CRYPTRECシンポジウム2010

「暗号技術の実装について」
ソフトウエア実装評価

三菱電機株式会社
情報技術総合研究所

中嶋 純子

ソフトウエア実装評価の環境

	1. PC環境	2. サーバ環境	3. ハイエンド環境
CPU	Pentium Ⅲ 650MHz	Ultra SPARC Ⅱi 400MHz	Alpha21264 463MHz
OS	Windows98 SE	Solaris 7	Tru64 UNIX V5.1
搭載メモリ	64MB	256MB	512MB
コンパイラ	Visual C++ Ver6.0 SP3	Forte C 6	DEC C
	Mandatory	Option 各暗号の設計思想を尊重し選択とした	

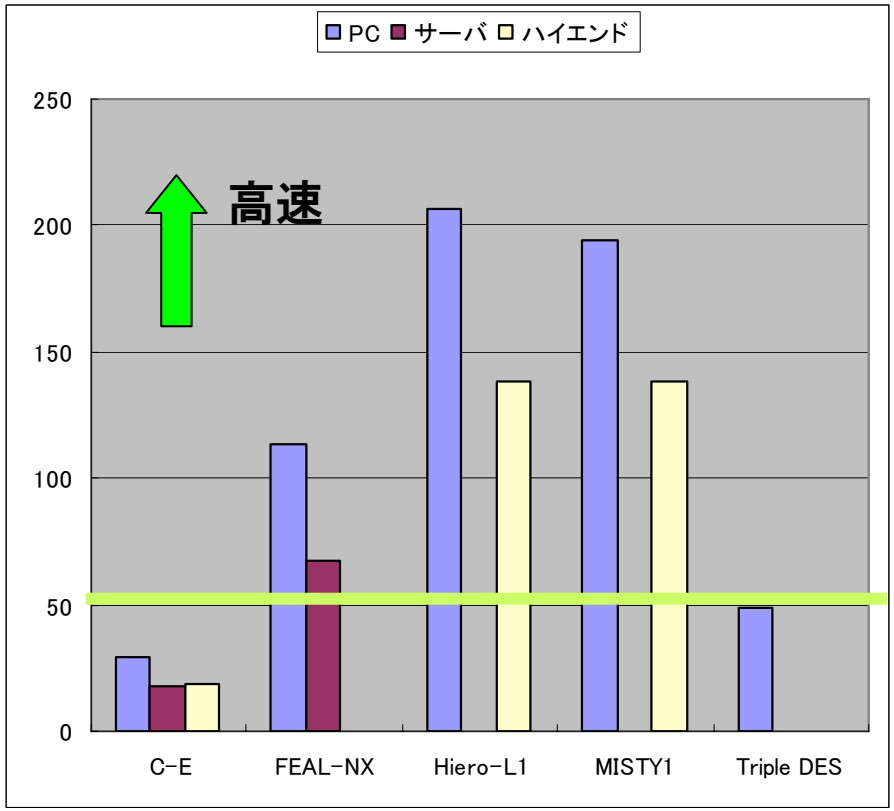
◆ ローエンド(8-bit MCU)での評価は、評価期間の制限から見送り

ソフトウエア評価 対象アルゴリズム

Algorithms		1. PC環境	2. サーバ	3. ハイエンド
64 bit	CIPHERUNICORN-E			
	FEAL-NX			-
	Hierocrypt-L1		-	
	MISTY1		-	
	Triple-DES		-	-
128 bit	Camellia			
	CIPHERUNICORN-A			
	Hierocrypt-3			
	RC6			-
	SC2000			

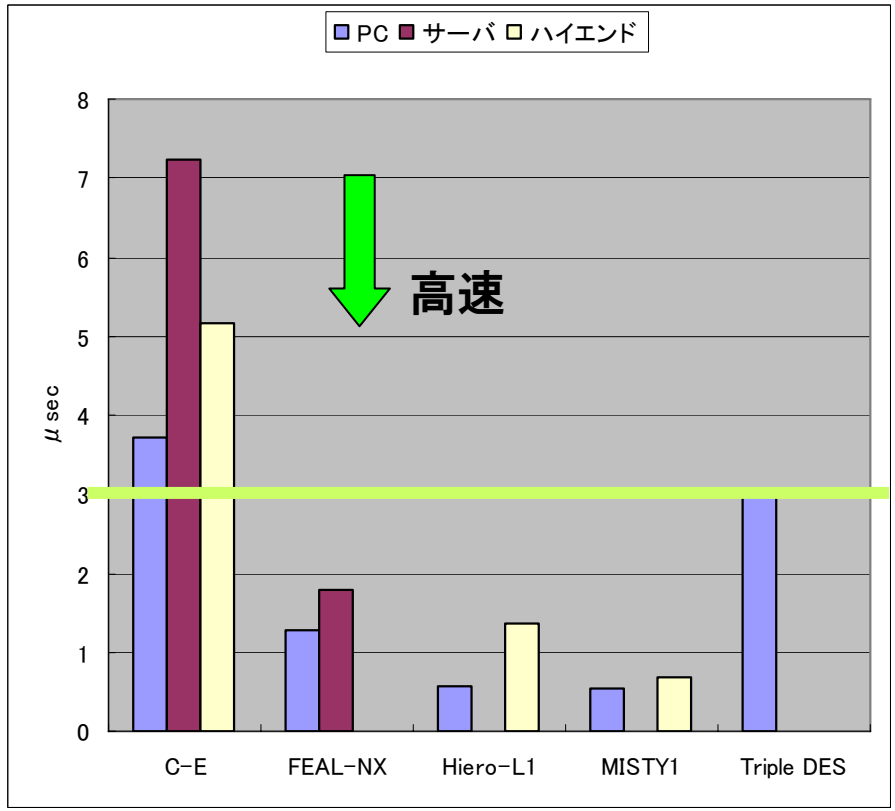
CRYPTOREC 2000 SW実装評価

64-bit ブロック暗号



データランダム化部

単位： Mbps

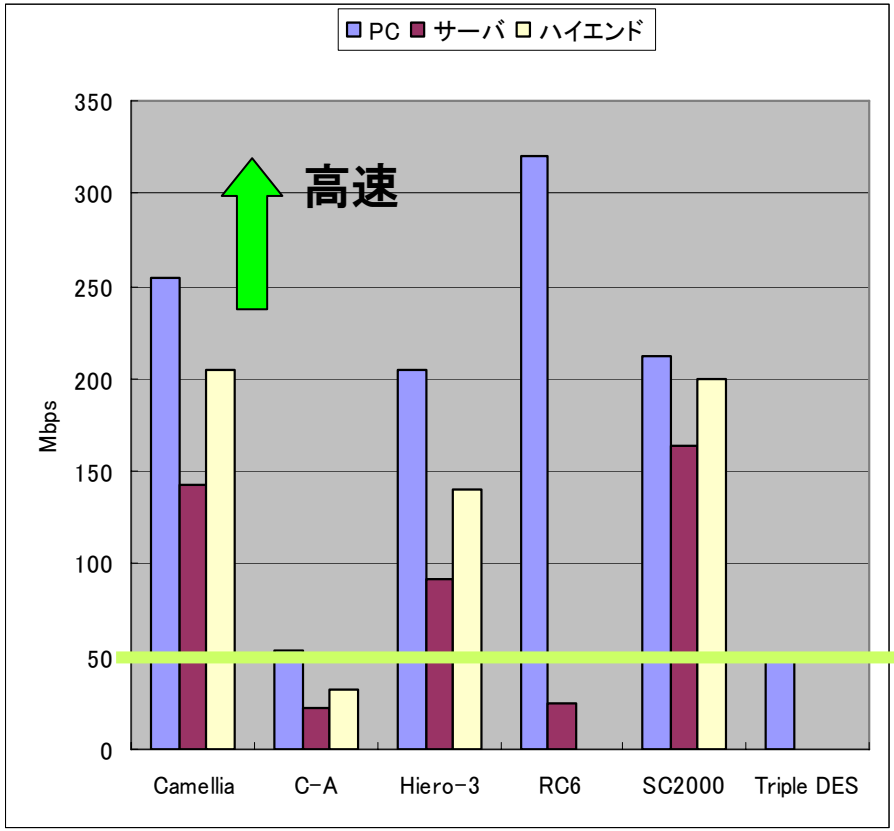


鍵スケジュール部＋データランダム化部

単位： μsec

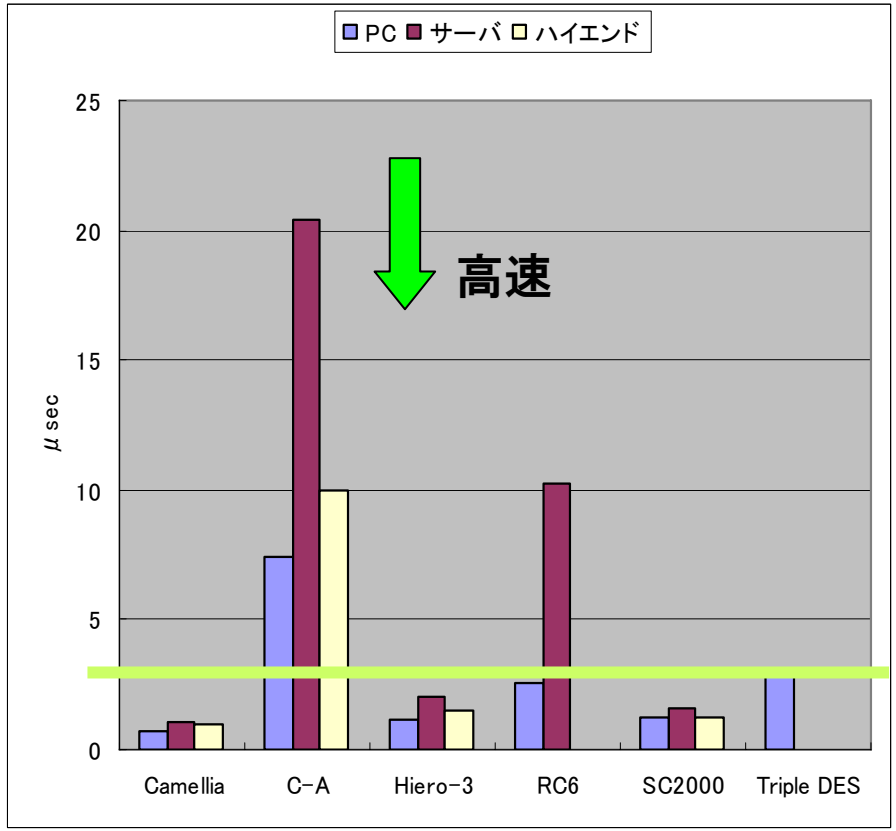
CRYPTOREC 2000 SW実装評価

128-bit ブロック暗号



データランダム化部

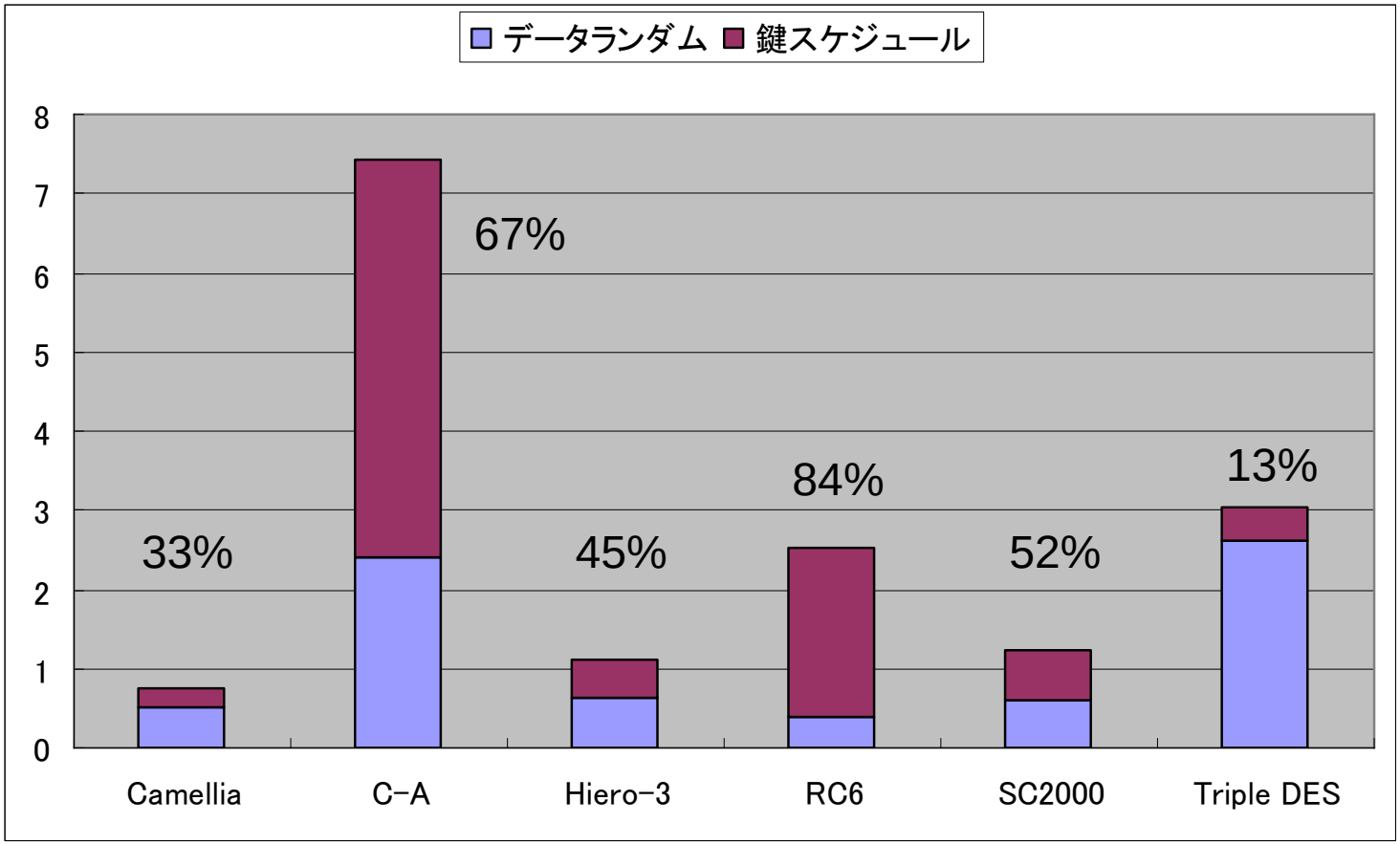
単位： Mbps



鍵スケジュール部＋データランダム化部

単位： μsec

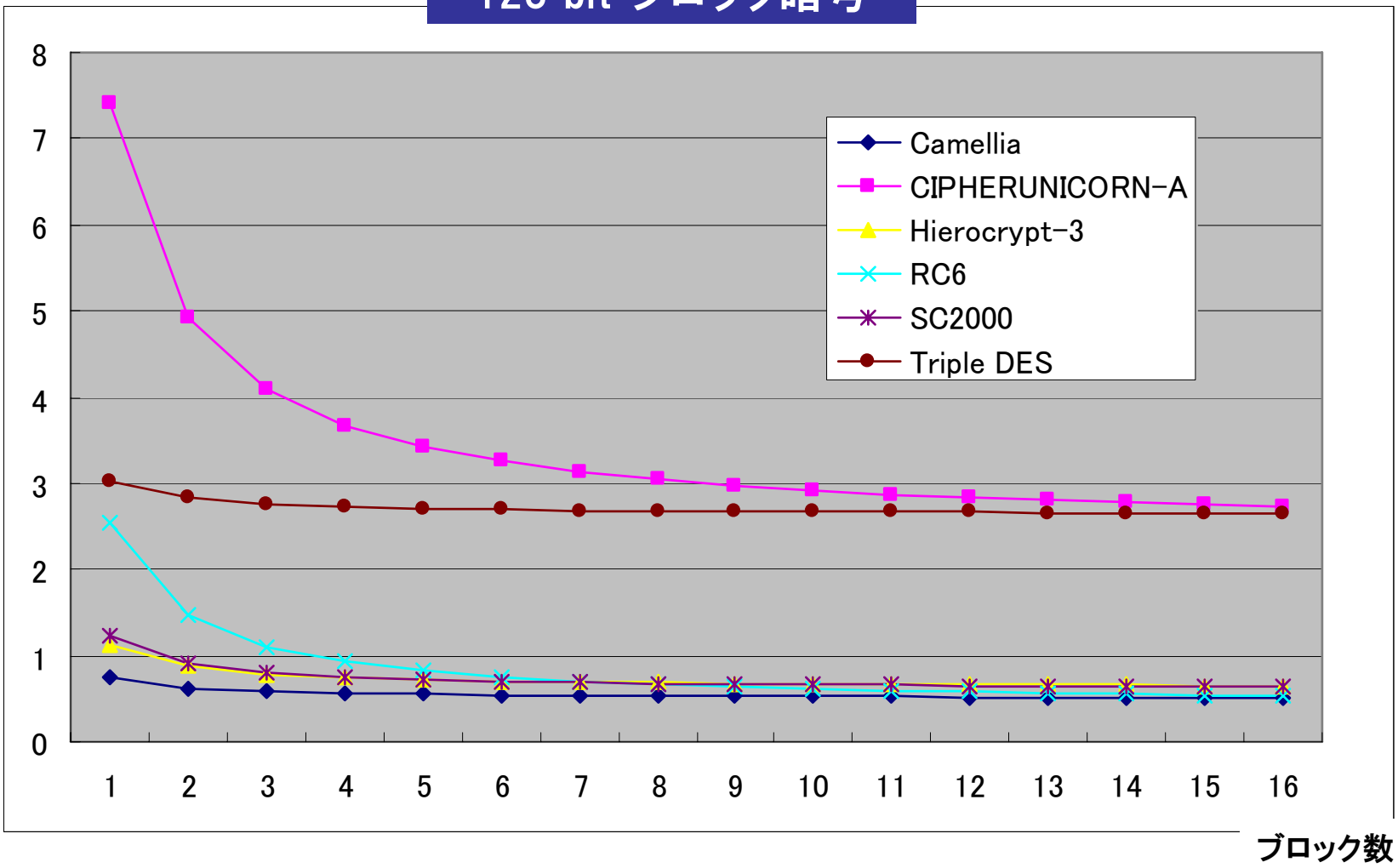
128-bit ブロック暗号



鍵スケジュール部＋データランダム化部

単位：　μsec

128-bit ブロック暗号



鍵スケジュール部＋データランダム化部

単位： μsec

評価環境の見直し

2000年	1. PC環境	2. サーバ環境	3. ハイエンド環境
CPU	Pentium Ⅲ 650MHz	Ultra SPARC Ⅱi 400MHz	Alpha21264 463MHz

PC と WS の 違 い が あ い ま い に

マルチコア化

More Clock から More Coresへ

PⅢ→P4→Core2→Core i5 → i7 …

クロスポイント 2006年頃

AES命令セット Westmere

かつてのMMX, SSE命令のように
いずれ標準に？

マルチコア化

特定用途化

・ラックマウント
/ブレード型サーバ
・通信、ネットワーク基盤

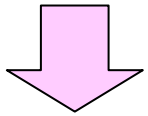
暗号化処理機構

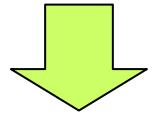
UltraSPARC T2
暗号アルゴリズム10種

2003～2004年頃
Phase Out …

新たな評価環境の検討

2000年	1. PC環境	2. サーバ環境	3. ハイエンド環境
	Pentium Ⅲ 650MHz	Ultra SPARC Ⅱi 400MHz	Alpha21264 463MHz



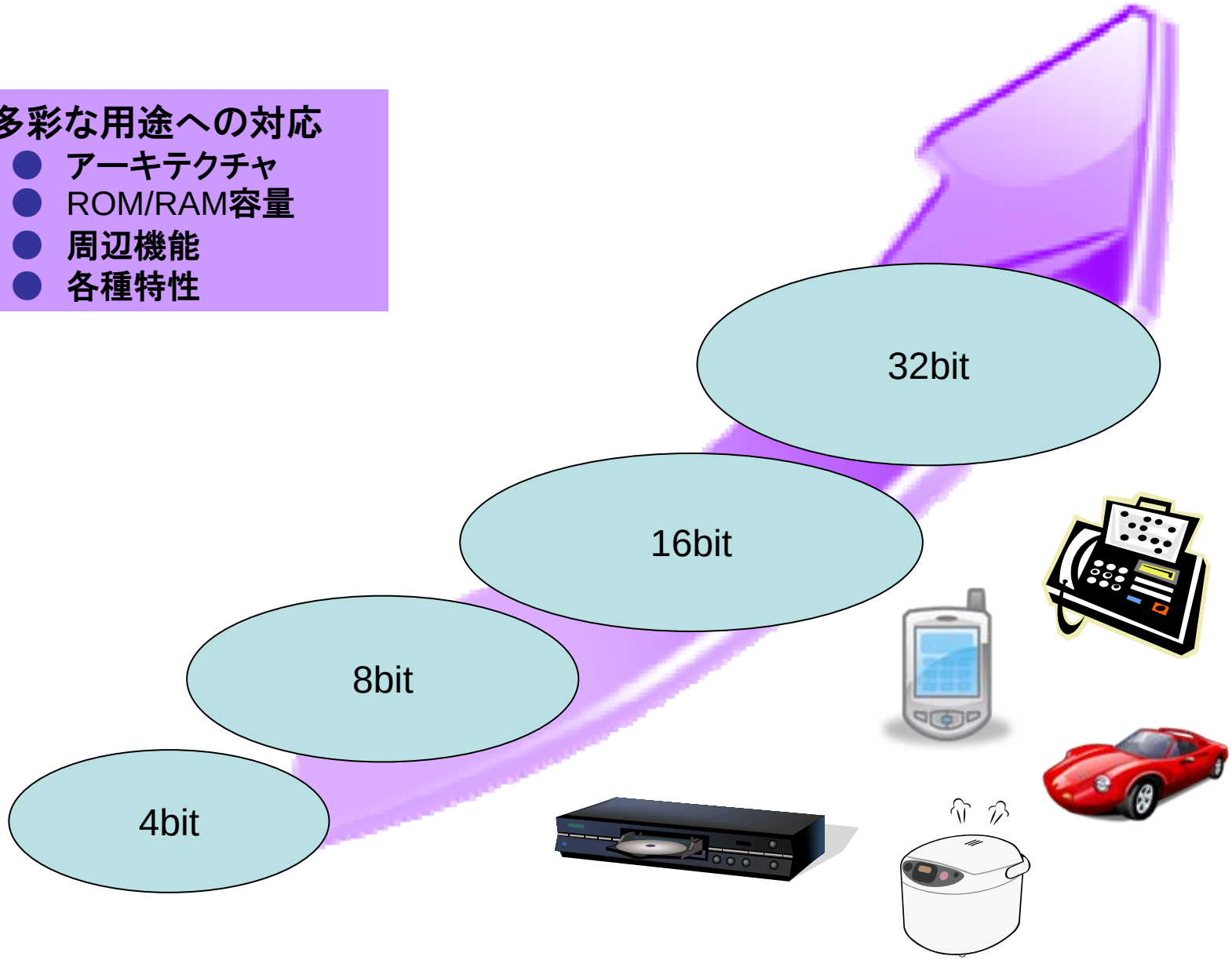


2010～	1. PC環境	2. 組込み環境	3. GPGPU環境
	x86系, Multi-Core Windows XP / 7	“組込み”定義曖昧 多品種で選定困難？	やや時期尚早？
	Mandatory	Mandatory/Option	Option

多様な機器組込み用マイコン

多彩な用途への対応

- **アーキテクチャ**
- ROM/RAM容量
- **周辺機能**
- **各種特性**



組込み環境での評価

ソフトウエア性能 （ 速度 ・ コードサイズ ）

target / candidate	t_1 A 8bit MCU	t_2 B 16bit MCU	t_3 C 32bit CISC	t_4 D 32bit RISC
Algorithm 1	[1]			
Algorithm 2		[2]		
Algorithm 3			[3]	
Algorithm 4				[4]

利点： 好きなターゲットを選択可能
アルゴリズムの特長をアピールできる

難点： それぞれ環境が異なるので、比較評価が行えない

組込み環境での評価

ソフトウエア性能 （ 速度 ・ コードサイズ ）

target / candidate	t_1 A 8bit MCU	t_2 B 16bit MCU	t_3 C 32bit MCU	… t_x X ** MCU
Algorithm 1	[1]	+	+	+
Algorithm 2	+	[2]	+	+
Algorithm 3	+	+	[3]	+
Algorithm N	+	+	+	[N]

利点： 好きなターゲットを選択可能、同一環境上での(公平な)評価

難点： プログラム開発量が増大

⇒ 必ずしも応募者が実施すべきとは限らない