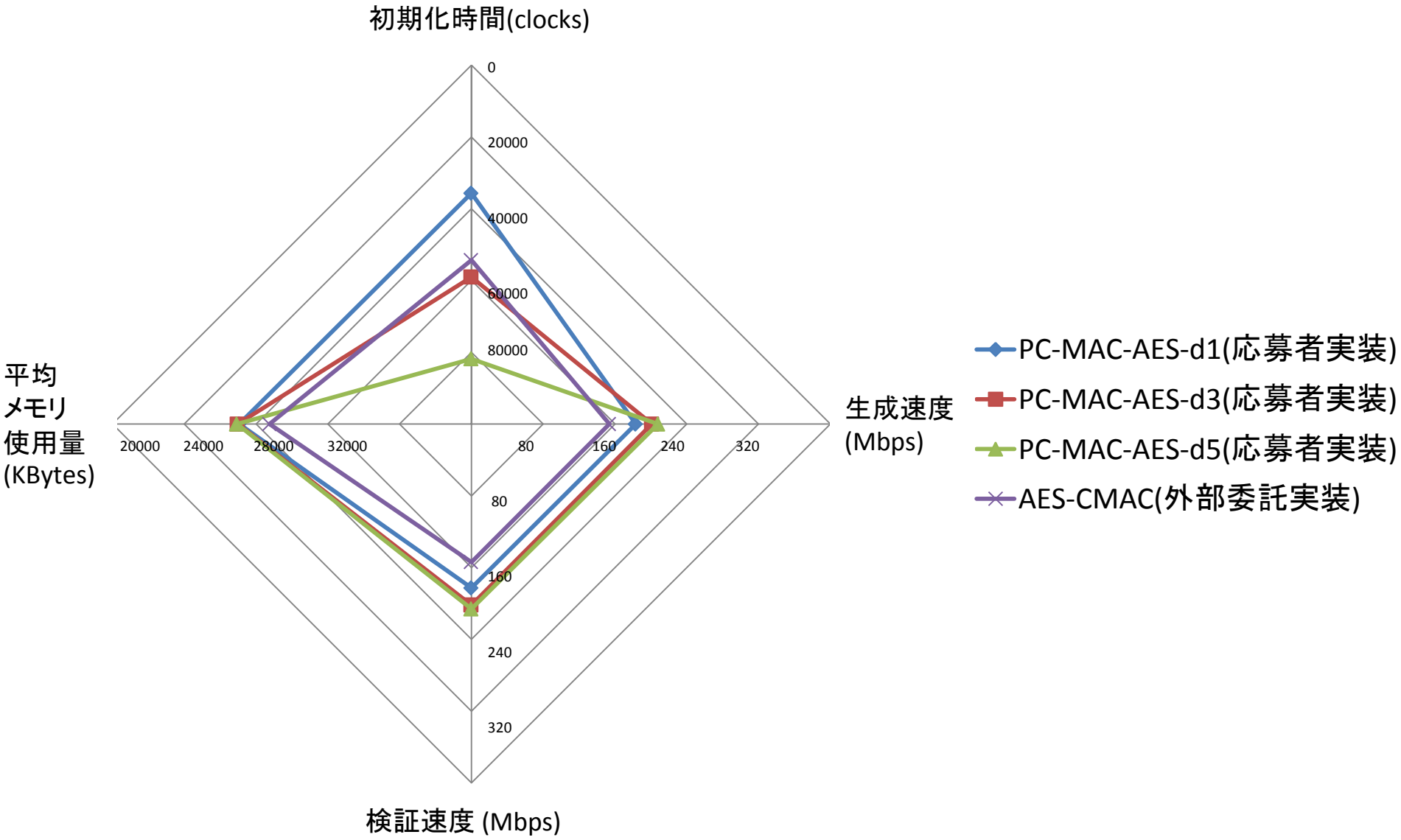
MAC（S/W, 平文16バイト）



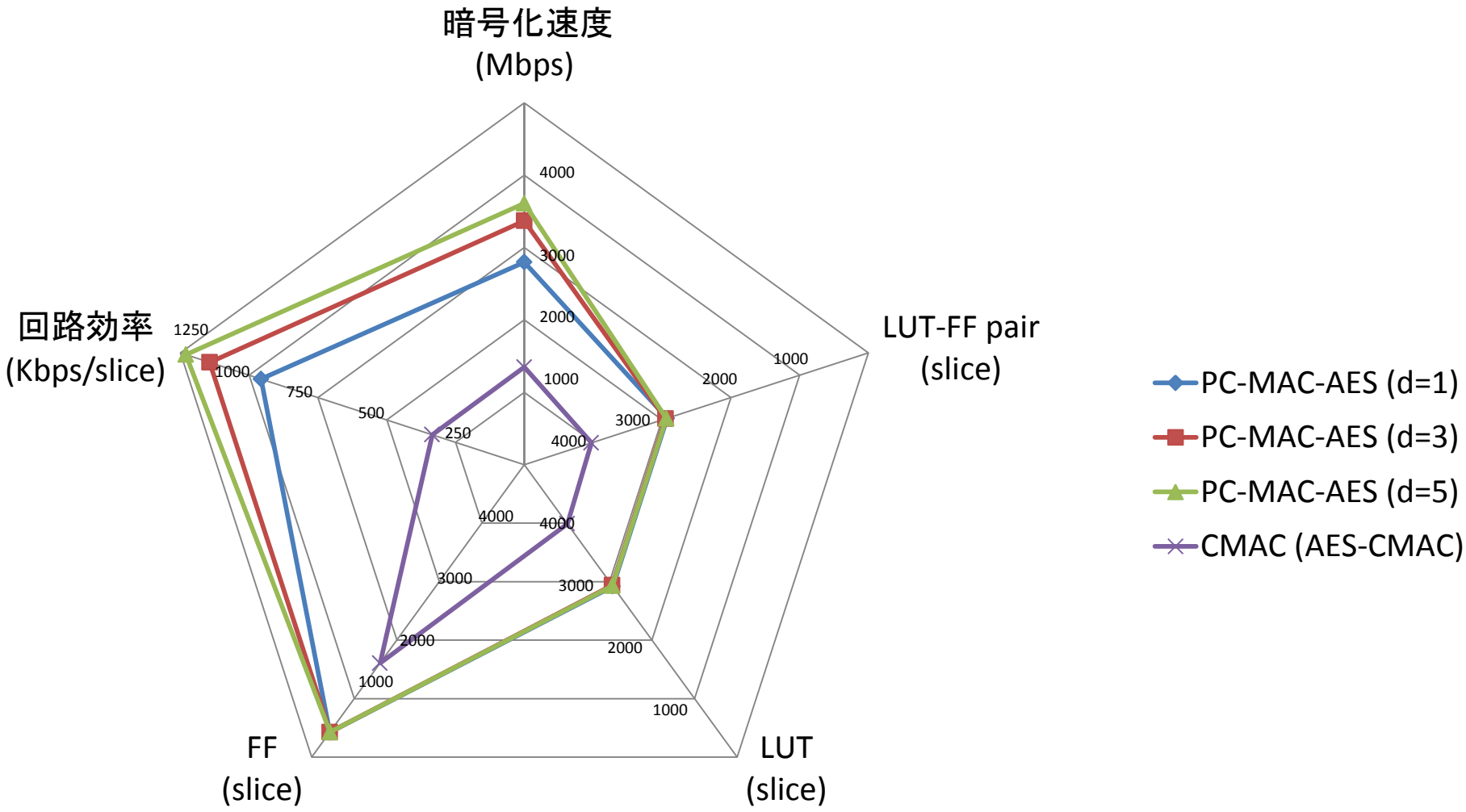
MAC（S/W, 平文1536バイト）



MAC（S/W, 平文1048576バイト）



MAC（H/W）



回路効率＝スループット／回路規模(LUT-FF)

10. 実装評価に関する文献（参考）

今回の評価では、ソフトウェア実装、ハードウェア実装ともに一種類の実装による評価しか実施しなかった。
そこで、実装に関する情報を補足するために、暗号技術の応募者による実装に関する文献等公開データを以下に示す。

実装評価に関する文献　CLEFIA

[1] Taizo Shirai, Kyoji Shibutani, Toru Akishita, Shiho Moriai, Tetsu Iwata, "The 128-Bit Blockcipher CLEFIA (Extended Abstract)." FSE 2007, LNCS 4593, pp.181-195, Springer-Verlag, 2007.

[2] 白井, 渋谷, 秋下, 盛合, 岩田, "128ビットブロック暗号CLEFIA." 電子情報通信学会技術研究報告, ISEC2007-1 (2007-05), 2007.

[3] 白井, 渋谷, 秋下, 盛合, 岩田, "128ビットブロック暗号CLEFIAのハードウェア実装評価." 電子情報通信学会技術研究報告, ISEC2007-49 (2007-07), 2007.

[4] Takeshi Sugawara, Naofumi Homma, Takafumi Aoki, Akashi Satoh, "High-performance ASIC implementations of the 128-bit block cipher CLEFIA." ISCAS 2008, pp.2925-2928, IEEE, 2008.

[5] Toru Akishita, Harunaga Hiwatari, "Very Compact Hardware Implementations of the Blockcipher CLEFIA." SAC 2011, LNCS 7118, pp.278-292, Springer-Verlag, 2011.

実装評価に関する文献　Camellia

[1] NTT and Melco: "Camellia," 1st NESSIE workshop, https://www.cosic.esat.kuleuven.be/nessie/workshop/

[2] 情報処理振興事業協会、通信・放送機構: "CRYPTREC Report 2002," http://www.cryptrec.go.jp/report.html

[3] NTT: "暗号エンジン," https://info.isl.ntt.co.jp/crypt/camellia/engine.html

[4] Melco: "参照コード," https://info.isl.ntt.co.jp/crypt/camellia/source.html

[5] 小田哲、青木和麻呂、小林鉄太郎: "Pentium 4におけるCamelliaの高速実装," SCIS 2006, 2C3-2

[6] Mitsuru Matsui: "How Far Can We Go on the x64 Processors?," LNCS 4047, FSE 2006, pp.341-358, Springer

[7] NESSIE: "Performance of Optimized Implementations of the NESSIE Primitives," https://www.cosic.esat.kuleuven.be/nessie/

[8] 及川一樹、児玉英一郎、王家宏、高田豊雄: "共通言語基盤上における暗号アルゴリズムの効率的な実装手法," SCIS 2008, 2C2-5

[9] Chung-Huang Yang, "Performance Evaluation of AES/DES/Camellia On the 6805 and H8/300 CPUs," updated version SCIS 2001 http://security.nknu.edu.tw/psnl/vita.htm

実装評価に関する文献　Camellia

[10] 市川哲也、松井充、中嶋純子、時田俊雄、青木和麻呂、神田雅透、盛合志帆: "128ビットブロック暗号Camelliaの実装評価", 信学技報ISEC2000-73

[11] T. Ichikawa, T. Kasuya, and M. Matsui: "A Compact Hardware Implementation Method for 128-Bit Block Cipher Camellia (in Japanese)," 信学技報ISEC2001-133

[12] 情報処理振興事業協会、通信・放送機構: "CRYPTREC Report 2000," http://www.cryptrec.go.jp/report.html

[13] Akashi Satoh, Sumio Morioka: "Hardware-Focused Performance Comparison for the Standard Block Ciphers AES, Camellia, and Triple-DES," LNCS 2851, ISC 2003, pp.252-266, Springer

[14] 菅原健、本間尚文、青木孝文、佐藤証: "ISO標準ブロック暗号のASICハードウェア性能評価," 信学技報ISEC2006-159

[15] T.Ichikawa, T.Sorimachi, T.Kasuya, M.Matsui: "On the criteria of hardware evaluation of block ciphers(1)," 信学技報ISEC2001-53

[16] 反町亨、市川哲也、粕谷智巳: "FPGAを用いたブロック暗号ハードウェア実装評価," SCIS 2003, 12D-3

[17] 朝日康介、五十嵐保隆、金子敏信: "ブロック暗号CamelliaのCUDAによる高速実装," 信学会2010年ソ大会, A-7-7

実装評価に関する文献　Camellia

[18] 高橋健司、市川哲也、鈴木大輔、粕谷智巳: "FPGAを用いた暗号アルゴリズムCamelliaのハードウェア高速実装," 信学会2004年ソ大会, A-7-7

[19] Daniel Denning, James Irvine, Malachy Devlin: "A Key Agile 17.4 Gbit/sec Camellia Implementation," the 14th International Conference on Field-Programmable Logic and its Applications, FPL 2004, LNCS 3203, Springer

[20] Daniel Denning, James Irvine, Malachy Devlin: "A HIGH THROUGHPUT FPGA CAMELLIA IMPLEMENTATION," PhD Research In Micro-Electronics & Electronics, PRIME 2005, Jul. 2005

[21] Akashi Satoh, Sumio Morioka: "Unified Hardware Architecture for 128-Bit Block Ciphers AES and Camellia," the 5th International workshop on Cryptographic Hardware and Embedded Systems, CHES 2003, LNCS 2779, Springer

実装評価に関する文献　CIPHERUNICORN-A

[1] 角尾幸保、久保博靖、宮内宏、中村勝洋、「128 ビットブロック暗号CIPHERUNICORN-A」、2000 年暗号と情報セキュリティシンポジウムSCIS2000, A18, 2000.

[2] 情報処理振興事業協会、通信・放送機構: "CRYPTREC Report 2002,"
http://www.cryptrec.go.jp/report.html

実装評価に関する文献　Hierocrypt-3

[1] Performance Evaluation of NESSIE First Phase, NESSIE
https://www.cosic.esat.kuleuven.be/nessie/deliverables/D14.pdf

[2] Performance of Optimized Implementations of the NESSIE Primitives, NESSIE
https://www.cosic.esat.kuleuven.be/nessie/deliverables/D21-v2.pdf

[3] M. Rogawski:
Analysis of Implementation Hierocrypt-3 algorithm (and its comparison to Camellia algorithm) using ALTERA devices,
http://eprint.iacr.org/2003/258

実装評価に関する文献　SC2000

[1] "共通鍵ブロック暗号SC2000の実装," SCIS2001 13A-4, pp.743-748. 2001.

[2] "共通鍵ブロック暗号SC2000の実装(II)," SCIS2002, 9B-4, 2002.

[3] "共通鍵ブロック暗号SC2000の実装(III)," ISEC, 2002/7/18-19, pp.183-188 2002.

[4] Helger Lipmaa. "Fast Software Implementations of SC2000", ISC 2002, LNCS 2433, pp.63-74, 2002.

実装評価に関する文献　Enocoro-128v2

[1] 三上 修吾, 渡辺 大, ストリーム暗号Enocoro-128v2 のソフトウェアおよびハードウェア実装と評価, CSS2012, 742-748, 2012..

実装評価に関する文献　KCipher-2

[1] Matt Henricksen, Ed Dawson, "Rekeying Issues in the MUGI Stream Cipher," LNCS 3897, pp.175-188, 2006.

[2] Erik Zenner, "On the Role of the Inner State Size in Stream Ciphers," pp. 237-250, INSTICC Press 2004, 2004.

実装評価に関する文献　MUGI

[1] 吉田 博隆, 古屋 聡一, 疑似乱数生成器のソフトウェア高速実装に関する考察, SCIS2003, 9C-4, 2003.

[2] 大和田徹, 平重喜, 五十嵐悠一, 北原潤, MUGIのハードウェア実装及び評価, SCIS2005, 1E3-5, 2005.

[3] M.Henricksen and E.Dawson, Rekeying Issues in the MUGI Stream Cipher, Selected Areas in Cryptography, SAC2005, Springer-Verlag, LNCS3897, pp.175-188, 2006.

[4] J.Takahashi, T.Fukunaga, K.Sakiyama, Differential Fault Analysis on Stream Cipher MUGI, IEICE Transactions 95-A(1), pp.242-251, 2012.

実装評価に関する文献　PC-MAC-AES

[1] Kazuhiko Minematsu, Yukiyasu Tsunoo: Provably Secure MACs from Differentially-Uniform Permutations and AES-Based Implementations.
Fast Software Encryption, 13th International Workshop, FSE 2006, Lecture Notes in Computer Science 4047 Springer 2006, pp . 226-241.