easyhashchecker について

Version 1.0_d20060207

本ドキュメントでは easyhashchecker の使い方について説明します。
最新の情報についてはプロジェクト・ホームページにて確認してください。

1. 本ツールの目的

easyhashchecker は何らかのメディアを媒介してファイルを移動／複製する際に,
そのファイルが正しく受け渡されたか検証することを目的とするツールです。
つまり, ファイルが破損しているか, 改竄されているか, といったことを確認できます。
ファイルの復元や, ファイルを正しく取得するためのツールではありません。
インターネットを経由するファイルの受け渡しでは, しばしば受け取ったファイルが部分的に破損している等の理由により本来の機能を果さないなどの分かりづらいトラブルも多く, ファイルが破損なく取得できたことを判断したい場合が多々あります。
このような状況において, ファイルの受け取り側が容易にファイルの破損チェックができるようにするために, 本ツールは作成されました。

2. 実現方法

ファイルの検証は, ファイルの指紋といえるハッシュ値を取得し, 配布元のハッシュ値と受け取ったファイルのハッシュ値を比較することで行います。
ハッシュ値のアルゴリズムとして MD5(Message Digest 5) もしくは SHA1(Secure Hash Algorithm 1)を用います。
これらのハッシュ値には, ファイルのサイズや内容が一部でも変更されると, その値もかわる性質があり, ハッシュ値が一致しなければ, その 2 つのファイルは異なる内容であると判断できます。
(まったく同じハッシュ値でありながら異なる内容である可能性もありますが, ほぼゼロと見なされるほど低い確率です。また, 同じ内容であれば同じハッシュ値となることは確実あるため, 「同じハッシュ値でなければ少なくとも同じ内容ではない」といえます。)
ハッシュ値は, ファイルのサイズに関わらず 16～20 バイトとコンパクトであり, またテキストファイルの形式であるため容易に配布することが可能です。

3. コンセプト／モチベーション

ファイルの内容が正しいかチェックする方法として広く md5 や sha1 が使われており, これらは sha1sum/md5sum といったツールを利用することで簡単に行うことができます。
しかし, Windows XP 等のエンドユーザ向けの環境には, これらのツールは存在せず, また, 使うためにコマンドラインの入力が要求されます。
これは md5sum や sha1sum に慣れていない初心者には難しいものと考えられます。
ハッシュ値の計算や検証を行うフリーソフトも多くあるものの, これらは汎用的に使うことが想定されており, インストール等の手順が必要です。
そこで, この easyhashchecker は, 配布するファイルと一緒に受け渡し先に取得してもらい, ダブルクリックするだけでファイルの検証を行い, 目的を達したあとは使い捨てることができる
『簡単で軽量』なツールとなることを目標としています。

4. 対応 OS

easyhashchecker は, 以下の OS で動作します。

- Windows 2000 (Professional/Server)
- Windows XP (Home/Professional)
- Windows 2003 Server

Windows95/98/ME では動作しません。

5. 特徴

1. 簡単であること。

ファイルの配布者は md5/sha1 の有用性について理解しており, それらのツールを使いこなせるとしても, ファイルの受け取り側が, それらの扱いに慣れているとは限りません。
そこで easyhashchecker では, ダブルクリックだけでファイルの検証を行えるようにしています。

2. 軽量であること。

ファイルの受け取り側の環境には特別なライブラリ等がインストール済みであることを仮定できないため, 実行ファイル(easyhashchecker.exe)単体で動作することが必要です。
また, ファイルを配布する際に, easyhashchecker.exe が目的とするファイルよりも大きなファイルであっては本末転倒ですから, 極力小さなサイズであることが望ましいといえます。
そこで easyhashchecker.exe は 15k bytes 程度のコンパクトなものとし, システム DLL 以外に依存しないものとします。
(ただし, md5/sha1 の計算などに Windows2000/2003/XP 以降の API を用いるため, Windows 95/98/ME では動作しません。)

3. 独自仕様でないこと

ファイルの受け渡し先のユーザが初心者ではなく md5/sha1 などを使い慣れており, そのための使い慣れたツールをもっている場合には, easyhashchecker を使わずに検証できることが望ましいでしょう。
あるいは, ハッシュ値の作成においても, すでに使い慣れたツールがある場合には, それを使いたいと思うことでしょう。
そこで easyhashchecker が生成／検証する md5/sha1 のフォーマットは md5sum/sha1sum と互換性のあるものとします。(バイナリモードのみをサポートします。)
ただし, easyhashchecker が扱うハッシュファイルにはシフト JIS(csWindows31j)を用いますので, 日本語ファイル名を使う場合は互換性が損なわれる可能性があります。
easyhashchecker で生成・検証を行う分には日本語ファイル名は問題ありません。

4. フリーであること。

easyhashchecker は誰でも無償で利用でき, 再配布も自由であることが望ましいため, 再配布に制限のある商用ライブラリは用いません。
また, この easyhashchecker には GPL(v2)ライセンスを適用します。

6. 使い方

1. ハッシュファイルの作成

これから説明するものは, ファイルを提供する側の作業です。

1. まず, 任意の新しいフォルダを作成し, そこに配布したいファイルをコピーします。
2. そのフォルダに easyhashchecker.exe をコピーします。
3. シフトキーを押しながら, easyhashchecker.exe をダブルクリックします。
   (シフトキーとコントロールキーを押しながら起動すると sha1 ハッシュの作成となります。)
4. ハッシュを作成するか問い合わせのダイアログが表示されるため「はい」を選択してください。
5. easyhashchecker.exe のあるフォルダの, すべてのファイルの md5 ハッシュが作成されます。ファイル名はハッシュ値を計算したファイル名の末尾に「.md5」をつけたものとなります。(既存のハッシュファイルは上書きされますので注意してください。)
6. ファイルは, 出来上がったハッシュファイルと easyhashchecker.exe とともに配布してください。
7. ファイルの検証方法を説明したテキストファイルも配布すると良いでしょう。

なお, 1 つのファイルに対して 1 つのハッシュファイルを作成しますが, これらは 1 個のファイルにまとめることもできます。(テキストエディタ等で連結してください。)

easyhashchecker はハッシュファイルの拡張子だけを見ており, ファイル名は識別しません。

ハッシュファイルの中には複数のハッシュをリストすることができます。

2. ファイルの検証

これから説明するものは, ファイルを受け取った側の作業です。

1. まず, 受け取ったファイルを新しいフォルダに保存します。
2. 拡張子が md5 もしくは sha1 のファイルも同じフォルダに保存します。
3. easyhashchecker.exe も同じフォルダに保存します。
4. easyhashchecker.exe をダブルクリックします。
5. easyhashchecker.exe のあるフォルダの拡張子 md5 もしくは sha1 からファイルの指紋を読み取り, 同じフォルダにあるファイルの指紋と比較した結果が表示されます。
6. 検証に成功すると「検証に成功しました」と表示されます。
7. 検証が成功したら拡張子 md5 もしくは sha1 ファイルと, easyhashchecker.exe は不要ですので削除してかまいません。

もし, 「**検証に失敗しました**」というエラーが発生したとき, そのダイアログに「ファイルがみつからないか読み込みに失敗しました」という表示がある場合, その左側に示される検証対象となるファイルが, そのディレクトリに存在しない可能性があります。

「**ハッシュ値が一致しません**」という表示がある場合, ファイルの検証を行った結果, そのファイルが元ファイルのハッシュ値と一致しない, つまり, そのファイルが元ファイルとは違う内容になっていることを意味しています。

「**ダイジェストファイル(*.md5/*.sha1)がカレントディレクトリに 1 つも見つからないため検証できません**」というエラーが発生した場合は, easyhashchecker.exe の起動時のカレントディレクトリに, 拡張

子 md5 もしくは sha1 のファイルがないため検証できないことを意味します。
このエラーが発生した場合は拡張子 md5/sha1 のファイルがあることを確認してください。

7. ソースコード

ソースコードは VisualC++.NET 2003 で作成されています。
必要に応じて GPL(v2)に従って修正してください。
バグ等があればプロジェクトホームページのバグトラッキングに報告していただけると幸いです。
また, もし修正された場合には, 必ず, ソースコードを zip 等にアーカイブしたものをパッチとして投稿してください。(「パッチ」である必要はありません。丸ごと一式でかまいません。)

8. ライセンス

このプログラムはフリーウェアです。
あなたはこれを, フリーソフトウェア財団によって発行された GNU 一般公衆利用許諾契約書(バージョン 2)の定める条件の下で再頒布または改変することができます。
このプログラムは有用であることを願って頒布されますが, *全くの無保証* です。
商業可能性の保証や特定の目的への適合性は, 言外に示されたものも含め全く存在しません。
詳しくは GNU 一般公衆利用許諾契約書をご覧ください。

ライセンスは GPL(v2)です。
商用, 非商用ともに自由にご利用, 再配布いただいてかまいません。
ソースコードを修正する場合は GPL(v2)に従ってください。
実行ファイルのみの再配布も可能ですが, その場合は以下の URL にアクセスできるように記載してください。

このソフトウェアに関する詳細, および問い合わせについては,
http://sourceforge.jp/projects/easyhashchecker/ で確認してください。