




はじめに

このたびは「Spybot Search & Destroy」をお買い上げいただきまことにありがとうございます。
とうございます。

このユーザーズガイドには、本製品のインストールから実際の使用方法までが記載されています。本製品を正しくご利用いただくために、必ずこのユーザーズガイドを一読されておくことをお奨めします。

また、説明に用いている用語や画像は本製品の開発段階のもので、今後、本製品の更新機能を利用することにより、予告なく画面の表示などが変更される場合があります。予めご了承ください。

マニュアルの表記について

- ・ Spybot Search & Destroyをインストール後、設定の変更を全く加えていない状態を「既定値」と表記しています。
- ・ アイコンやボタンなどに  ポインタを合わせ、マウスの左ボタンを1度押すことを「クリック」、すばやく2回押すことを「ダブルクリック」、マウスの右ボタンを1度押すことを「右クリック」と表記しています。
- ・ ダイアログなどのチェックボックス、及びラジオボタンをクリックし、  の状態にすることを『チェックを「オン」にする』と表記しています。

商標

Microsoft、Windows、Windows NT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、記載されている会社名、製品名は各社の登録商標または商標です。

ソフトウェアライセンス契約書

本ライセンス契約は、Spybot Search & Destroy（以下「本製品」とします。）の使用許諾に関する、お客様とアイルランド共和国法人Safer Networking, Ltd.（以下「Safer」とします。）との法的な契約です。お客様が、インストールの過程で、合意を示すボタンあるいはチェックボックスをクリックする、あるいは、本製品が電子媒体（CD-ROM）で提供されている場合、当該媒体（CD-ROM）の梱包を開梱することで、本契約に同意したものと見なされます。本契約に同意されない場合、ダウンロードで購入された場合には、購入元に、電子媒体で購入された場合には、付属文書を含むパッケージ全体を、ご購入の確証を添付して、購入元もしくは販売代理店キヤノンシステムソリューションズ株式会社（以下「販売代理店」とします。）に返品下さい。お客様が購入された金額を返金いたします。

第1条（定義）

本契約の用語は以下の各号の定義に従うこととします。

- 「本製品」とは、Patrick M. Kolla氏等が開発し、Saferが使用許諾権を有するパッケージソフトウェアSpybot Search & Destroyおよびその関連文書を言います。
- 「使用」とは、本製品を1台のコンピューターにインストールし、当該コンピューターの内部から外部に不当に通信するソフトウェア（総称して「スパイウェア」といいます。）を発見するために、使用することを言います。
- 「アップデート」とは、ユーザーインターフェースの変更を含まない、本製品に関するデータの更新を言います。
- 「アップグレード」とは、ユーザーインターフェースの変更を含みそれに限定されない、全面的な本製品の更新を言います。

第2条（使用許諾）

- Saferは、お客様に対し、本製品の1台のコンピューター上で（CPUを搭載し入出力制御機能を備えた基盤一式を1台とします。）の使用を許諾します。本製品を、複数のコンピューターにインストールし使用する場合には、台数分のライセンスを購入する必要があります。本製品を一時的に他のコンピューターに移転して使用すること、および、ネットワーク接続された他のコンピューターに対して、本製品を使用することはできません。本製品を当初インストールされたコンピューター以外のコンピューターに使用する場合、お客様は、本製品を恒久的に移動するものとし、他のコンピューターにインストールした上で、元のコンピューターに本製品を残すあるいは再インストールすることは、当該他のコンピューターが元のコンピューターの故障等で使用できない場合の一時的な代替である場合を除き、認められません。
- お客様は、本製品のソフトウェアを保管目的で必要最低限の数量のみ複製することができます。

第3条（サポートとアップデート）

本製品はご購入（ご登録）から1年間無償にてサポートおよびアップデートが、提供されます。アップデートの入手については、販売代理店のホームページを参照下さい。また、アップデートの利用については、本契約の規定が準用されます。なお、ご購入から1年間経過した以降のサポートおよびアップデートの入手については、販売代理店のホームページを参照下さい。

第4条（アップグレード）

本製品のアップグレードが、場合により、Saferの選択により、有償または無償で提供されます。アップグレードが、単独で動作可能なものである場合にも、お客様はアップグレードを本製品がインストールされたものと異なるコンピューターにインストールし、使用することはできません。但し、お客様が恒久的にコンピューターを変更する場合には、この限りではありません。

当該アップグレードの使用については、当該アップグレードに添付されるライセンス契約があり、その規定が適用される場合を除き、本契約の規定が適用されます。

第5条（禁止事項）

- お客様は、本製品を本契約により明示された以外で、複製することおよび送信可能化すること、送信することを禁止されています。
- 本製品を使用するためのシリアル番号は、Saferならびに販売代理店キヤノンシステムソリューションズ株式会社の営業秘密です。お客様は、本契約で認められる譲渡の場合を除いて、第三者に当該シリアル番号を開示することを禁止されています。
- お客様は、法令で禁止されている場合を除き、本製品をリバースエンジニアリング・デコンパイル・その他の手法で解析することは禁止されています。
- お客様は、本製品を本製品の機能として組み込まれている変更可能な部分以外で、改変・改造・変更・翻訳することを禁止されています。当該変更が必要な場合には、販売代理店を通じSaferへご連絡下さい。Saferおよび販売代理店の選択により、別途当該変更が加えられた本製品を販売できる場合があります。

第6条（譲渡）

お客様は、本製品を恒久的にお客様のコンピューターから削除し、パッケージの全てを被譲渡人に渡す場合、または、当該コンピューターを譲渡する場合で、かつ、本契約の条項を被譲渡人が遵守し、譲渡人から販売代理店に、被譲渡人への譲渡が連絡される場合に限り、第三者に譲渡することができます。

第7条（免責）

本製品が第三者の知的財産権を侵害していることを理由として、お客様に対し当該第三者より請求がなされた場合には、Saferおよび販売代理店が、責任を持って対応することとし、お客様を免責致します。但し、当該請求の事態が速やかに販売代理店に連絡されない場合にはこの限りではありません。

第8条（保証限定）

Saferおよび販売代理店は、本製品を使用している場合でも、お客様がコンピューターに登録された情報およびお客様のコンピューターに一時的あるいは定期的に記録された情報の一部あるいは全てが、外部に不適切に送信されないことを保証いたしません。また、本製品を使用して情報がコンピューターから不適切に削除されることにより生じる、お客様のコンピューターの使用上の不具合、および、お客様と第三者の間の通信の障害について、それが生じないことを保証しません。本製品により検出された、全てのプログラムおよびデータの削除および変更については、お客様が自らの危険負担により行うものとし、本製品の使用あるいは使用できないことにより発生した、経過的、派生的損害については、本契約に明示されているものを除き、Saferおよび販売代理店は一切の責任を負いません。

本契約に基づく賠償責任は、本契約に明示されている場合を除き、お客様の購入額を上限といたします。

第9条（契約の解除）

お客様が本契約の条項の一に違反した場合、Saferは、お客様への通告により、ただちに本契約を解除することができます。お客様はまたいつでも通告無く本契約を解除することができます。本契約が解除された場合、お客様は、ただちに本製品の使用を中止し、本製品をコンピューター上より削除し、本製品の複製物を含むすべての有形物を廃棄することとします。

第10条（一般条項）

本契約の管轄法は日本法とします。

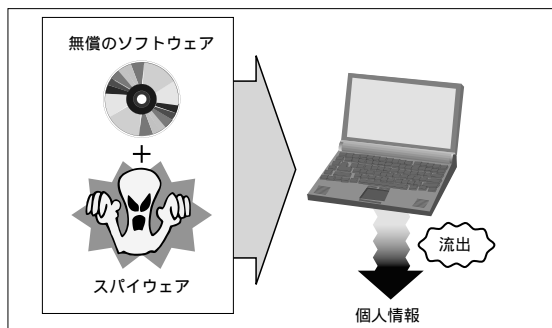
目次

はじめに	1	
ソフトウェアライセンス契約書	2	
目次	3	
Part 1 概要		4
スパイウェアとは何か	4	
スパイウェアの目的	4	
スパイウェアとウイルスとの違い	5	
本製品の特長・動作環境	6	
本製品の特長	6	
動作環境	7	
Part 2 導入		8
インストール方法	8	
Part 3 利用		12
起動方法と基本画面について	12	
Spybot S&Dの起動方法	12	
基本画面の構成	14	
「検査と除去」実行前に「更新」を行う	16	
「検査と除去」機能でスパイウェアを除去する	18	
スパイウェアの検査から除去までの手順	18	
「検査と除去」画面構成	21	
検査結果の見方とスパイウェア等の除去について	22	
Part 4 便利な機能を利用する		24
「リカバリー」機能で除去ファイルを復元する	24	
「保護」機能でスパイウェアを防御する	26	
「TeaTimer」機能でシステム設定を防御する	28	
Part 5 付録		30
アンインストール方法	30	
FAQ	31	
Part 6 サポート		34
サポートについて	34	
お問い合わせ	34	
ユーザー登録のお願い	35	
お問い合わせシート	36	

スパイウェアとは何か

スパイウェアとは、何らかの形でコンピュータに侵入し色々な個人情報を収集し、その情報をインターネット経由で第三者に送信するソフトウェアのことです。スパイウェアはほとんどのケースで、何か無料のソフトウェアと一緒に配布され、そのソフトウェアをインストールするとスパイウェアも一緒にコンピュータにインストールされるようになっています。

インストール時に「無料のソフトを提供する代わりに、情報収集を行います」という趣旨の使用許諾が表示されるのですが、ライセンスを説明した冗長な文章全てに目を通し、スパイウェアによる個人情報収集について理解した上でソフトウェアを使用するユーザーは多くありません。結果的に本人に理解されないまま個人情報が勝手に送信され、第三者に利用されてしまいます。



また、スパムメールのように一方的に送りつけて、確認もなく勝手にインストールをする悪質なスパイウェアもあります。

スパイウェアは他のソフトウェアと一緒にインストールされ、コンピュータ上の個人情報を流出させる

スパイウェアの目的

スパイウェアの目的は個人情報の収集にあります。インターネットが発達した昨今、スパイウェアが第一に収集するのは、個人がどのようなWebサイトを訪れるかという情報です。バナー広告を掲載する上で、人々がよく訪れるページを知るのは非常に重要な情報だからです。スパイウェアによって得られた情報をもとに、人気サイトにバナー広告が掲載されるわけですが、現在では、人々の色々な嗜好を調査し、個々のニーズに合った広告を掲載することが求められるようになっています。

スパイウェアが個々に収集する個人情報は、コンピュータによって効率的に処理されるため、いつも新鮮で非常に質の高い情報であると見なされています。実際、広告主はこの情報に従って柔軟にバナー広告を打っています。もちろんスパイウェアによって収集された個人情報が、広告以外の目的で利用される可能性も否定できません。

スパイウェアの収集する主な情報

アクセスしたWebサイトのURL
 ブラウザーによって蓄積されたCookie
 コンピュータの機種情報
 インストールされているソフトウェアの種類 等

スパイウェアとウイルスとの違い

スパイウェアがインストールされるときには、何らかの形でその旨が表示されます。つまりほとんどのスパイウェアはユーザーの了解を経て、合法的にインストールされる場合が多いのです。またスパイウェアは個人情報を通じた期間収集することが目的なので、コンピュータシステムにダメージを与えないように作られていることが多いのです。一方、ウイルスやワームはすべてが悪質なプログラムであり、ソフトウェアのセキュリティホールやオペレーションミスを利用して勝手にコンピュータに侵入し、情報を収集したりシステムにトラブルを引き起こしたりします。

ご注意

多くのスパイウェアは、有用なソフトウェアを無償で使用する代償としてインストールされるため、スパイウェアを除去すると、その有用なソフトウェアが使用できなくなるケースがあります。

また、本製品はスパイウェアやスパイウェアと思われるモジュールを慎重に判定し、その除去処理を行っています。誤判定によりスパイウェア以外を除去してしまうケースもあり得ます。このような場合は、除去した項目を本ソフトウェアの「リカバリー」機能で元に戻してください(24ページ参照)。



スパイウェアはコンピュータ上の個人情報を流出させるだけでなく、CPUやHDD等のシステムリソースを圧迫し、システムを不安定にさせることがあります

本製品の特長・動作環境

本製品の特長

スパイウェアを高度な処理により判定、安全に除去します

Spybot Search & Destroy（以下、Spybot S&D）はスパイウェアだけでなく、個人情報を内包したCookieや不必要なレジストリエントリ等を検出し、一覧表示します。そしてそれを除去することができます。もちろん操作によって、除去の可否を個々に設定することもできます。

除去したスパイウェアやレジストリ、ファイルなどを再度、リカバリーできます

万が一、必要なファイルをスパイウェアと誤認し、誤って除去してしまった場合なども、Spybot S&Dの「リカバリー」機能によりそれらを復活させ、システムをリカバリーさせることができます。

インターネットにより、最新の状態に更新できます

新たに出現するスパイウェアを検出するため、Spybot S&Dはインターネットを使って最新のモジュールに更新することができます。この「更新」により、Spybot S&Dはスパイウェアを駆逐し続けます。

本製品はご購入（登録）後1年間無償にて更新いただけます。

標準モードと詳細モードの2種類を用意しています

Spybot S&Dはコンピュータ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。簡単操作の標準モードのみでもスパイウェアを検出し、完全に除去することができます。

保護機能により、スパイウェアを侵入段階で食い止めることができます

Spybot S&Dの「保護」機能によりブラウザのセキュリティ設定を強化したり、スパイウェアの強制ダウンロードを拒否することができます。Spybot S&Dはスパイウェアを検出&除去するだけでなく、スパイウェアを侵入段階で阻止します。

コンピュータの操作履歴を消去することができます

他の人とコンピュータを共有していて、自分が行った作業を知られたくない場合など、Spybot S&Dを利用することにより、その使用履歴を消すことができます。そして、上級ユーザーには、レジストリの矛盾を修正したり、様々なレポートを作成することもできるようにしています。

動作環境**【OS】**

日本語 Microsoft Windows 98/98SE/Me/NT 4.0 Workstation(Service Pack6以降)/2000 Professional/XP Home Edition/XP Professional

【CPU/メモリ】

次のOSごとに必要なIntel Pentium及び互換プロセッサを搭載したDOS/V機またはNEC PC98-NXシリーズのコンピュータ(NEC PC-9801/9821シリーズは動作不可)

OS	CPU	メモリ
Windows 98/98SE	133MHz以上	64MB以上
Windows Me	150MHz以上	64MB以上
Windows NT 4.0	133MHz以上	64MB以上
Windows 2000	133MHz以上	64MB以上
Windows XP	300MHz以上	128MB以上

【HDD】

15MB以上の空き容量

【グラフィックカード】

VGA以上

【その他必要条件】

インターネット接続環境必須

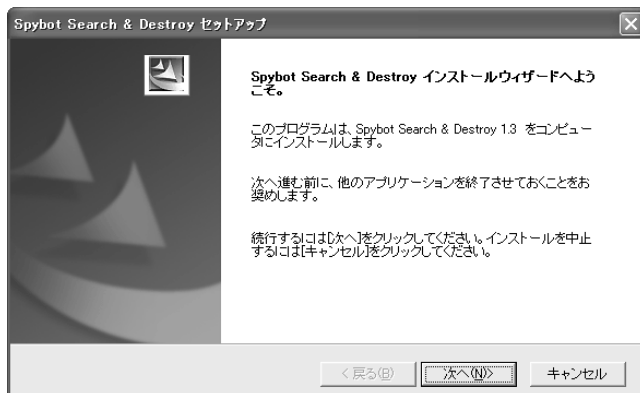
Internet Explorer 5.5 (Service Pack2以降) 以上

- Windows NT/2000/XP上でご利用になる場合は、アドミニストレータ(管理者)権限にてインストールしてください。
- Windows NT/2000/XP上で完全に動作させるには、管理者権限を持つアカウントが必要です。
- Windows 98/98SE/NT4.0では、一部動作しない機能があります。詳しくは弊社ホームページをご覧ください。

インストール方法

Spybot S&D は、次の方法でインストールします。

1

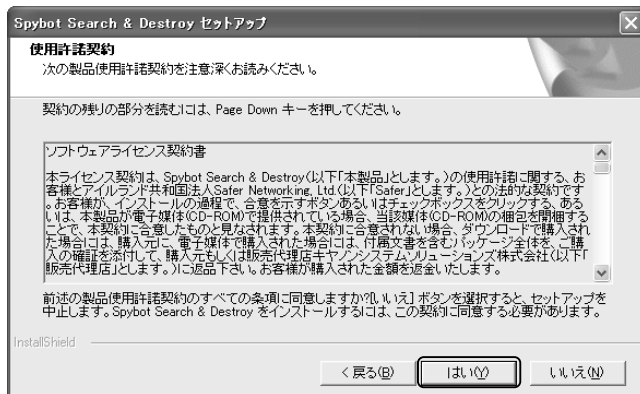


Spybot S&DのインストールCDをCD-ROMドライブに挿入してください。インストールウィザードが起動します。「次へ」ボタンをクリックします。

POINT

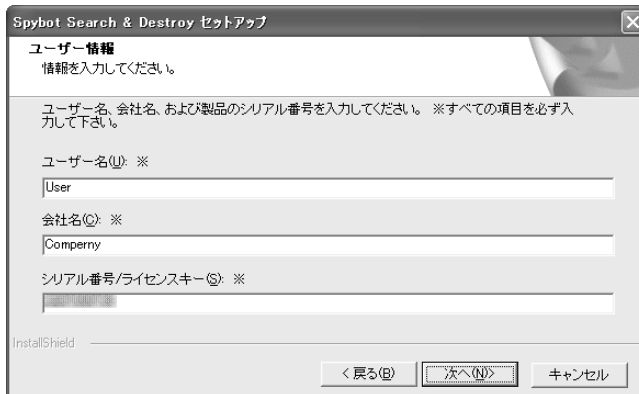
起動しない場合はWindowsの「マイ コンピュータ」より挿入したドライブを開き、「setup.exe」のアイコンをダブルクリックします。

2



「使用許諾契約」画面が表示されます。よくお読みいただき、同意される場合は「はい」ボタンをクリックします。

3



「ユーザー情報」画面が表示されます。「ユーザー名」「会社名」「シリアル番号/ライセンスキー」をそれぞれ入力します。シリアル番号は、パッケージに同梱のオンラインユーザー登録のご案内用紙に明記されていますので、そちらをご参照ください。入力が終了したら「次へ」ボタンをクリックします。

4



「インストール先の選択」画面が表示されます。既定値でのインストール先のフォルダでよろしければ、そのまま「次へ」ボタンをクリックします。インストール先のフォルダを変更したい場合は「参照」ボタンをクリックし、好みのフォルダを指定します。特別な理由がない場合は、既定値にインストールすることを推奨します。

5



インストール先の選択が終了すると、「オプションの選択」画面が表示されます。チェックボックスを「オン」「オフ」し、設定するオプションを選択します。それぞれの項目の内容は次の通りです。

アイコンの作成

デスクトップアイコンを作成	デスクトップにショートカットアイコンを作成します。
クイック起動アイコンを作成	クイック起動バーにアイコンを作成します。
ユーザー補助モード用デスクトップアイコンを作成	ユーザー補助モード用デスクトップアイコンを作成します。

常駐保護

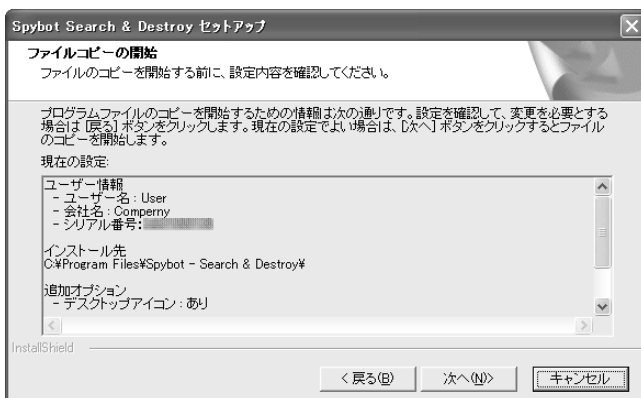
Internet Explorerの保護を有効(SDHelper)	Internet Explorerの保護(SDHelper)を有効にします。
システム設定の保護を有効(TeaTimer)	システム設定の保護(TeaTimer)を有効にします。

POINT

ユーザー補助モードとは、メニューバーに「ナビゲーション」や「アクション」などを設けて、通常の操作よりも使いやすくしたものです。コンピュータを利用するうえで、特に操作の難しさを感じていらっしゃる方はチェックを「オン」にする必要はありません。

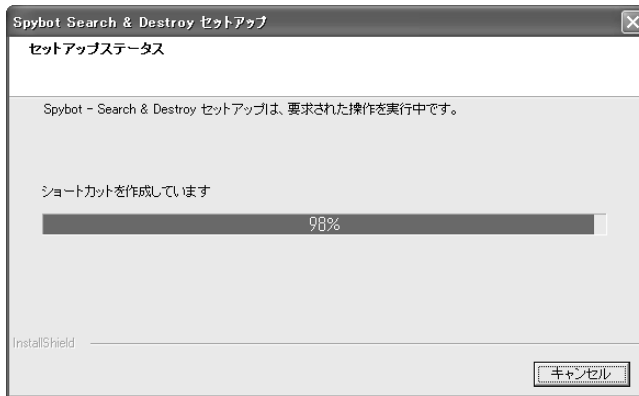
常駐保護の設定項目である「Internet Explorerの保護を有効」については26ページを、「システム設定の保護を有効」については28ページをご参照ください。基本的には、とくにチェックボックスを「オン」「オフ」する必要はありません。既定値のままでお進みください。

6



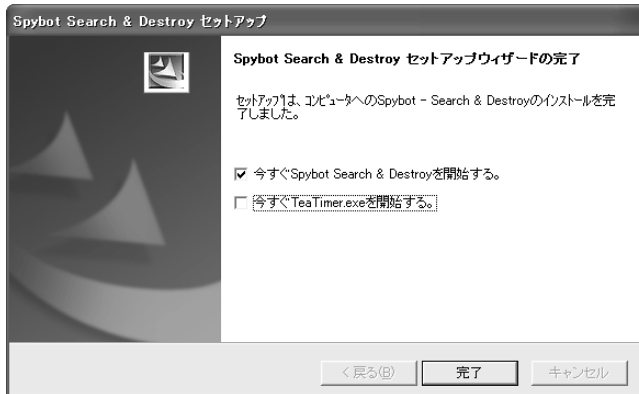
「ファイルコピーの開始」画面が表示されます。表示されている内容で問題なければ、「次へ」をクリックします。ファイルのコピーが開始されます。

7



進捗状況が画面表示されます。

8



「セットアップウィザードの完了」画面が表示されます。「完了」ボタンをクリックするとSpybot S&Dのインストールは完了します。チェックボックスにチェックを入れた状態で「完了」ボタンをクリックすると、その項目に応じた動作を行い、Spybot S&Dが起動します。TeaTimerに関しては、28ページをご参照ください。

起動方法と基本画面について

Spybot S&Dの起動方法

1



Spybot S&Dの起動は「スタート」メニューから「すべてのプログラム」「Spybot - Search & Destroy」と選択し、「Spybot - Search & Destroy (default)」を選択します。

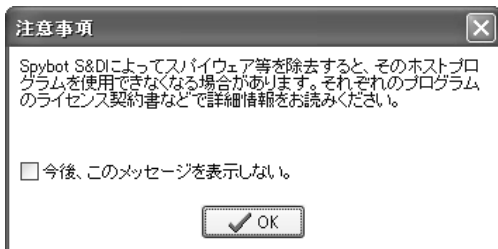
POINT

インストール時のウィザード画面で、「デスクトップアイコンを作成」のチェックを「オン」にして進めた場合は、デスクトップ上にSpybot S&Dのショートカットアイコンが表示されます。こちらをダブルクリックしても、同様に標準モードで起動することができます。



Spybot - Search & Destroy (advanced)	Spybot S&Dを詳細モードで起動します。詳細モードでの操作はコンピュータとスパイウェアについて、より詳しい知識が必要です。通常は標準モードを使用してください。詳細モードについては、ヘルプを参照してください。
Spybot - Search & Destroy (default)	Spybot S&Dを標準モードで起動します。この標準モードによる操作で、十分にスパイウェアの駆逐を行うことができますので、通常はこちらから、Spybot S&Dを起動してください。
Spybot - Search & Destroy アンインストール	Spybot S&Dのアンインストールを行います。詳細は30ページをご参照ください。
Spybot - Search & Destroy シリアル番号	Spybot S&Dのシリアル番号(ライセンスキー)を確認するためのウィンドウが表示されます。また「ユーザー登録」ボタンが表示されますので、ユーザー登録がまだお済みでない方は、ユーザー登録を行ってください。

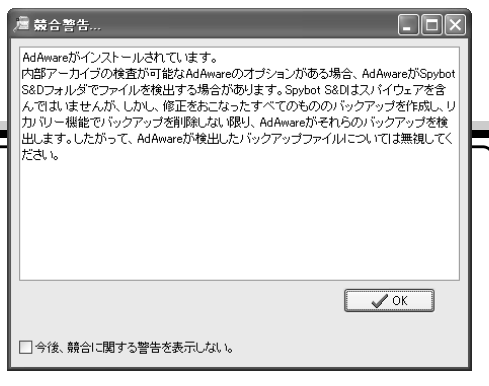
2



Spybot S&Dの起動前に、次の画面が表示されます。一部のスパイウェアは有用なソフトウェアを無料で使用する代償として、インストールされることがあります。この画面では、Spybot S&Dによりスパイウェアを除去した場合、スパイウェアの動作が前提のソフトウェアが正常に動作しなくなる可能性について説明しています。「今後、このメッセージを表示しない」をチェックを「オン」にすると、この画面は表示されなくなります。

POINT

Spybot S&Dと同種のソフトウェアがインストールされている場合、起動時に「競合警告」画面が表示されることがあります。よくお読みいただき、「OK」ボタンをクリックしてください。



3



Spybot S&Dが起動します。

基本画面の構成

Spybot S&D を起動し、最初に表示される基本画面の構成は次の通りです。



① 検査の開始	直ちにスパイウェアの検査が行われ、その結果を表示します。この処理は④の「検査と除去」ボタンをクリックして表示される画面で、「検査の開始」ボタンをクリックすることと同じ意味を持ちます。「ファイル」メニューから「検査の開始」を選択しても、「検査の開始」ボタンをクリックした場合と同様の処理が行われます。「検査の開始」については、18ページも併せてご参照ください。
② リカバリー	除去したスパイウェア等を復元させ、除去前の状態に戻すことのできる設定画面に移行します。スパイウェアの除去でシステムに不都合が起きたときは、この「リカバリー」画面からシステムを復元させることができます。「リカバリー」画面は⑤の「リカバリー」ボタンをクリックしても表示させることができます。「リカバリー」については、24ページをご参照ください。
③ 更新検索	Spybot S&Dの最新モジュールを検索します。この処理は⑦の「更新」ボタンをクリックして表示される画面で、「更新検索」ボタンをクリックすることと同じ意味を持ちます。
④ 検査と除去	「検査と除去」画面に移行します。この「検査と除去」画面では、スパイウェアやブラウザーが蓄積したCookie、不要なレジストリエントリを検査し、その除去を行うことができます。「検査と除去」については、18ページをご参照ください。
⑤ リカバリー	②と同じです。「リカバリー」については、24ページをご参照ください。
⑥ 保護	「保護」画面に移行します。この「保護」画面ではブラウザーに関するセキュリティを高め、スパイウェアの侵入を未然に食い止める保護機能の設定を行うことができます。「保護」については、26ページをご参照ください。
⑦ 更新	「更新」画面に移行します。この「更新」画面では、Spybot S&Dを最新バージョンに更新することができます。「更新」については、16ページをご参照ください。

⑧ ファイルメニュー



検査の開始	スパイウェアの検査が直ちに行われ、その結果を表示します。①の「検査と除去」ボタンをクリックして表示される画面で、「検査の開始」ボタンをクリックすることと同じ意味を持ちます。
終了	Spybot S&Dを終了します。

⑨ モードメニュー



Spybot S&Dの動作モードを設定します。

標準モード	Spybot S&Dを簡単操作の標準モードにします。通常はこの標準モードによる操作で、十分にスパイウェアの駆逐を行うことができます。
詳細モード	Spybot S&Dをより複雑な操作を可能にする詳細モードにします。詳細モードでの操作は、コンピュータとスパイウェアについて、より詳しい知識が必要です。詳細モードへ移行する場合は、その旨の警告画面が表示されますので、「はい」をクリックしてください。なお、詳細モードの詳細はヘルプをご参照ください。

⑩ ヘルプメニュー



Spybot S&Dのヘルプやバージョンを表示します。

ヘルプ	Spybot S&Dのヘルプを表示します。
チュートリアル	ヘルプファイルのチュートリアルページを表示します。
キーワード	ヘルプファイルをキーワード検索状態に表示します。
バージョン情報	Spybot S&Dのバージョン情報を表示します。
ホームページ	Spybot S&Dのサポートページをブラウザで表示します。

「検査と除去」実行前に 「更新」を行う

Spybot S&D 自身のプログラムモジュールや、スパイウェアの情報を最新の状態へと更新します。スパイウェアは常に変化し、新種が発生することもあります。そのためにSpybot S&Dも、最新の状態を保つ必要があるのです。確実なスパイウェア検出とその除去を行うため、定期的にこの「更新」を行っていただくのはもちろんのこと、検査や除去を行う前には必ずこの「更新」を実行してください。

1



「更新」ボタンをクリックします。

2

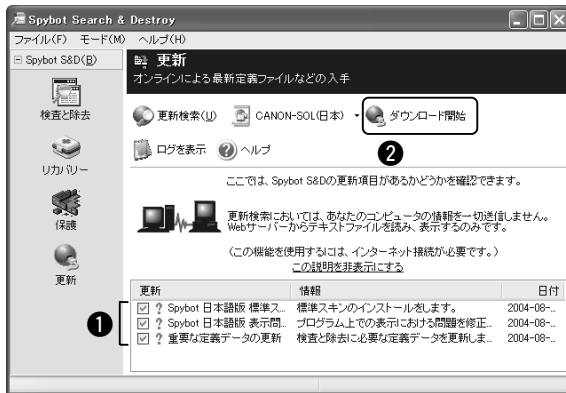


「更新検索」ボタンをクリックします。更新すべき項目の検索が始まります。

POINT

手順 1 で「更新検索」ボタンをクリックしても検索を始めることができます。

3



新しい更新項目が存在した場合、更新項目が下部ウインドウ(「更新項目一覧」ウインドウ)に表示されます。①更新したい項目のチェックボックスを「オン」にします。Spybot S&Dを常に最新の状態に保つために、全てのモジュールを更新することをお勧めします。②「ダウンロード開始」ボタンをクリックします。以上で更新は終了します。

POINT

その他の機能は次の通りです。



<p>① サーバー選択</p>	<p>更新検索の結果、更新項目がある場合に、ダウンロードサーバーを選択することができます。</p> <p>注意！ ダウンロードサーバーが複数存在しない場合、サーバーを選択することはできません。</p>
<p>② ログを表示</p>	<p>更新に関するログをメモ帳で表示します。</p>
<p>③ ヘルプ</p>	<p>Spybot S&Dのヘルプファイルで、「更新」に関するページを表示します。</p>
<p>④ この説明を非表示にする / 説明を表示する</p>	<p>このリンクをクリックすると、更新機能に関する説明を表示、または非表示にします。</p>

ご注意：本製品はご購入（ご登録）後1年間無償にて更新いただけます。1年間ご利用後の更新手続きについては弊社ホームページにてご案内致します。

「検査と除去」機能で スパイウェアを除去する

スパイウェアの検査から除去までの手順

1



スパイウェアの情報を最新の状態に更新したら、いよいよ「検査及びその除去」を行います。ちょうど更新が終了した状態が左画面となります(ここでは特に更新すべき情報がなかった画面を表示しています)。「検査と除去」ボタンをクリックします。

2



「検査の開始」ボタンをクリックします。

POINT

起動画面の「検査の開始」ボタンをクリックすることでスパイウェア等の問題点の検査が開始されます。

3



コンピュータ上のスパイウェアが検査されます。検査中はその進捗が、ウィンドウ下部のステータスバーに表示されます。


4



検査結果の画面が表示されます。スパイウェアが発見された場合、その一覧が表示されます。除去しない項目があれば、そのチェックをオフにしてください。ただし赤い色で表示されている項目については、特別の理由がない限り除去したほうがよいでしょう。「選択項目を除去」をクリックし、スパイウェアの除去を実行します。

5

システムの復元ポイントを作成中...

 選択された問題点を修正する前に、Spybot S&Dがシステムの復元ポイントを作成しています。

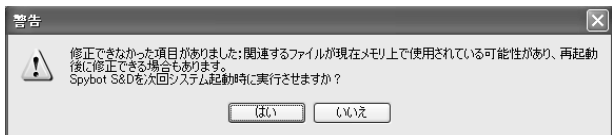
システムの復元ポイントは、特定の変更を行う前のポイントへシステムを復元することができ、Windows MEおよびXPの特有の機能です。もし、システムの復元ポイントが必要なければ、「モード」メニューから「詳細モード」に切り替え、「設定」画面から、この作成を無効にしてください。

このウィンドウは、システムの復元ポイント作成が終了したら、自動的に閉じます。

OSがWindows XPの場合、ここで除去項目に対する復元ポイントを作成します。元々Windows XPは、システムを復元する機能を持っていますが、Spybot S&Dではこの機能を利用してスパイウェア等を除去する前の状態に戻せるようにしています。処理が終了し、この画面が消えるまで、しばらくお待ちください。

CAUTION!

すでに他のプロセスで使用されているファイルなどは、除去できないことがあります。その場合には、次回のシステム起動時に除去を行うように設定することができます。「はい」をクリックすると、次回のシステム起動時に Spybot S&D が自動起動され、除去が行われます。



6



検出された問題点の除去を行うため再度確認が行われます。除去を行う場合は「はい」ボタンをクリックしてください。除去が実行されます。

7



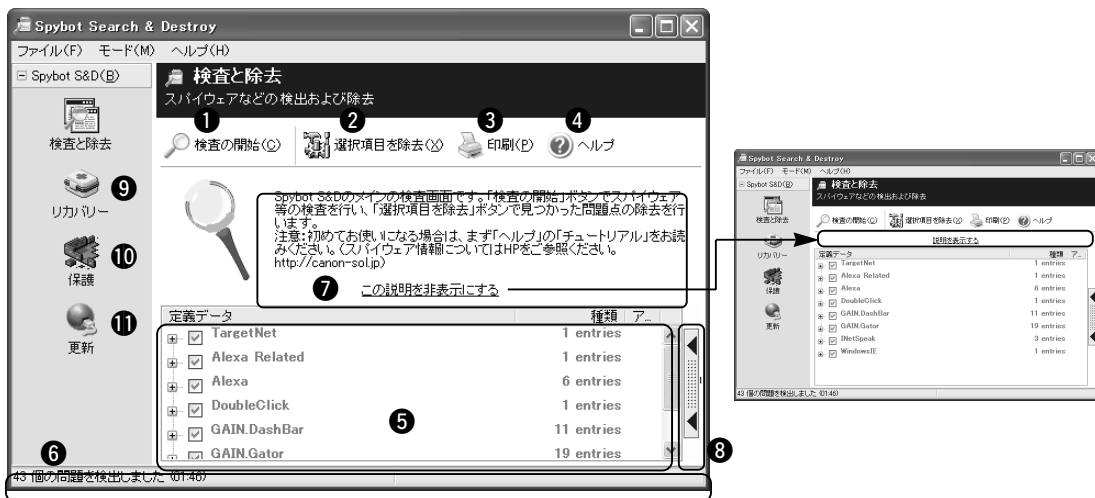
検出された問題点の除去が行われました。

CAUTION!

システムの稼働中に除去できなかった問題点がある場合は、次回のシステム起動時に Spybot S & D が起動し、検査を行います。



「検査と除去」画面構成



① 検査の開始 / 中止	スパイウェア等の検査を開始 / 中止します。「検査の開始」をクリックすると、スパイウェアの検査を行います。スパイウェアを検査した結果は、下部の「結果一覧」ウインドウ部分⑤に表示されます。また検査中には「中止」と表示され、「中止」をクリックすると検査を中断します。
② 選択項目を除去	スパイウェアの検査を行った後、表示されます。「選択項目を除去」をクリックすると、検出されたスパイウェアやCookie、不要なレジストリエントリが除去されます。なお、除去の可否は、検査された個々の項目に対し任意に設定することができます。詳細は「検査結果の見方とスパイウェア等の除去」をご参照ください。
③ 印刷	Spybot S&Dの内部ファイルリストやスパイウェアの検査結果を印字します。
④ ヘルプ	Spybot S&Dのヘルプファイルで「検査の開始」に関するページを表示します。
⑤ 結果一覧	この部分に検査結果を一覧表示します。セキュリティやプライバシー情報の漏洩など、対策を必要とする問題部分は赤い表示になります。緑の文字で表示される項目は、履歴ファイルです。この履歴ファイルにより、ブラウジングに関する情報などが漏洩する可能性があります。詳しくは22ページをご参照ください。 <div style="border: 1px solid black; padding: 5px; margin: 5px 0;">使用履歴は、Webブラウザの履歴だけでなくMicrosoft OfficeやWindows Media Player、RealPlayerなど様々なアプリケーションの履歴も検出できます。ただし、Spybot S&Dに登録されているものに限ります。</div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;">注意！：ブラウザの履歴ファイルを消去してもシステム自体には悪影響はありませんが、ブラウザから履歴を参照することができなくなります。</div>
⑥ ステータスバー	この部分には検査中のプロセスや検査結果、検査時間などが表示されます。
⑦ この説明を非表示にする / 説明を表示する	このリンクをクリックすると、検査機能に関する説明を表示、または非表示にします。
⑧ 補助ウインドウ	検査結果を補足する補助ウインドウを表示・非表示にします。
⑨ リカバリー	Spybot S&Dを使用して除去したファイルなどを復活させることのできる「リカバリー」画面に移行します。「リカバリー」については、24ページをご参照ください。
⑩ 保護	コンピュータのセキュリティを高め、スパイウェアの進入を未然に防ぐことのできる「保護」画面に移行します。「保護」については、26ページをご参照ください。
⑪ 更新	Spybot S&Dを最新の状態へと更新する「更新」画面に移行します。「更新」については、16ページをご参照ください。

検査結果の見方とスパイウェア等の除去について

スパイウェアの検査を行うと、その結果が一覧表示されます。除去する項目をチェックし、「選択項目を除去」をクリックしてください。その項目が除去されます。



- 1 [+] : 検出された問題点は、ツリー構造で表示されます。この表示の場合は、[+]をクリックするとさらに詳しい項目が表示されます。
- 2 チェックされている項目が、除去の対象になります。除去しない場合には、チェックをオフにしてください。
- 3 スライダーで、表示をスクロールさせることができます。
- 4 この部分をマウスで移動させると、それぞれの項目の表示幅を変えることができます。
- 5 この部分をクリックすると、詳しい解説を表示する補助ウインドウを表示させることができます。検索された一覧から詳しい内容を知りたい項目をマウスで選択してください。補助ウインドウには、その項目に対応する情報が表示されます。補助ウインドウに表示された情報内に URL がある場合、補助ウインドウを右クリックすることで、表示された URL をメニュー表示します。表示された URL をマウスで選ぶとブラウザが起動し、その Web サイトを表示します。

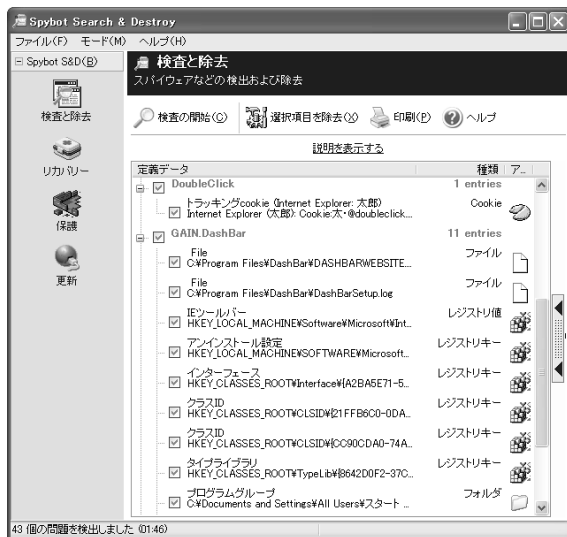


検査された項目を選択し、マウスを右クリックするとメニューが表示されます。メニューからそれぞれの機能を選択することができます。



POINT

検査により検出される問題点について解説します。



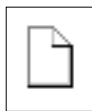
検査された問題点がレジストリエントリの場合、このアイコンが表示されます。スパイウェアによって多くのレジストリエントリを書き換えてしまうことがあります。このアイコンをクリックすると、レジストリエディタが起動し、該当レジストリが表示されます。



検査された問題点がCookieファイルの場合、このアイコンが表示されます。ブラウザの蓄えたCookieを解析することにより、ブラウザによるアクセス履歴やアクセス内容などが漏洩する事があります。



検査された問題点がスパイウェア等を含んだフォルダの場合（赤色の文字）、このアイコンが表示されます。このアイコンをクリックすると、そのフォルダをエクスプローラーで表示することができます。



検査された問題点がスパイウェア等を含んだファイルの場合（赤色の文字）、このアイコンが表示されます。このアイコンをクリックすると、そのファイルを含むフォルダをエクスプローラーで表示することができます。使用履歴の場合も表示されますが、その場合は緑色の文字です。

キャッシュ、Cookie、ログなど一部の種類は復元することはできません。

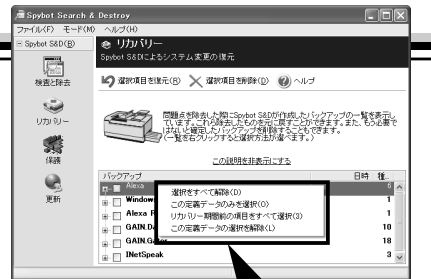
「リカバリー」機能で 除去ファイルを復元する

Spybot S&Dにより、すでに除去したスパイウェア等を復元させます。スパイウェアの除去などでコンピュータシステムに不都合が生じた場合、このリカバリーで除去したファイル等を復元し、システムの問題を解決することができます。



POINT

「バックアップ一覧」で表示された項目をマウスで右クリックするとメニューが表示され、表示された機能を選択することができます。



選択をすべて解除(D)
この定義データのみを選択(O)
リカバリー期間前の項目をすべて選択(S)
この定義データの選択を解除(L)

CAUTION!

スパイウェア等の除去を行っていない場合は、「バックアップ一覧」には何も表示されません。

POINT

上記POINTで表示される右クリックメニューから「リカバリー期間前の項目をすべて選択」を選択すると、除去してから一定の期間(リカバリー期間)を過ぎた項目のみ、チェックが「オン」になります。リカバリー期間の設定は、標準で30日です。

設定の変更は、詳細モードで表示される「環境設定」で行えます。操作方法は、ヘルプファイルをご参照ください。

選択をすべて解除(D)
この定義データのみを選択(O)
リカバリー期間前の項目をすべて選択(S)
この定義データの選択を解除(L)

3 「選択項目を復元」ボタンをクリックします。その内容が復元されます。

CAUTION!

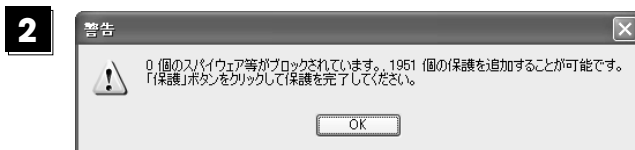
「選択項目を除去」ボタンをクリックすると、「バックアップ一覧」においてチェックした項目を完全に除去します。この除去によりバックアップされたデータは完全に消滅しますので、操作には十分注意してください。

「保護」機能でスパイウェアを 防御する

スパイウェアがコンピュータに進入しないよう、「保護」機能を使うことでInternet Explorerなどのブラウザのセキュリティを高め、スパイウェアの進入を未然に防止することができます。



画面左の「保護」ボタンをクリックします。



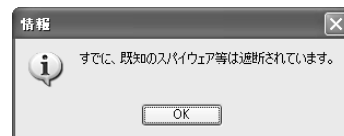
現在の保護状態がウィンドウ表示されます。「OK」ボタンをクリックします。



画面中央付近の「保護」ボタンをクリックします。

POINT

既知のスパイウェアに関する情報が表示される場合もあります。「OK」ボタンをクリックします。



4

Internet Explorer において悪意あるダウンロードをブロックするか否かを設定します。「悪意あるアドレスに対するInternet Explorerの常駐ブロックを有効」のチェックを「オン」にした場合は、異常を検出したときの対処をリストボックスから選択してください。

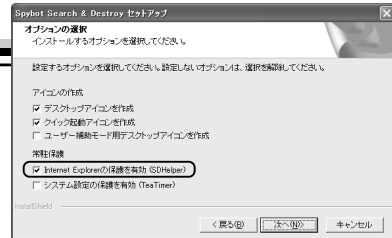
またブラウザの1つである「Opera」がインストールされていたら、「Opera」に対する悪意のあるプラグインのブロックを設定できます。

自動的にブロックする	ダウンロードを自動的にブロックします。
ブロック後にダイアログを表示	ダウンロードをブロックしたとき、その旨を表示します。
ブロック前に確認ダイアログを表示	ダウンロードをブロックする前にその旨を表示し、ユーザーにダウンロード可否の選択を促します。

POINT

「常駐ダウンロードブロック」は通常の常駐保護に加え、Spybot S&Dデータベースに登録された悪意あるサイトから、ファイルのダウンロードを防止する機能です。またこの設定はSpybot S&Dインストール時に、有効/無効を設定することもできます。

インストール時に表示される画面



「Internet Explorerの常駐ダウンロードブロック」の設定は以上で終了です。

POINT

その他のボタンの設定は次の通りです。

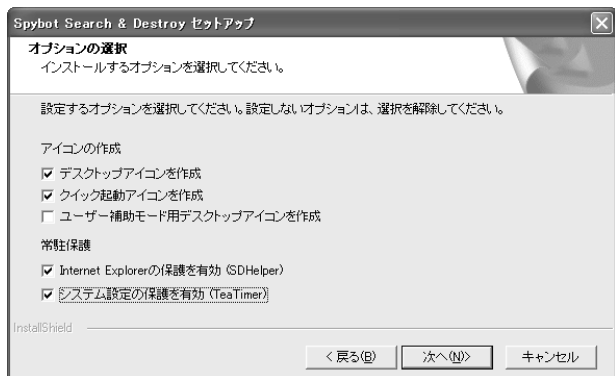
- A 保護機能を使う場合クリックします。
- B 再チェックを行いたい場合は「再チェック」ボタンをクリックします。
- C ブラウザーの常駐保護を解除したい場合は「解除」ボタンをクリックします。
- D このリンクをクリックすると、保護機能に関する説明を表示、または非表示にします。
- E 「SpywareBlaster」のサポートサイトを表示します。「SpywareBlaster」とは、Internet ExplorerにおけるActiveX関連のセキュリティを高めるソフトウェアです。Spybot S&Dと「SpywareBlaster」を併用することで、Internet Explorerのセキュリティをさらに高めることができます。



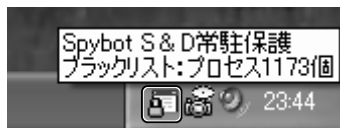
注意! 「SpywareBlaster」はSpybot S&Dと直接の関係はありませんで、サポート対象外になります。

「TeaTimer」機能でシステム設定を防御する

Spybot S&Dにおけるモジュールの1つである「TeaTimer」は、Windowsに常駐するプログラムです。多くのスパイウェアはレジストリなどを書き換えますが、「TeaTimer」を常駐させておくと、レジストリエントリなどの書き換えを検出し、それを防ぐことができます。



「TeaTimer」を常駐モードで使用するには、Spybot S&Dのインストール時に「システム設定の保護を有効」のチェックボックスを「オン」にしてください。



「TeaTimer」が常駐すると、通知領域にウインドウ枠に鍵をあしらったアイコンが表示されます。



「TeaTimer」のアイコンをマウスで右クリックすると、メニューが表示されます。メニューの内容は次の通りです。

<p>① Spybot S&Dの実行</p>	<p>Spybot S&Dを起動します。</p>						
<p>② IEの常駐保護</p>	<p>Internet Explorerの常駐保護について設定を行います。「IEのダウンロードブロック (SDHelper) を使用」をチェックした場合は、その動作について設定を行います。</p> <table border="1" data-bbox="525 519 1253 696"> <tr> <td data-bbox="525 519 882 548"> <p>Ⓐ 自動的にブロック</p> </td> <td data-bbox="882 519 1253 548"> <p>ダウンロードを自動的にブロックします。</p> </td> </tr> <tr> <td data-bbox="525 548 882 608"> <p>Ⓑ ブロック時にダイアログを表示</p> </td> <td data-bbox="882 548 1253 608"> <p>ダウンロードをブロックしたとき、その旨を表示します。</p> </td> </tr> <tr> <td data-bbox="525 608 882 696"> <p>Ⓒ ブロック前に確認ダイアログを表示</p> </td> <td data-bbox="882 608 1253 696"> <p>ダウンロードをブロックする前にその旨を表示し、ユーザーにダウンロード可否の選択を促します。</p> </td> </tr> </table> <p>POINT</p> <p>「IEのダウンロードブロック (SDHelper) を使用」とは、保護機能における「Internet Explorerの常駐ダウンロードブロック」を示します。保護機能については、26ページをご参照ください。</p>	<p>Ⓐ 自動的にブロック</p>	<p>ダウンロードを自動的にブロックします。</p>	<p>Ⓑ ブロック時にダイアログを表示</p>	<p>ダウンロードをブロックしたとき、その旨を表示します。</p>	<p>Ⓒ ブロック前に確認ダイアログを表示</p>	<p>ダウンロードをブロックする前にその旨を表示し、ユーザーにダウンロード可否の選択を促します。</p>
<p>Ⓐ 自動的にブロック</p>	<p>ダウンロードを自動的にブロックします。</p>						
<p>Ⓑ ブロック時にダイアログを表示</p>	<p>ダウンロードをブロックしたとき、その旨を表示します。</p>						
<p>Ⓒ ブロック前に確認ダイアログを表示</p>	<p>ダウンロードをブロックする前にその旨を表示し、ユーザーにダウンロード可否の選択を促します。</p>						
<p>③ Spybot S&Dの常駐保護を終了</p>	<p>「TeaTimer」の常駐を終了します。</p>						

アンインストール方法



「スタート」メニューから「Spybot - Search & Destroy」を選択し、「Spybot - Search & Destroy アンインストール」をクリックします。

POINT

コントロールパネルから開く「プログラムの追加と削除(アプリケーションの追加と削除)」画面からもアンインストールを行うことができます。



メンテナンスウィザードが表示されます。「削除」を選択し、「次へ」をクリックします。以降は、「ファイル削除の確認」画面、「セットアップステータス」画面が表示されます。画面の指示に従ってください。最後に「メンテナンスの完了」画面が表示されますので、「完了」をクリックすることでアンインストールが完了します。

FAQ

ここではよくある質問についてお答えしています。サポートへご連絡される前にぜひご一読されることをお勧めします。



1 Spybot S&Dは他のスパイウェア対策ソフトと併用できますか？

基本的にできます。

ただし、Spybot S&Dがスパイウェアを検出および削除した際にリカバリー用のファイルを作成し、そのファイルを他社のスパイウェア対策ソフトがスパイウェアとして誤検出してしまうことがあります。リカバリー用のファイルはスパイウェアとして活動しないので、この場合は無視してください。



2 ネットワークドライブも検査しますか？

いいえ、検査しません。他のコンピュータを検査したりファイル除去を行うことは、大変危険です。ファイルだけでなく、レジストリ項目によるリンクを除去することにより、多くのエラーを引き起こしかねません。

LSPハイジャッカー(Windowsのシステムドライブを書き換える)のファイル除去 = LSP除去は、削除されたマシンのネットワークアクセスを無効にします。また、レジストリの修復によりLSPを修復することも障害の危険性があります。Spybot S&Dは各々のマシンで作動する必要があります。



3 レジストリの変更時にダイアログが表示されるのですが、どうすればいいですか？

TeaTimer機能を有効にしている場合に、レジストリ変更を監視しているため、変更が生じた場合にそれに同意するかどうか確認するためにダイアログが表示されます。

また、アプリケーションのアップデート時、およびインストール/アンインストール時(Office Update、Windows Updateなど)には多くのレジストリを変更するので、あらかじめTeaTimerをオフにしておくことをお勧めします。

4

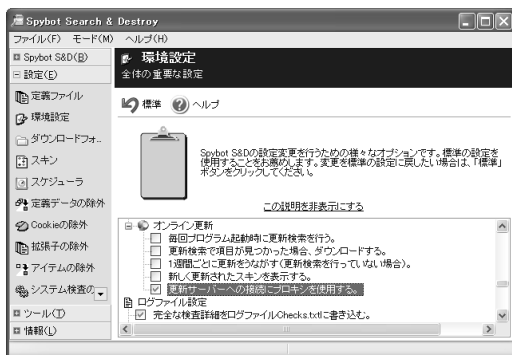
更新に失敗するのはなぜですか？

更新はインターネット経由で行われます。したがって、インターネット接続が正常に使用できる環境でなければなりません。

また、インターネット接続にプロキシを使用している場合はSpybot S&Dに設定を施しておく必要があります。



設定方法は次の通りです。まず、詳細モードで起動し、「設定」ボタンをクリックします。表示される「設定」画面の「環境設定」ボタンをクリックします。様々な設定変更を行うためのオプション画面が表示されます。その中の「自動化」項目内の「オンライン更新」にある「更新サーバーへの接続にプロキシを使用する」のチェックを「オン」にします。プロキシ設定のダイアログが表示されますので、ホスト、ポート、ユーザー名、パスワードを設定し、「OK」をクリックします。以上で設定は終了です。



5

Spybot S&Dを再インストールしても以前のデータが残っているのはなぜですか？

Spybot S&Dの設定情報や検査・除去・更新の履歴、リカバリー用ファイルなどは、Spybot S&Dをアンインストールしても残るように設定されています。

OSごとにデータの場所は異なります。

Windows XP/2000の場合

Documents and Settings¥All Users¥Application Data¥Spybot - Search & Destroy フォルダ

Windows NTの場合

Winnt¥Profiles¥[ユーザー名]¥Application Data¥Spybot - Search & Destroy フォルダ

Windows Meの場合

WINDOWS¥All Users¥Application Data¥Spybot - Search & Destroy フォルダ

Windows 98/98SEの場合

WINDOWS¥Application Data¥Spybot - Search & Destroy フォルダ



6 シリアル番号を紛失した場合は？

ユーザー登録済みの場合

以下の内容をご記入の上、下記へお送りください。

内容

件名：シリアル番号確認依頼

製品名：Spybot S&D

ご登録の郵便番号 / 住所 / 氏名 / 電話番号 / E-Mail アドレス

ご登録日とご登録方法（ご記憶の範囲でお願いいたします）

お送り先

電子メール：spybot-info@canon-sol.co.jp

ファックス：03-5730-7122

未登録の場合

Spybot S&D CD-ROM 表面とユーザーズガイドの表紙を複写機でコピーし、余白に以下の内容をご記入の上、ファックスにて03-5730-7122までお送りください。

弊社にてユーザー登録後、シリアル番号を再発行いたします。

件名：シリアル番号確認依頼

製品名：Spybot S&D

ご登録の郵便番号 / 住所 / 氏名 / 電話番号 / E-Mail アドレス

ご登録日とご登録方法（ご記憶の範囲でお願いいたします）

サポートについて

お問い合わせ

本製品についてお問い合わせいただく前に、下記Webサイトのサポート情報を参照してください。

<http://canon-sol.jp/supp/sb>

本ユーザーズガイド、ヘルプ、ホームページ等をご覧いただいても問題が解決しなかった場合は、キヤノンシステムソリューションズサポートセンターまでご相談ください。ご相談は、電話やFAX、電子メールにて受け付けております。

なお、下記につきましてはサポートをいたしかねる場合がございますので予めご了承ください。

- ・ユーザー登録をお済ませでない方
- ・動作保証外、サポート対象外の環境でご使用のお問い合わせ
- ・お客様の故意や改造等による紛失、不具合の発生、破壊等によるサポート
- ・訪問、出張が伴うサポート
- ・弊社休業日、受付時間外でのサポート
- ・FAXまたは電子メールでお問い合わせいただいた際、必要な内容が書かれていない場合
- ・法的な不正やライセンス契約内容に違反する事実が判明した場合

ホームページURL <http://canon-sol.jp/>

お問い合わせに関しましては、巻末にあるお問い合わせシートの内容をお知らせください。尚、製品専用のお問い合わせシートがある場合はそちらをご使用ください。

電話でのお問い合わせ先：キヤノンシステムソリューションズ サポートセンター

TEL：03 - 5730-7197 受付時間：月曜日～金曜日（祝祭日、夏季・年末年始等の休業日を除く）
10：00～12：00、13：00～16：30

日時によっては混み合っている場合がございます。その際は、誠に恐れ入りますが時間を改めてお掛け直しいただけますようお願いいたします。

FAXでのお問い合わせ先：キヤノンシステムソリューションズ サポートセンター

FAX：03 - 5730-7122

電子メールでのお問い合わせ先：キヤノンシステムソリューションズ サポートセンター
Spybot S&D係 電子メールアドレス：spybot-info@canon-sol.co.jp

お問い合わせにはできるだけ迅速に対応いたしますが、お問い合わせの内容によっては、弊社または開発元での動作検証が必要になる場合がございます。このような場合には、返信にかなりのお時間をいただく場合がございます。予めご了承くださいませようお願い申し上げます。

ユーザー登録のお願い

サポートや今後の最新情報をお受けいただくには、ユーザー登録が必要です。

同梱の「オンラインユーザー登録のご案内」をご参照の上、お早めに弊社ホームページからオンラインにてご登録ください。

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

お問い合わせシート [ご購入後]

この「お問い合わせシート」は、Spybot S&DのCD-ROMのルートフォルダに、お問い合わせ.txt というファイル名で格納されておりますので、電子メールやFAXでお問い合わせの際にご利用ください。

FAX番号：03-5730-7122

電子メール：spybot-info@canon-sol.co.jp

(宛先) Spybot S&D サポートセンター行

(日付) 20 年 月 日

製品情報

製品名	Spybot S&D	バージョン(例：1.3 CSOL)
シリアル番号		

お客様情報

ユーザーID	
氏名	
連絡先	
会社・部署名/学校・学科名	

【ご質問】(操作方法などのご質問の場合に記入してください)

質問内容 (どのような目的でどのような結果を得られたいのか詳しく記入してください)	
--	--

【トラブル】(トラブルの場合に記入してください)

トラブル内容 (トラブルに至る操作手順、現象、表示されるメッセージやモジュール名などの詳細を記入してください)	
--	--

再現性 (必ず再現する、ときどき再現する、再現しないなど、具体的にご記入ください)	
その他 (トラブル発生後に操作したこと、他の製品やハードウェアに関して過去にあったトラブル、お気づきの点などを記入してください)	

【ご使用環境】(お問い合わせ内容に応じておわかりになる範囲で記入してください)

パソコン	メーカー名	型番
CPU	メーカー名	型番
	周波数	MHz
実装物理メモリ	MB	
OS	Windows NT4.0(SP6以降) Windows XP Home Edition Windows XP Professional Windows 2000 Windows Me Windows 98 Windows 98SE	
OSインストール方法	新規インストール ()からアップグレード その他()	
ドライブ構成		
インストールしている 主なソフト		
常駐しているソフト		
ウイルス対策ソフト		
パーソナル ファイアウォール		
インターネット接続方法		
Webブラウザと そのバージョン		