09/06/25 Rev.2

CUDA を使った ToraTora(Ver1.1.0.0) の性能評価

1GByte のランダムデータの AES 復号化とベリファイの所要時間(単位　秒)

	VistaSP2 HDD		VistaSP2 RAM		XPSP3 HDD		XPSP3 RAM	
C7-D	89	87	96	91	105	104	111	107
GeForce8500GT	51	51	58	56	57	56	57	49
GeForce9800GT	42	33	29	24	37	30	27	23
C7-D Padlock	42	33	28	24	36	30	27	23

●ToraTora1.1.0.0 の SHA-1 ハッシュ値

ToraTora1.1.0.0.zip	ae41 d922 bd27 592c bd6a a22b dd17 c34e ca27 5f13
ToraTora1.1.0.0_ENU.zip	6625 6c28 36cb 6943 ba5b 0adc 9215 ac4f b472 f113

●計測 PC

マザーボード MM-3500
CPU　C7-D　1.5GHz
I/F　 PCI-Express　x16　(Ver1)
メモリ PC2-4200 3GByte (シングルチャネル)
HDD I/F ATA133

●CPU スペック

VIA C7-D　1.5GHz　Padlock 暗号ハード装備
「C7-D」は、Microsoft の CSP を利用
「C7-D Padlock」は、iAesCSP Padlock 版 Ver0.9.4 を利用

●GPU スペック

	GeForce 8500GT	GeForce 9800GT
ドライババージョン	185.85	185.85
ストリームプロセッサ	16	112
コアクロック	459 MHz	600 MHz
シェーダークロック	918 MHz	1500 MHz
メモリクロック	400 MHz	900 MHz
メモリ　インターフェース	128 bit	256 bit

●計測条件

暗号アルゴリズム　256bit AES 暗号　CBC モード

テスト名	計測条件
VistaSP2　HDD	OS: Windows Vista SP2 HDD1 にある暗号化データ 1GByte を HDD2 へ復号化 or ベリファイ
VistaSP2 RAM	OS: Windows Vista SP2 RAM DISK にある暗号化データ 1GByte を同じ RAM DISK へ復号化　or ベリファイ
XPSP3 HDD	OS: Windows XP SP3 HDD1 にある暗号化データ 1GByte を HDD2 へ復号化　or ベリファイ
XPSP3 RAM	OS: Windows XP SP3 RAM DISK にある暗号化データ 1GByte を同じ RAM DISK へ復号化　or ベリファイ

●HDD 及び RAM DISK の性能

CrystalDiskMark 2.2.0　1000MB 5 回による測定値 (単位　MByte/Sec)

			1000MB	512KB	4KB
HDD1	Vista SP2	READ	34.49	10.37	0.341
		WRITE	33.38	18.33	0.691
	XP SP3	READ	36.77	11.20	0.406
		WRITE	35.82	21.39	0.839
HDD2	Vista SP2	READ	52.00	25.36	0.387
		WRITE	46.87	19.38	0.818
	XP SP3	READ	51.50	25.89	0.402
		WRITE	44.62	20.02	0.796
RAM DISK	Vista SP2	READ	246.8	235.9	144.1
		WRITE	251.5	239.1	147.7
	XP SP3	READ	270.5	264.6	214.4
		WRITE	278.8	270.3	262.8

●RAM DISK

BUFFALO　RAMDISK ユーティリティ　Ver1.0.0.1

RAM DISK は、HDD よりも高速だが、HDD のように並列に動作しない。

コメント

GeForce 8500GT(ストリームプロセッサ数 16 個)では、CPU より約 1.8 倍高速であるが、HDD の性能が遅い場合、性能向上はしない。

GeForce 9800GT(ストリームプロセッサ数 112 個)では、CPU よりも約 3 倍高速であるが、HDD の性能が遅い場合、性能向上はしない。

性能向上がストリームプロセッサ数に比例していないのは、GeForce では CPU と異なり PCI-Express 経由でデータを送受信する必要があるためであり PCI-Express Ver1 のマザーボードであったため転送の遅さが影響している。PCI-Express の 1GByte のデータの送受信に約 11 秒ではないかと実測した。pinned メモリによる最適化で多少性能の改善は、見込めるか？

高性能な CPU では、GeForce よりも CPU のほうが高速になるのでその場合は、CUDA オプションをはずして CPU で処理すると良い。