



## 暗号化がディスク・パフォーマンスに 与える影響の検証

暗号化ディスクと非暗号化ディスクのパフォーマンスはほぼ同じとのテスト結果

# Contents

本書の内容

概要 .....	3
Passmarkによるパフォーマンス・テストについて .....	4
パフォーマンスの考え方 .....	5
パフォーマンスのテスト方法 .....	8
パフォーマンス・テストの結果 .....	10
まとめ .....	11

## 概要

本書では、Check Point Endpoint Security Full Disk Encryption™による暗号化ディスクと非暗号化ディスクの各ディスク・パフォーマンスを測定し、比較した結果について解説します。テストには、Pentium III 750MHzを搭載したノートPCとPentium 4 3GHzを搭載したデスクトップPCを使用しました。OSはどちらもWindows 2000 Professional SP4です。

ディスク暗号化製品の使用がビジネス・ユーザに与える影響は、基本的にはほとんど無視できるレベルです。AES (Advanced Encryption Standard) などの効率的な暗号化アルゴリズムと、普及価格帯のPCに搭載された標準クラスのCPUにより、暗号化がPC全体のパフォーマンスに及ぼす影響は最小限に抑えられています。暗号化を実施した場合、ある程度のパフォーマンス低下が発生することは避けられませんが、ほとんどのユーザはその違いに気付きません。この技術白書では、暗号化がパフォーマンスに与える影響を前述の2つの環境で測定した結果を示します。

ディスク・パフォーマンスの測定にあたっては、Passmarkのパフォーマンス測定ソフトウェア ([www.passmark.com/products/pt.htm](http://www.passmark.com/products/pt.htm)) を使用しました。このソフトウェアの総合テスト・スイート (ディスク・パフォーマンスの重要度係数は全体の20パーセント) を使用し、PCのパフォーマンスを測定しています。テスト・スイート全体を実行したところでは、Check Point Endpoint Security Full Disk Encryption製品がインストールされたデスクトップPCのパフォーマンスは、暗号化が行われていない場合と比較して、わずか2.9パーセント低下しているだけという結果が出ました (図1を参照)。

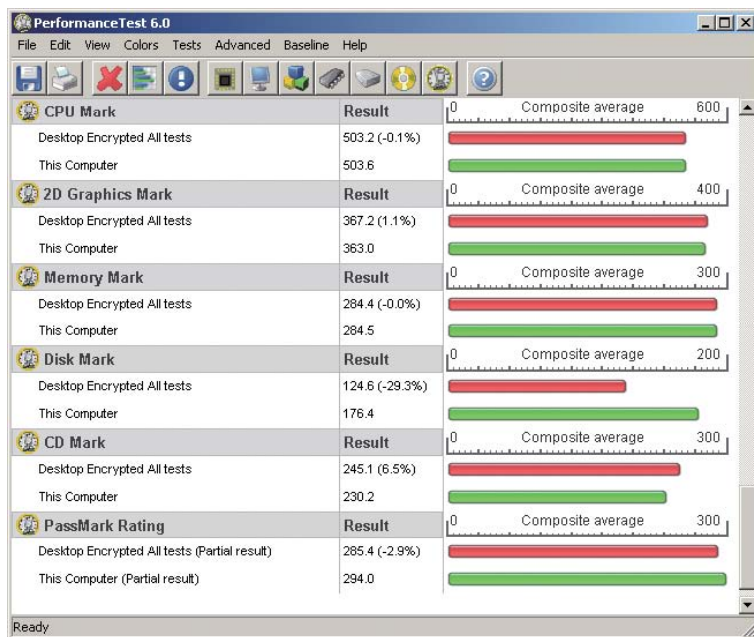


図1 テスト・スイート全体を実行した場合のPassmark評価 (3Dグラフィック・テストは実施せず)

パフォーマンスを測定したディスク操作は、「サイズが大きいファイルの連続読み取り」、「サイズが大きいファイルの連続書き込み」、そして最も重要な「読み取り/書き込みを伴うランダム・シーク (ランダム・シーク+RW)」の3つです。

ディスク上に保存されたファイルは、数週間使用しているうちに断片化していくことから、ランダム・シーク+RWテストは、大半のユーザの実際の使用方法を最も正確に反映していると考えられます。断片化したディスク上のファイルの読み取り/書き込みを行う場合は、ディスク上の連続していない複数の領域に対してデータの読み取り/書き込みを行う必要があります。通常、連続読み取りはオペレーティング・システムが真新しい状態である場合にのみ発生し、連続書き込みはディスクが使用開始後間もない場合に発生します。このため、ランダム・シークを測定することが、実際のデータ転送速度を測るのに最適な方法であると考えられるのです。ランダム・シーク・テストでは、断片化したディスク上でファイルの読み取り/書き込みを行う際の、ディスク・ヘッドのトラック間の動きをエミュレートします。このランダム・シーク・テストが、暗号化ディスクと非暗号化ディスクのパフォーマンスの違いを最も明確に表すテストとなります。

ランダム・シーク+RWテストでは、非暗号化ディスクに対する暗号化ディスクのパフォーマンス低下は、ノートPC (2.4パーセント) とデスクトップPC (5.1パーセント) で若干異なることが分かりました (図2を参照)。連続読み取りと連続書き込みでの差は、ランダム・シーク+RWよりも大幅に大きくなります。連続読み取り/書き込みのパフォーマンスは高速なCPUの方が高くなりますが、コンピュータの一般的な使用方法においては、連続読み取り/書き込み性能の重要性はランダム・シーク性能よりもはるかに低くなります。暗号化はCPU負荷の高い処理ですが、断片化したデータの読み取り/書き込みをディスクが行う速度は、実際には暗号化アプリケーションやCPU設定ではなく、トラック間のシーク時間によって決まるからです。

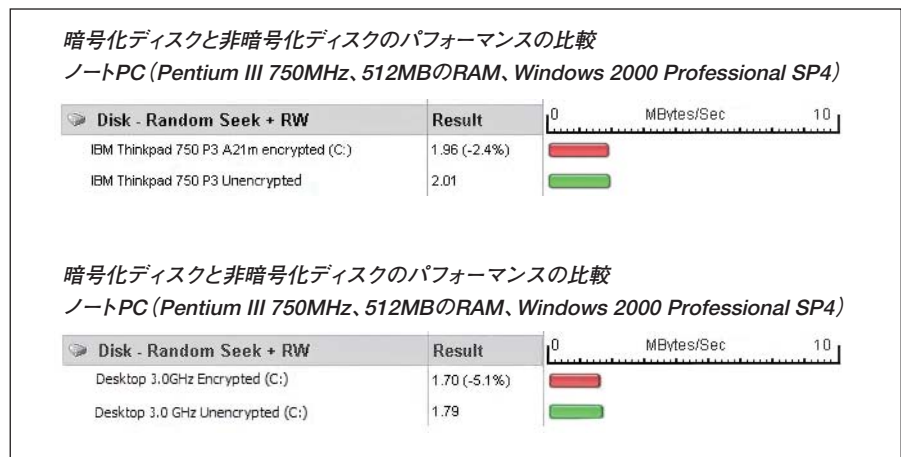


図2 ランダム・シーク+RWテストの結果

## Passmarkによるパフォーマンス・テストについて

Passmarkソフトウェアには、複数の標準テスト・スイートが用意されています。各スイートには、コンピュータ・システムのパフォーマンスをさまざまな観点から測定する複数のテストが含まれています。スイートに含まれる各テストの結果は、セクション・スコア (「マーク」と呼ばれる) に合算され、特定の単位を用いて棒グラフで表されます。

Passmarkには、次の標準テスト・スイートおよびテストが用意されています。

**CPUテスト・スイート:** CPU演算をテストします。

- 整数 (32ビットおよび64ビットでの加減乗除)
- 浮動小数点 (32ビットおよび64ビットでの加減乗除)
- SSE (加算、減算、乗算などの128ビットでのSSE演算)
- 圧縮

- 暗号化
- 画像回転 (メモリ内での画像座標の回転)
- ランダムな文字列のソート
- 素数検索

**グラフィック・テスト・スイート:** Windowsの標準グラフィック関数を実行する一般的な2次元グラフィック機能をテストします。この種の機能は、企業向けコンピュータで多く使用されます。

- 線画: 500本ごとに色を変更しながら、テスト・ウィンドウ内に線を描画します。
- ビットマップ画像の描画: ウィンドウ内に、できるだけ高速にビットマップ画像を描画します。
- 輪郭の描画: ウィンドウ内に、楕円と角を丸めた正方形を描画します。
- フォントとテキスト: フォントとテキストの基本的なレンダリングを実行し、グラフィック・カードのパフォーマンスを測定します。
- GUI: グラフィック・カードのパフォーマンスと、GUIを操作するためのウィンドウ表示設定をテストします。このテストでは、ツリー・ビューやリスト・ビュー、スライダ、編集ボックスなどの標準GUIコントロールと、ウィンドウの移動やサイズ変更といった操作のパフォーマンスが測定されます。

**ハードディスク・テスト・スイート:** ファイルの読み取り/書き込み時のパフォーマンスを測定します。このテストについては、後ほど詳しく解説します。

**CD/DVDテスト・スイート:** CDドライブからデータを読み取る単一のテストを実行します。

**3Dグラフィック・テスト・スイート:** 3Dグラフィック・システムであるDirectXをテストします。企業向けコンピュータのパフォーマンスを測定する場合、通常このテストは実施されません。そのため、本書でも割愛しています。前掲の1つ目の図の結果部分に「Partial result」とあるのはこのためです。

図1に示されているように、ディスク暗号化が全体的なパフォーマンスに与える影響はごくわずかに留まっています。今回のテストでは複数種類のハードディスク・テストが実施されていることを考えると、これは重要なことです。以降のセクションでは、テストの構成、実施内容、結果について詳しく解説します。

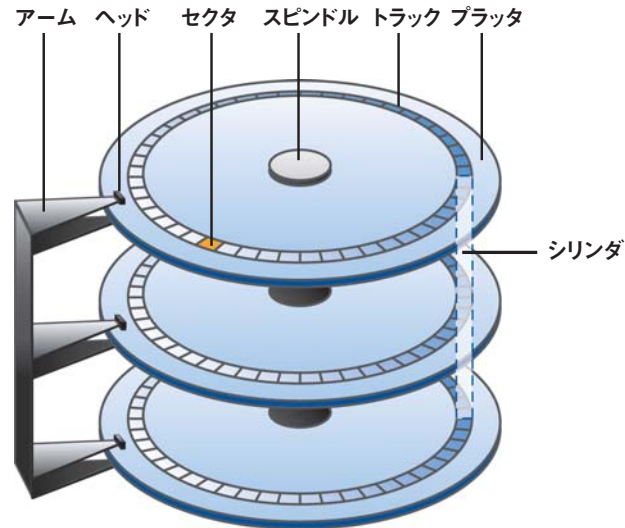
## パフォーマンスの考え方

### 暗号化ディスクのパフォーマンスの理解

暗号化はCPU負荷の高い処理です。これは、AESなどの効率的なアルゴリズムを使用している場合も同様です。効率性に優れたディスク暗号化プログラムは、低レベルのフィルタ・ドライバを使用して実装されており、ディスクに送られるすべてのデータを暗号化し、ディスクから読み取られるデータを復号化します。一般的には、暗号化フィルタ (暗号化アルゴリズム自体とフィルタ機能) が効率的であるほど、暗号化処理がコンピュータの全体的なパフォーマンスに与える影響は小さくなります。またクロック速度の速いCPUは、クロック速度の遅いCPUよりも高速にデータをフィルタに通すことができます。ディスクが低速である場合は、単位時間あたりにフィルタに渡すデータ量が少なくなるため、高速なディスクに比べてCPUの負荷が小さくなります。このほか、平均シーク時間などのハードディスク性能も暗号化処理に大きな影響を及ぼします。

## ハードディスクの構造

ハードディスクは、プラッタと呼ばれる円盤の層で構成されています。各プラッタは2つの面を持ち、同心円状の輪(トラック)で区切られています。各トラックはさらにセクタに分割され、このセクタが、ディスクに対して読み取り/書き込みを行うことのできる情報の最小単位となります。セクタは、アドレス指定が可能な最小のディスク要素です。



セクタにアクセスするには、操作ごとにトラックとセクタを指定する必要があります。ヘッドを動かすことなくアクセスできる単一ドライブ上のすべてのトラックは、シリンダと呼ばれます。各トラックの記憶容量はすべて同じであるため、内側のトラックほど記録密度が高くなります。これにより、読み取り/書き込みヘッドはトラックを問わず常に同じ速度で動作することが可能となっています。セクタのサイズは決まっていますが、一般的には512バイトです。通常、1つのディスク表面には数千のトラックがあります。I/O効率を向上させるため、メモリとディスク間のデータ転送は、1つ以上のセクタで構成されるブロック単位で行われます。

ディスクの動作は、シーク時間、回転待ち時間、転送時間という時間を発生させる3つの物理的な操作で構成されています。ディスク上のブロックにアクセスするため、システムはまず、ヘッドを目的のトラックまたはシリンダに移動する「シーク」という操作を行う必要があります。この操作を完了するまでの時間を「シーク時間」と呼びます。現在主流となっているマルチスレッド対応のオペレーティング・システムでは、複数のプロセスが同時にディスクにアクセスしようとするため、異なるトラックをシークするという状況が極めて頻繁に発生します。現在入手可能なハードディスクの平均シーク時間は、一般的なディスクで15ミリ秒(ms)以下、高性能なディスクで7ms以下です。

ヘッドが目的のトラックの位置に移動したら、今度は目的のブロックが読み取り/書き込みヘッドの下に回転してくるのを待機する必要があります。この時間を「回転待ち時間」と呼びます。平均的なハードディスクの回転数は1分あたり約5,000回(rpm)です。つまり、12msで1回転します。

通常、回転待ち時間は半回転分、すなわち約6msです。ただし、シークの場合と同様、これら平均の数値は、ディスク表面のある地点から目的のトラックまで読み取り/書き込みヘッドが移動する場合にのみ当てはまります。多くの環境では、回転待ち時間は平均よりも大幅に短くなる場合があります。読み取り/書き込みヘッドの直下に目的のデータが来たら、そのデータを転送できます。その際の転送時間は次の式で計算されます。

$$\begin{aligned} \text{転送時間} &= \text{転送するバイト数} \\ &\quad \times \text{回転時間} \\ &\quad / \text{トラック上のバイト数} \end{aligned}$$

1つのセクタの転送時間は、トラック上のセクタ数に依存します。例えば、トラックあたりのセクタ数が63である場合、1つのセクタを転送するのに必要な時間は1回転の1/63となります。ディスク・リクエストに対応するまでの合計時間は、シーク時間、回転待ち時間、転送時間の総和です。ほとんどのディスクではシーク時間の割合が最も大きいため、平均シーク時間を短縮できればシステムのパフォーマンスは大幅に向上します。ディスク・パフォーマンスを向上させるうえで最も重要なのは、シーク時間と回転待ち時間を最小限に抑えることです。しかしながら、企業における一般的な使用方法ではディスクはすぐに断片化してしまうため、この目標を達成することは容易ではありません。

### 一般的な断片化

ファイル・システムにおけるファイルは、ブロックと呼ばれる小片に分割されます。ディスクがまだ新しい場合、ファイルの各ブロックは一箇所にまとめて保存できます。このため、高速な連続読み取り/書き込みを行うことができます。その後、ファイルの追加や削除、サイズ変更が繰り返されると、ディスクは徐々に断片化していき、新しいデータに対して連続した領域を確保できなくなります。この状態で、新しいファイルが書き込まれたり、既存ファイルのサイズが大きくなったりすると、新しいデータ・ブロックはディスク上の連続していない領域に分散して保存されます。この結果、読み取り/書き込みヘッドのシーク時間と回転待ち時間が長くなり、データ・アクセス速度が低下することになります。図3は、完全デフラグの実行後わずか1ヶ月で、一般的なディスクがどれだけ断片化するかを示しています。



図3 ディスクを4週間使用した後の一般的な断片化パターン

## パフォーマンスのテスト方法

### ディスク・パフォーマンスを測定するテスト・スイート

実際のディスク・パフォーマンスを測定するにあたっては、Passmarkのパフォーマンス測定ソフトウェアを使用しました。真のディスク・パフォーマンスを導き出すため、本書では、標準ディスク・パフォーマンス・テストに焦点を絞り、「サイズが大きいファイル(200MB)の連続読み取り」、「サイズが大きいファイルの連続書き込み」、そして最も重要な「ランダム・シーク+RW」という3種類のディスク操作を使用してディスク・パフォーマンスのみを測定しています。

転送速度にはいくつかの要素が影響しますが、特に重要なのはディスクの元々のアクセス/シーク時間です。同じ条件下であれば、高性能なディスクほどデータ転送速度が高速になります。

システム・キャッシュもディスクの読み取り/書き込み速度に影響します。キャッシュとは、高速なデータ転送を行うために確保された特定のメモリ領域のことで、Microsoft Windowsは最近アクセスしたデータをこの領域に保存します。アプリケーションが同じデータに対する要求を繰り返し行う場合、そのデータがキャッシュに保存されていれば、要求のたびに復号化を行うことなく素早くデータを取り出すことができます。また、ディスクからデータを読み取る回数も減らすことができます。

ほとんどのアプリケーションはデフォルトでキャッシュを使用しますが、非キャッシュの読み取り/書き込み操作を要求する場合があります。Passmarkの基本テストでは、結果を比較しやすくし、想定外の結果とならないようにするため、キャッシュは使用されません。そのため、キャッシュされたデータに対して読み取り/書き込みを行う実際の使用方法と比較して、パフォーマンスは大幅に低くなります。

Passmarkの詳細テスト・オプションを使用すると、パフォーマンスを向上させるための設定を試すことができます。本書では、各システムの結果を比較しやすくするため、標準のディスク・テスト設定を使用しています。

すでに述べたように、実際の使用方法を最も正確に再現できるのは、断片化した典型的なディスクに対する操作に近い、ランダム・シーク+RWテストです。このテストの結果は、ディスクが暗号化されたシステムと暗号化されていないシステムのパフォーマンスの違いを最も正確に表します。

### テスト構成

本テストでは、2種類のPCを使用しています。Pentium III 750MHz、512MBのメモリ、60GBのハードディスク(5,400rpm/平均シーク時間12ms)を搭載したノートPCと、Pentium 4 3GHz、2GBのメモリ、10GBのハードディスク(5,400rpm/平均シーク時間9.4ms)を搭載したデスクトップPCです。いずれもOSはMicrosoft Windows 2000 Professional SP4です。

### テスト前の準備

効果的かつ正確にパフォーマンスを測定するため、次の点に留意しました。

- パフォーマンス・テストを実施する前に他のすべてのアプリケーションを停止する。これには、インターネット接続プログラム、自動アップデート・プログラム、タスクバー・プログラムも含まれます。
- ディスク・テストを実施する際にはアンチウイルス・プログラムを無効にする。多くのアンチウイルス・プログラムは、暗号化処理よりもはるかに大きな影響をパフォーマンスに及ぼします。
- テスト開始後は、他のアプリケーションを起動したり操作したりしない(マウスを動かしたり、Alt+Tabキーで他のアプリケーションに切り替えたりしない)。

- ディスク上のデータを適正な量にする。容量の使用率やクラスタ・サイズは、ディスクの読み取り/書き込みパフォーマンスに影響する場合があります。また、テスト・ファイルのディスク上の位置(内側のシリンダか外側のシリンダか)もパフォーマンスに影響を及ぼす可能性があります。この問題を回避する唯一の方法は、新規にフォーマットし、クラスタ・サイズを統一したディスクを使用することです。例えば、ディスクがほぼ満杯の場合は、フォーマット直後ではほぼ空の場合と比較して、パフォーマンスが50パーセント以上低くなる場合があります。
- ディスクの断片化は、パフォーマンスに悪影響を及ぼす場合があります。そのため、Windowsに付属のユーティリティを使用して、テスト前にディスクのデフラグを実行しています。暗号化ディスクのテストを実行後、非暗号化ディスクのテスト前にデフラグを実行することはしていません。テスト・ファイルの書き込み位置が変更され、結果が大きく変わる可能性があるためです。Check Point Endpoint Security Full Disk Encryptionは、テストを実行する前にMy Documents以下のフォルダにインストールしています。
- Windowsが実行するプロセスの中には、テストの正確性を低下させる可能性のあるものが存在します。そのため、正確な結果を得るためにテストを複数回または長時間にわたって実行することが必要になる場合があります。
- システムのパフォーマンスを正しく測定するには、適正な量のメモリが必要になります。テスト中にディスクへのスワップが発生すると、パフォーマンスと結果の正確性は大幅に低下します。

## Passmarkによるテストの実施

標準のディスク・テスト・スイートには、コンピュータのハードディスクを動作させる多数のテストが含まれています。これらのテストごとに、指定されたディスクのルート・ディレクトリに1つのファイルが作成されます。正しい測定結果を得るには、ファイル・サイズを大きくする必要があります。テスト・ファイルのサイズは200MB、読み取り/書き込みブロックのサイズは16KBです。Windows 2000/XPの場合、各テストではキャッシュなしの非同期ファイル操作が実行されます。

**連続読み取りテスト:** サイズの大きいテスト・ファイル(200MB)をディスク上に作成し、始点から終点まで連続読み取りを行います。

**連続書き込みテスト:** サイズの大きいテスト・ファイル(200MB)をディスクに書き込みます。ファイルの始点から終点まで連続書き込みを行います。

**ランダム・シーク+RWテスト:** サイズの大きいテスト・ファイルをディスクに作成し、ファイルをランダムに読み取ります。シークが実行され、ファイル・ポインタがファイルのランダムな位置に移動して16KBのブロックを読み取るか書き込むかした後、別のシークが実行されます。この際、実際の使用時に近い量のデータが転送されますが、具体的なデータ量はディスクのシーク時間によって大きく異なります。

「テスト前の準備」で述べた作業を実施した後に、Passmark Performance Test 6.0(以降)プログラムを開始します。デフォルトではC:ドライブが使用されますが、これは[Preferences]ダイアログ・ボックスで変更できます。まずは、非暗号化ディスクからテストを実施します。ツールバーにあるディスクのアイコンをクリックするか、メニューの[Test] → [Disk] → [All]を選択します。

直ちにテストが開始され(図4)、数分で結果が表示されます(図5)。

[File] → [Save as baseline]を選択し、このテスト結果を新しいベースライン(基準値)として保存します。ファイル名には、テスト内容が分かるような名前([Desktop 3.0GHz P4 Unencrypted.bt]など)を付けます。次に、ドライブを暗号化して再度テストを実行します。棒グラフのアイコンをクリックし、先ほど保存したベースラインを選択して[add]をクリックしてから、[OK]をクリックします。

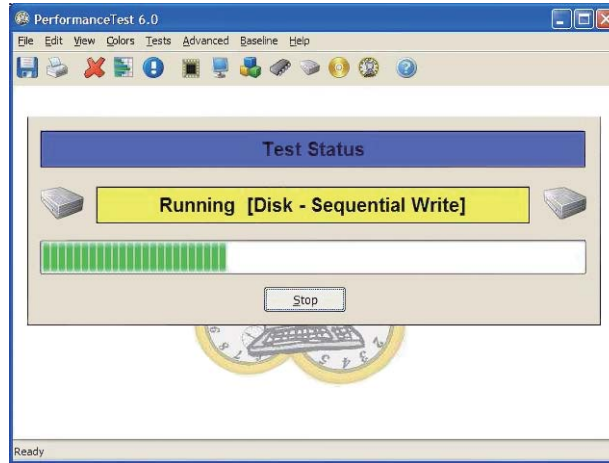


図4 Passmarkのディスク・パフォーマンス・テスト：手順1 テストの実行中

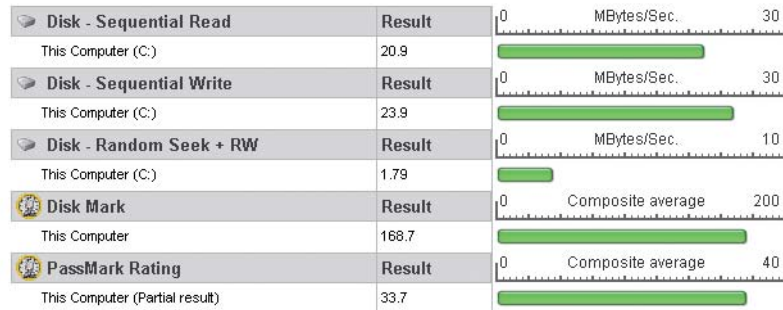


図5 Passmarkのディスク・パフォーマンス・テスト：手順2 結果の表示

2つのテスト結果を比較します（次項の「パフォーマンス・テストの結果」を参照）。

注意：次項「パフォーマンス・テストの結果」で示すのと同じ形式のグラフを作成するには、非暗号化ディスクのテストで説明したのと同様の手順で暗号化ディスクのテスト結果をベースラインとして保存し、その後PCの暗号化を解除してから再度テストを実行する必要があります。

### パフォーマンス・テストの結果

デスクトップPCとノートPCそれぞれのテスト結果を図6と図7に示します。

この結果からは、日常的な使用方法（ランダム・シーク+RWのテスト・ケース）の場合、テスト・プラットフォーム上での暗号化ディスクと非暗号化ディスクのパフォーマンスは、2.5パーセント～5パーセント程度しか変わらないということが分かります。これは、ほとんど無視できるレベルの差です。同じテストを複数回実行しても、この差は2パーセント～6パーセントの範囲に留まっています。

連続読み取りテストと連続書き込みテストにおける差はこの数値よりもかなり大きくなるものの、前述したように、実際のコンピュータの使用方法を考慮すればこの点は大きな問題にはなりません。ディスクを暗号化すると、起動に要する時間が多少長くなることがありますが、これは暗号化によって連続読み取り/連続書き込みのパフォーマンスが低下することに起因しています。コンピュータが起動した後やスタンバイ機能を使用する場合、認識できるほどのパフォーマンス低下は発生しません。

暗号化はCPU負荷の高い処理ですが、システムのパフォーマンスを左右するのは、暗号化のプロセスやCPU設定ではなくトラック間のシーク時間です。

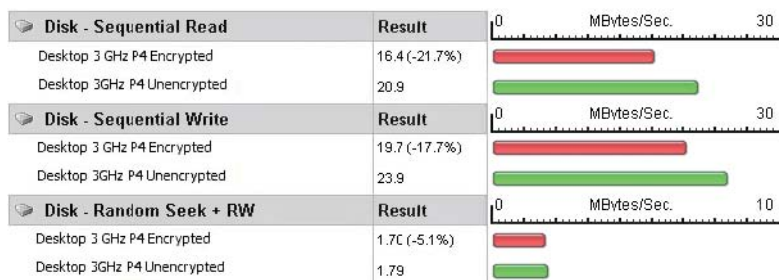


図6 パフォーマンス・テスト：暗号化ディスクと非暗号化ディスクの比較  
デスクトップPC (Pentium 4 3.0GHz、2GBのRAM、Windows 2000 Professional SP4)

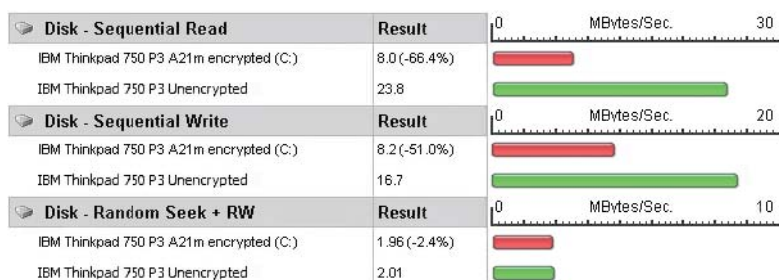


図7 パフォーマンス・テスト：暗号化ディスクと非暗号化ディスクの比較  
ノートPC (Pentium III 750MHz、512MBのRAM、Windows 2000 Professional SP4)

## まとめ

通常、ディスク暗号化製品がシステムのパフォーマンスに与える影響は、企業における一般的な使用方法ではほとんど無視できるレベルであると言えます。デスクトップPC/ノートPCのパフォーマンスが向上し、AESなどの効率的な暗号化アルゴリズムが登場したことにより、ディスク暗号化の有用性はかつてないほど高まっています。ハードディスクのデータ転送速度が頭打ちの状況にあるのとは対照的に、CPU性能が飛躍的に向上している今日、フルディスク暗号化製品と、重要データの暗号化漏れが発生する可能性があるファイル単位の暗号化製品とでは、前者に優位性があることは明らかです。

Passmarkパフォーマンス・テスト・プログラムの標準テスト・スイートでは、Check Point Endpoint Security Full Disk Encryptionがインストールされた普及価格帯のPCの全体的なパフォーマンスは、暗号化が行われていないPCと比較してわずか2.9パーセント劣るだけでした。

また、テスト・スイートの標準ディスク・テストで、企業における日常的なハードディスクの使用方法をシミュレートして実際のディスク・パフォーマンスを測定したところでは、暗号化ディスクと非暗号化ディスクのパフォーマンスには、2.5パーセント～5パーセント程度の差しかありませんでした。しかも、この2.5パーセントというわずかなパフォーマンス低下も、キャッシュを利用すればさらに小さくすることができます。

以上のことから、一般的なビジネス・ユーザの場合、データを保護するためにディスクを暗号化したとしても、それによってPCのパフォーマンスに実質的な影響が生じることはないということが、テストによって明らかになったと結論付けることができます。

## Check Point Software Technologies Ltd.について

チェック・ポイント・ソフトウェア・テクノロジーズ・リミテッド (www.checkpoint.com) はインターネット・セキュリティにおけるトップ企業として、世界中の企業向けファイアウォール、パーソナル・ファイアウォール、データ・セキュリティおよびVPN市場においてマーケット・リーダーとして広く認められています。チェック・ポイントは、ネットワーク・セキュリティ、データ・セキュリティ、およびセキュリティ管理ソリューションを含む広範囲なポートフォリオにより、ITセキュリティへのPUREなフォーカスを実現します。チェック・ポイントは、NGXプラットフォームを通じて、企業ネットワークおよびアプリケーション、リモート・ユーザ、支店・支社環境、およびパートナー各社のエクストラネットのビジネス通信およびリソースに対する広範なセキュリティ保護を実現する、統一されたセキュリティ・アーキテクチャを提供しています。更にチェック・ポイントは、業界をリードするデータ・セキュリティ・ソリューションである、Check Point Endpoint Security 製品ラインナップを通じ、PCやモバイル端末に保存してある各種企業データや重要なデータの暗号化と保護を提供します。数々の受賞歴のあるチェック・ポイントのZoneAlarm Internet Security Suiteとその他のコンシューマ向けセキュリティ・ソリューションは、世界中で何百万にも及ぶお客様のPCをハッカー、スパイウェア、および情報窃盗から未然に保護しています。またチェック・ポイントは、350社を超える各分野のトップベンダーが提供する“ベスト・オブ・ブリード”ソリューションとの統合および相互運用性を実現するフレームワークであるOPSEC (Open Platform for Security) により、自社ソリューションの能力をさらに拡大します。現在、チェック・ポイント・ソリューションは、世界中のパートナー・ネットワークを通じて販売、導入、サービス提供されています。チェック・ポイントの顧客には、Fortune 100社の全社と何万ものあらゆる規模の企業や組織が含まれています。

### チェック・ポイント・ソフトウェア・テクノロジーズ株式会社

〒160-0022

東京都新宿区新宿5-5-3 建成新宿ビル6F

E-mail : info\_jp@checkpoint.com

Tel : 03 (5367) 2500

<http://www.checkpoint.co.jp/>

©2003-2008 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Express, Check Point Express CI, Check Pointのロゴ, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpec, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Provider-1, PureAdvantage, PURE Security, puresecurityのlogo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, Zone Labsのロゴは、Check Point Software Technologies Ltd. あるいはその関連会社の商標または登録商標です。ZoneAlarm is a Check Point Software Technologies, Inc. Company. その他の企業、製品名は各企業が所有する商標または登録商標です。本書で記載された製品は米国の特許No.5,606,668、5,835,726、5,987,611、6,496,935、6,873,988、6,850,943、および7,165,076により保護されています。その他の米国における特許や他の国における特許で保護されているか、出願中の可能性があります。

### Testing the Impact of Encryption on Disk Performance

P/N:P/N 502823-J 2008.2

※記載された製品仕様は予告無く変更される場合があります。

