新感覚セキュリティRETURNIL(リターニル)の紹介・解説

■トップページ ＞PC・インターネット関係メニュー＞ ■管理者へメール

□RETURNIL2010設定説明はここ □RETURNIL2011設定説明はここ □よくある質問Q&Aはここ
□2ちゃんねる掲示板内 Returnilスレ（セキュリティ板）
＊2ちゃんねるスレで質問する前に既出かもしれないので過去スレを読むこと、スレの雰囲気を察して投稿すること。

＊サイトは公式サイトではありません。情報の取り扱いは自己責任でお願いします。

RETURNIL（リターニル）

パソコンを使う上で、アンチウイルスソフトをはじめとするセキュリティソフトを使用することは常識であり、マナーであるという時代です。

最近のアンチウイルスソフトは、総合セキュリティソフトへと変化してきており、様々なパソコントラブルのリスクを低減してくれます。
・・・そう低減してくれるだけ。 絶対安心ではないのです。

現在主流の定義ファイル更新方式は、どうしても対策が遅れますしマイナーウイルス（日本国内対象とか）への対策は更に遅れたり、対応する気がない？と思われるモノもあります。

最近定義ファイル式アンチウイルスソフトの欠点を補う興味深いソフトを見つけたので使用をはじめました。

それは「なかったことにしちゃう新感覚セキュリティ」RETURNIL（リターニル）

逆向きRが目印です。
Virtual System（バーチャルシステム）って書いてありますね。
バーチャル・・・仮想環境がこのセキュリティソフトのポイントです。

フルネームは Returnil Virtual System 略して「RVS」（2010）です。
Returnil2011 では System Safe（RSS)として、よりシステムの保護性が前面に出てきています。

☆現在主流のウイルス定義ファイル参照式ウイルスガードとその欠点を補う仮想モード保護を組み合わせたセキュリティソフトです。

詳細＆ダウンロードは→[RETURNIL 日本語公式サイト]（更新が遅い）
最新版のダウンロード（こちら推奨）は→[RETURNIL](こちらのWeb言語をEnglishのままでダウンロード)

参考までに
RETURNIL2010（RETURNIL Virtual System）仮想モード保護にウイルスガード付けましたって雰囲気
RETURNIL2011（RETURNIL Syatem Safe）ウイルスガードをはじめ総合セキュリティが強化されました。

有料版を使う場合、日本円よりドル決済のほうがお得かもしれません。

1）RETURNIL(リターニル）ってどんなソフト？

RETURNILには、現在主流の定義ファイル参照式ウイルス検出・駆除の機能とシステムドライイブ仮想化機能の２種類のシステムでパソコンを守るセキュリティソフトです。２０１１の製品版（有料版）ではさらに、システムの復元機能が追加されてます。

ここでは一般的に馴染みの薄い仮想モード保護を中心に説明してみます。

仮想モード保護機能を有効にすると、システムパーテーション（通常Cドライブ）のクローンを一時的に展開して全てのシステムパーテーション上の動作が展開されたクローン上で動作します。

「え？」って人が多いかと思うので具体的な例をあげてみます。

RETURNILの仮想環境下でウイルスに感染したとします。
ウイルスはシステムドライブに自身のコピー（ウイルス実行ファイル）を配置して、
さらにウイルスは起動毎に実行させるためにシステムのレジストリを書き換えます。
ついでにウイルスはシステムドライブ上にあった大切なデータを削除してしまったとします。

普通なら大切なデータは消えるし、これから起動する度にウイルスも起動してしまいます。
駆除するのにも専門的な知識が必要だったりします。

ところがRETURNIL仮想環境下でウイルスに感染したとしても、再起動するだけでウイルスも消滅、ウイルスに書き換えられたレジストリも元通り、さらにウイルスに消されたはずの大切なデータも元通り・・・。
まさに「ウイルス感染をなかったことにしてしまう」新感覚のセキュリティソフトです。

従来のウイルス定義ファイルでは検出できない未知のウイルス・スパイウエアといったマルウエアの感染に対して、一時的に感染は許したとしても、再起動すれば元通りになるというセキュリティソフトです。
さらに設定によっては、保護中に入り込んだウイルス実行ファイルの起動を禁止することができますので感染しても発症を無くすこともできます。

ほとんどのウイルスやスパイウエア等のマルウエアはシステムドライブであるCドライブに感染しますので、このシステムドライブ（Cドライブ）保護という考え方は安全度の高いものです。

RETURNILの仮想モード保護が開始されてもパソコンは違和感なく普通に使う事ができます。
システムドライブ（通常Cドライブ）へのファイルの追加や変更・削除といった動作は実際のドライブ上ではなく、RETURNILが展開した仮想領域（ドライブの特定領域）に反映されます。それでいて、それを参照したりするソフトは問題なく動作します。仮想領域上に新たにインストールしたソフトさえ問題なく動作します

そして再起動すると、それまでの仮想領域は破棄されるので全てが元通りになるのです。

学校とかネットカフェとかでは、再起動で元通りという同種のソフトは珍しくありませんが、RETURNILはパーソナルに気軽に使え、しかもFree版は無償でも使えるというのがポイントです。

しかし、RETURNILの動作をよく理解した上で使わないと失敗する事もあります。

仮想モード保護下でシステムドライブ（通常Cドライブ）への変更は全て無効（なかったことになる）になるので、新しいソフトのインストールや、各種自動アップデートも無効にされるばかりでなく、例えばエクセルで作ったモノをCドライブに保存しておくと、再起動と同時に消滅します。
ブラウザのお気に入りの追加や履歴・各種ソフトのログも全て消滅します。
メールを受信してもCドライブがメールの保存先なら消滅します。

もちろん、送信したメール、他のサイトへの変更（書き込み）、他のドライブのデータへの変更はそのまま残ります。 万がーウイルスに感染して外部へ情報が漏れた場合、その漏れた情報については取り消せません。

保護されるのは自分のパソコンのCドライブのみってのをしっかり頭に入れておけば賢い使い方ができます。

通常の作業のデータ保存はCドライブ以外を使えばいいし。消したくないデータはパソコンをシャットダウン（再起動）する前に別のドライブに保存しておけば良いしね。

私のパソコンにはCドライブしかありませんって方でも、RETURNILには別のドライブ（仮想ドライブ＞ディスク上への変更が保存される）をマウントする機能があるので大丈夫です。

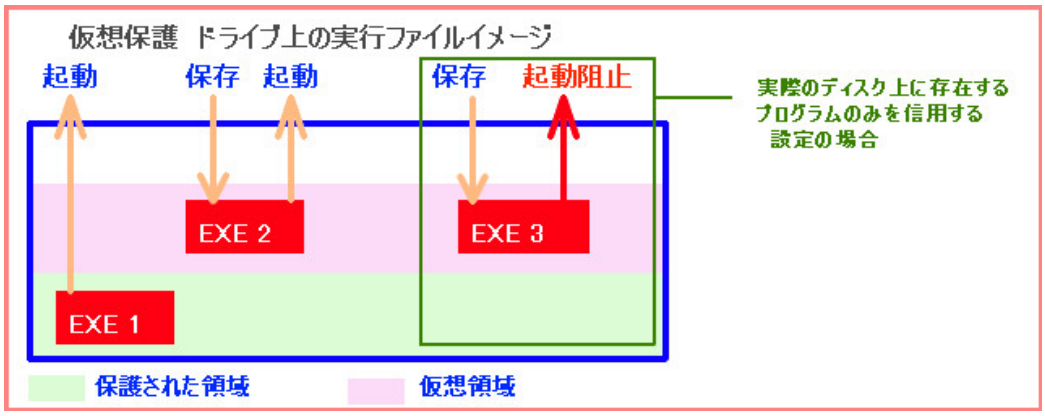
新しいソフトのインストール・Windowsや別のソフトの自動更新・あるいは別のセキュリティソフトの定義ファイル更新等は、それを行った後に仮想環境を実行すれば大丈夫です。

・・・ここまで書いたのを見て、少し面倒そうって思った方・・・それ正解です。

確かにRETURNILは他の一般的なセキュリティソフトと違い、ソフト動作への理解とちょっと使い方にコツが必要です。でもその使いこなしが出来ていれば、一般的なセキュリティソフトよりも遥かに安全な環境を作れます。

下の図はRETURNIL（リターニル）で仮想モード保護を有効にした状態でのCドライブイメージです。
（技術的に実際の動作を示したものではなく、あくまでもイメージ図です。）

〇実行ファイル（アプリケーション）のイメージ



A） 既存の実行ファイルEXE1は通常通り起動して実行できます。

B） 仮想モードで保存（インストール）した実行ファイルEXE2は、仮想領域に保存されますが普通に起動して実行できます。

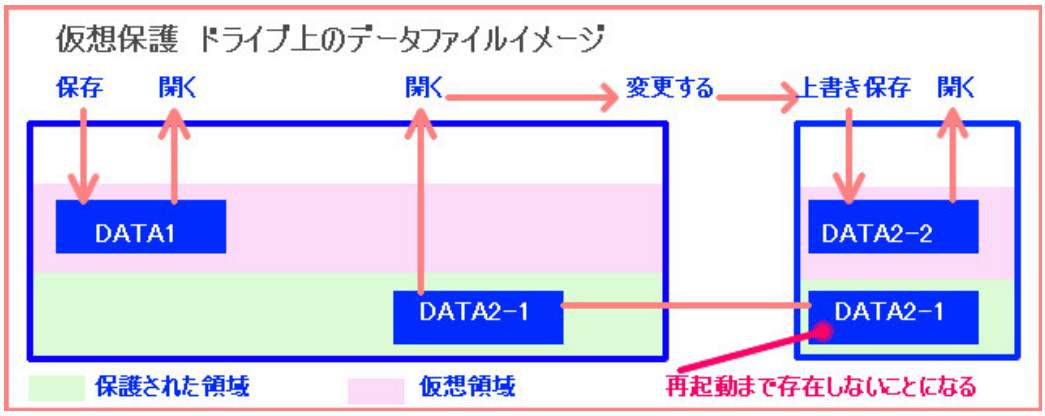
C）「実際のディスク上に存在するプログラムのみを信用する」という設定にした場合は、仮想環境下に実行ファイルEXE3は保存（インストール）されますが、起動実行することはできません。

再起動することにより、仮想領域のファイルは消滅します。

Bパターンは、一時的なアプリケーションソフトを使う場合、あるいは試用してみる場合に便利です。
（インストールに再起動を必要としないソフトに限る）
但し、この場合はウイルス等に感染してもウイルスが動作する事になります。
もちろん再起動すればアプリケーションだろうがウイルスだろうが消滅します。

Cパターンのような設定をすると、ウイルスに感染してもウイルスが動作できなくなり安全度が高まります。
もちろん、再起動で消滅します。この状態では万が一情報漏えいに関するウイルスに感染したとしても、ウイルスが活動できずに情報漏洩の被害さえ食い止める事ができます。

○データファイルイメージ



D） DATA１のように仮想モードでデータファイルを保存すると仮想領域に保存されますが、普通に開く事ができます。再起動することによって消滅します。

E） DATA２－１のように既存のファイルも当然普通に開くことができます。
それをアプリケーションで変更して上書き保存したものがDATA２－２です。
上書きされた以後、元データのDATA２－１は保護された領域に存在しますが、再起動して仮想領域が破棄されるまでは存在しないファイルとして扱われます。（仮想モードでDATA2−1を消去しても基本は同じ）
もし変更したDATA２－２が必要な場合は、他のドライブに移動やコピーして破棄されないようにします。

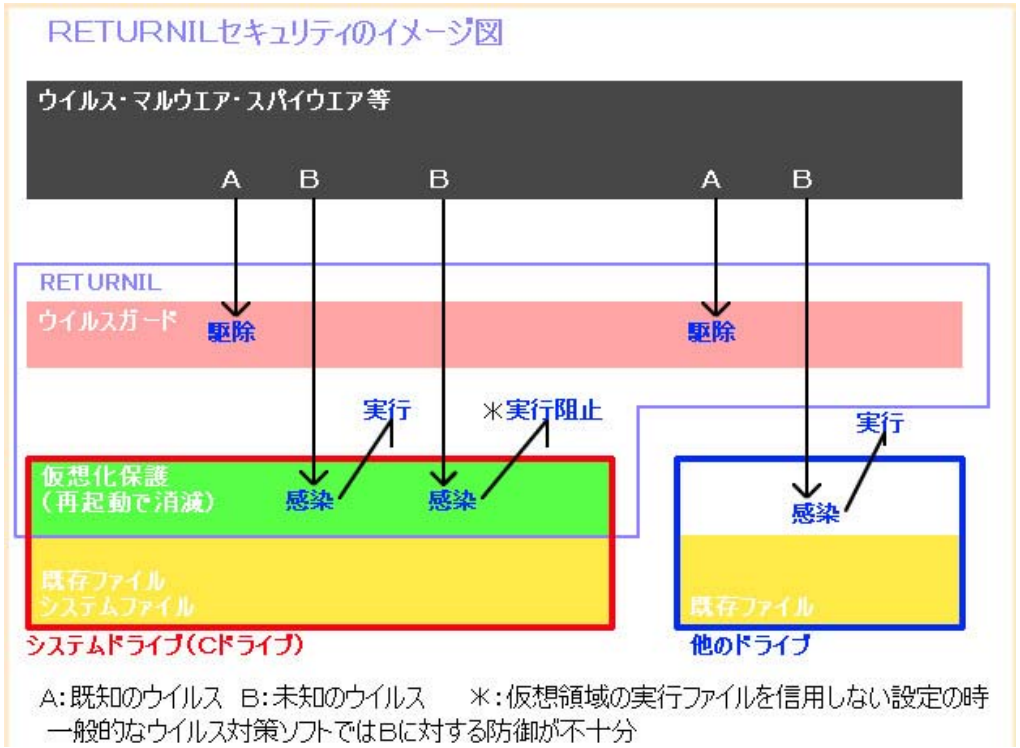
DATAという書き方をしましたが実行プログラムでも扱いは一緒です。

そしてパソコンを再起動することにより、ピンク色の仮想領域は消滅し元からの保護された領域が残ります。

もし上の説明で変更されたデータDを今後も使いたい場合は、再起動する前に保護されてない別のドライブに一度保存して仮想モード保護を有効にしてない時に保護領域に上書きするか、有料版だけの機能であるファイルマネージャーを使用して保護された領域に保存します。

一般に馴染みのない仮想モード保護について書いてきましたが、RETURNILには定義ファイル参照式のウイルスガード機能（一般的なアンチウイルス対策ソフトの検出機能）もついてますので、通常のパソコン使用ではウイルスガードのみを使用して危険を感じたら仮想モード保護をONにするという使い方もできます。

○RETURNILセキュリティの総合イメージ図



＊ウイルスガードと仮想モード保護は独立して制御（OnOff）できます。
＊システムドライブ以外に感染したとしても、システムドライブが保護されていれば再起動後にウイルスが自動的に活動する事は極めて困難です。
＊RETURNILL２０１１の製品版（有料）には、さらにシステムの復元機能が追加されています。

一般的なセキュリティとしては、これにファイアーウォールソフト（FW)を組み合わせる事で基本を抑えた事になります。（XP-SP2以後 Windowsには標準でFW機能がついてます）

＜参考＞
現状では、RETURNILの仮想モードのみを使い、ウイルス対策ソフトには別のソフトを使ってる人が多いようです。自分の判断で定義ファイル参照式のウイルスガードを信頼できるのであればRETURNILだけでも問題ありません。RETURNILの定義ファイル式ウイルス対策エンジンは F-PROT Antivirus （FRISK Software International ）を使用しています。

２）RETURNILの応用的な使い方

RETURNILはウイルスや他のマルウエア感染をなかった事にしてしまう以外にも、便利な利用方法があります。

場合によってはウイルスとかマルウエアにわざと感染して挙動を見るとかも可能です。（推奨しません！）

他にも、セキュリティ意識の乏しい子供にパソコンを使用させる時に、あるいは友人や知人に使わせる時に仮想モードさせて使用させれば、まさかのトラブルも少なくできます。

一時的に必要になったソフトウエアのインストールや、試験的にインストールして動作させてみる時も便利です。ソフトウエアを使用して再起動すればレジストリを汚す事もありません。
（インストールに再起動を必要とするソフトを除きます。）

また再起動を要しないパソコンシステムやソフトウエアの設定変更を試してみるときも安心です。

またインターネットの履歴や一時ファイルも残さないので、履歴を残したくない時にも良いかもしれません。

それから、WindowsOSは使い込む程重くなるという傾向がありますが、仮想モードでの使用をメインにするとそれらも防げると同時に時間のかかるHDDデフラグの頻度も少なくする事ができます。結果的にパソコンそのものの寿命が延びるかもしれません。

何よりも仮想モードを常にONにしてパソコンを使うようにすれば、従来の対策ソフトでは感染を防げなかった新種（未知）のウイルスなどのマルウエアの感染を強力に防いでくれます。

３）RETURNILを使う上での注意点

仮想モード保護をいつも行ってるとWindowsの正常な終了処理が結果的に行われない事になるかもしれませんので、時々仮想モード保護をせずにWindows起動して何もせずに１０分程度安定させた後再起動をしましょう。

また新しいソフトのインストールやバージョンアップ更新があった場合も、保護せずに一度だけWindowsを普通に再起動させてから仮想モード保護を行った方がトラブルの危険が小さくなると思われます。

☆RETURNILは軽くてパソコンへの負担が少ないソフトなので、筆者としては今お使いのセキュリティソフト（アンチウイルスソフトやファイヤーウォール）と組み合わせて使う事を推奨します。
他のアンチウイルスソフトと組み合わせて使う場合はVirusGuard(ウイルスガード）機能は無効にしておきましょう。

☆インストール直前にCドライブのデフラグを実行した後にインストールする事を推奨します。
これにより、仮想領域断片化や仮想ディスクのマウントの不具合によるトラブルが減少するようです。

☆仮想保護を使用していいる時はデフラグを絶対しないで下さい。特に自動でデフラグの設定等は必ず無効にしておきましょう。

＜重要＞
万が一仮想モード保護中にウイルスやマルウエアに感染した場合に、ウイルス等が外部との通信を行おうと

した場合それを阻止する事は仮想モード保護機能だけではできません。もちろん、再起動後は通信機能を持つウイルスや通信によってダウンロードさせられた他の悪意あるファイルは消滅します。(外部に漏れた情報情報をなかったことにする事はできません)これを防ぐにはファイアーウォールを合わせて使いましょう。(Windows標準でもないよりはマシです)

ただし設定によっては感染した実行ファイルの起動を阻止できるので、その場合は例え通信機能を持つウイルスであっても情報漏えいの危険性は著しく減少します。

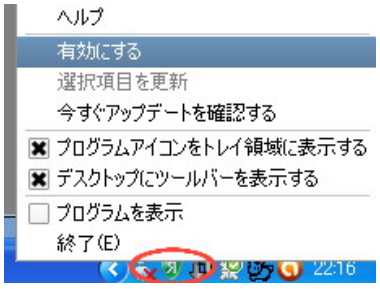
4)実際のRETURNIL

下がRETURNILのメインパネルです。(RETURNIL2010のもの)
VirusGuard(ウイルスガード)は よくある定義ファイルを使ったウイルス検出機能です。
そしてSystem Safe(システムセーフ)が 仮想システムの機能です。

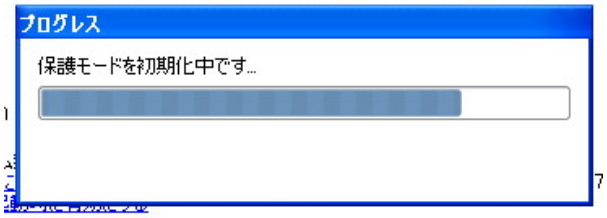
下の図はRETURNIL2011のメイン画面(UIが整理された感じです)

筆者はウイルス検出機能は他のソフトを使ってるので、仮想システムだけを必要に応じて使ってます。
起動時から自動的に仮想モード保護状態にする事も可能ですが、Windowsをはじめ様々なソフトの自動アップデートが欠かせないと感じてるので（仮想状態では無効になります）、必要に応じて仮想モードに入れるという使い方をしています。

仮想モード保護に入るには、このメインパネルを開かなくても、タスクトレイのアイコンを右クリックメニューから有効にできます。



有効にすると　下のような　仮想モードの準備に入り、まもなく仮想モードに入ります。
通常１０秒以下で仮想状態に入る筈です。



仮想モード環境下でパソコンはそれまでと変わりなく普通に使用することができます。

そして、再起動することにより、システムドライブ（Cドライブ）への変更は全て無効に・・・・

現在RETURNILを使う人の多くは他のウイルス対策ソフトを併用しています。
RETURNILは他のセキュリティ総合ソフトに比べると軽快である為、このような使い方をしても重さを感じる事はありません。

5）Cドライブへの変更が無効になる事が嫌という方へ

RETURNIL最大の特徴であるCドライブの保護は同時に、このソフトの使用を敬遠させるモノであるかもしれません。でもセキュリティやデータの保護を真剣に考えてる人にとってはなんら問題のない部分です。

Cドライブは通常システムドライブとして使います。そこにはOS(Windows)の大切なシステムや様々なアプリケーションソフトが格納されています。しかし、ほとんどの場合このCドライブはパソコンハードに最初から組み込まれているものであり、パソコンと運命を共にする事が多いドライブです。

パソコンもHDD（ドライブ）もいつかは壊れます。CドライブはHDDドライブの障害だけじゃなく、パソコン本体の障害と運命を共にする事が多いので、壊れるリスクはさらに高まります。OSやアプリケーションは新しくインストールすれば復活できますが、作成したデータは失われれば取り戻す事ができません。
この事を知ってるユーザーは大切なデータは必ずバックアップを取りますし、データー保存先をCドライブ以外や外部のHDDをメインにする人が少なくありません。

Cドライブはシステムとアプリケーション、保存するデータも一時的なモノという認識で使用するなら
RETURNILのCドライブ保護は歓迎されるべき機能です。たまにあるOSの更新やアプリケーションのアップデートの時だけ保護を無効にすれば良いのですから。

セキュリティと大切なデータ保護を考慮した上でのドライブ（記憶メディア）の使い方をもう一度考えてみませんか？

＊2010年7月作成　以後加筆＆修正

＊このページは筆者の個人的な経験と知識・公式サイト及び2ちゃんねる掲示板の同ソフト関連スレを参照しながら製作してます。

▲一番上に戻る▲

制作：2010　最終更新：2010

-Web Site Copains(コパン)-