

2005年11月10日

**急激に増え続けるスパイウェアから個人情報を保護
スパイウェア検出・除去ソフト「Spybot Search & Destroy V1.4」
11月18日(金)から販売開始**

キヤノンシステムソリューションズ株式会社(本社:東京都港区、代表取締役社長:浅田和則)は、スパイウェアの検出を更に強化したスパイウェア検出&除去ソフトの最新バージョン「Spybot Search & Destroy V1.4」を2005年11月18日より販売開始いたします。

「Spybot Search & Destroy」は、インターネット経由で第三者に個人情報などを自動的に送信してしまう隠れた脅威(スパイウェア)を検出・除去するソフトウェアです。30,000以上(2005年10月時点)の定義データを使用し、侵入したスパイウェアの検出・除去を行うだけでなく、スパイウェアやハッカーツールの強制ダウンロードも阻止します。また、レジストリ情報の書き換え行為を検出するため、システム設定の保護もできます。

さらに、パソコンに不慣れな方でも簡単にスパイウェアを検出・除去できる標準モードと、より専門的な操作を行う詳細モードを装備しています。詳細モードでは、書き換わってしまったブラウザのスタートページを元に戻したり、システムスタートアップやインストールされたActiveXおよびBHO(ブラウザヘルパーオブジェクト)を無効化したり、通信しているプロセスを特定することなどができます。



Spybot Search & Destroy の主な特長

- ・高速処理でスパイウェアを検出・除去 (強化)
- ・常駐保護でブラウザセキュリティを向上 (強化)
- ・リカバリー機能で除去ファイルを復元
- ・選べる2モード設定 (標準モード・詳細モード)

販売情報

製品名	希望小売価格(税別)	販売開始日
Spybot Search & Destroy V1.4	¥5,000	11月18日
Spybot Search & Destroy V1.4(ダウンロード版)	¥3,000	11月18日

次年度更新料 年間 ¥2,000(税別)

本製品はご登録後1年間のサポートおよびオンラインによる更新がご利用いただけます。

企業様や教育機関様向けに、ライセンス販売も行っています。

尚、目標販売本数は、初年度3万本です。

動作環境

[対応 OS/CPU/メモリ]

OS	CPU	メモリ
Windows 98/98SE	133MHz 以上	64MB 以上
Windows Me	150MHz 以上	64MB 以上
Windows NT4.0 (SP6)	133MHz 以上	64MB 以上
Windows 2000	133MHz 以上	64MB 以上
Windows XP	300MHz 以上	128MB 以上

[ハードディスク] 15MB 以上の空き容量

[その他] インターネット接続環境必須

Internet Explorer 5.5 (Service Pack 2 以降) 以上

開発元情報

Spybot Search & Destroyの開発元である Safer Networking社は、Spybot Search & Destroyを開発した、Patrick M. Kolla氏によって2003年アイルランドに設立されたセキュリティソフトウェア開発会社です。開発は、ドイツ連邦共和国のボーフムで行われています。

[<http://www.safer-networking.org/en/index.html>]

Spybot Search & Destroy は、Safer Networking 社の商標です。

Microsoft、Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。

その他の製品名および社名などは各社の商標または登録商標です。

お客様からのお問い合わせ先(記事などへの掲載用)

キヤノンシステムソリューションズ株式会社

住所 : 〒108-0073 東京都港区三田 3-11-28

TEL : 03-5730-7198 (土日祭日を除く、10:00 ~ 12:00、13:00 ~ 16:30)

E-mail : spybot-info@canon-sol.co.jp

URL : <http://canon-sol.jp/>

報道関係からのお問い合わせ先

キヤノンシステムソリューションズ株式会社 コミュニケーション企画部

住所 : 〒108-0073 東京都港区三田 3-11-28

TEL : 03-5730-7108 FAX : 03-5730-7101

E-mail : comdep@canon-sol.co.jp

Spybot Search & Destroy の主要機能

1. 高速処理でスパイウェアを検出・除去【強化】

30,000 以上(2005 年 10 月時点)の定義データを使用し、個人情報流出の原因となるスパイウェアやハッカーツールなどの危険なプログラムを高速に検査し、安全に除去を行います。使用履歴や Cookie といった様々な情報も検出し、さらにメモリ上に展開してしまうスパイウェアを、システムの再起動時に自動除去することができます。

2. 常駐保護でブラウザセキュリティを向上【強化】

ブラウザに常駐させることにより、スパイウェアやハッカーツールの強制ダウンロードを阻止できます。これにより、スパイウェアを侵入の段階で阻止することが可能です。また多くのスパイウェアが実行するレジストリの書き換え行為を検出し、システム設定を保護します。 1 Internet Explorer に対応

3. リカバリー機能で除去ファイルを復元

スパイウェアやレジストリの情報などを除去する際、自動でバックアップをとるため、誤って除去した重要なファイルを復元することができます。これにより、スパイウェアとして判断しにくい場合でも安心して除去することができます。

4. 選べる 2 モード設定 (標準モード・詳細モード)

パソコンに不慣れな方でも簡単にスパイウェアを検出・除去できる標準モードと、より専門的な操作を行う詳細モードを装備しています。詳細モードではスパイウェアの感染から復旧するための様々なツールが揃っており、書き換わってしまったブラウザのスタートページを元に戻したり、システムスタートアップやインストールされた ActiveX および BHO(ブラウザヘルパーオブジェクト)を無効化したり、通信しているプロセスを特定することなどができます。

5. その他機能(詳細モード機能)

- ・定義ファイルの更新
- ・スキンの変更
- ・hosts ファイルの表示・項目の削除
- ・アンインストール情報の削除・一覧の表示
- ・検査対象からの除外設定
- ・システム情報の表示・書き出し
- ・実行プロセスの終了・一覧の表示
- ・Winsock LSP の一覧の表示
- ・検査のスケジュール設定
- ・ActiveX、BHO の無効化・一覧の表示
- ・通信プロセスの表示
- ・検査結果の統計情報の表示
- ・検査や除去などのログ保存・表示
- ・ブラウザのスタートページ変更・一覧の表示
- ・システムスタートアップの無効化・一覧の表示
- ・有効期限の表示