知らないうちにパソコンに潜み
情報を秘密裏に送り続ける

スパイウェアの正体と仕留め方

text : 佐々木俊尚 (Press Archives) P116 – P119 + 山崎誠也 P120 – P125
illust. : Kaneko Nampei

奴らの行動と手口を暴け！

何を目的に暗躍するのか

スパイとウイルスの脅威の差

自分の口座がすっからかん

東京都内に住む転職支援のウェブサイト運営者の男性（43歳）が、取引している外資系銀行からの不審なメールに気づいたのは、昨年9月18日のことだった。その自動応答メールには「振込を完了しました」というタイトルが付けられ、金額は口座残高のほぼ全額にあたる1,640万円。何かの間違いかと思った男性が銀行に問い合わせてみると、預金はすべて消え失せてしまっていた。何者かが男性のIDとパスワードを使ってネットバンキングを利用し、架空名義の口座に送金したのだ。

事件から半年後の今年3月、警視庁は川崎市の元大手シンクタンク社員（35歳）ら2人を、電子計算機詐欺などの容疑で逮捕した。容疑者らの供述で明らかになったのは、ネットカフェのパソコンにスパイウェアを仕込むというきわめて単純な手口だった。容疑者らは、ユーザーのキーボードタイピングを記録する「キーロガー・プログラム」を、渋谷などのネットカフェ十数店舗にこっそりインストールしておき、数週間後に再び店に出向いてタイピングのログを“回収”していた。ログデータを自分のフリーメールアドレスに向けて送信し、別のネットカフェで受信する。ログを読んでネットバンキングのIDとパスワードを抽出していたのだ。この手口は「書店でパソコン雑誌を立ち読みしていて思いついた」（容疑者の供述）と言う。

取材に対し、被害者の男性はこんなふうに気持ちを打ち明けた。

「ネットカフェでバンキングを利用したのは2年も前にたった一度やっただけ。そんな昔のログが今ごろになって悪用されたなんて……」

ネズミのような存在が不気味

この事件は、これまであまり知られていなかったスパイウェアの存在を、きわめて鮮明に浮かび上がらせたと言える。誰でも簡単にインターネットで見つけられるフリーのスパイウェアを悪用でき、そして誰でも簡単に監視される対象になってしまう。「監視社会」は警察当局と個人の間だけの問題ではない。企業と個人、個人と個人の間にまで監視というスキームは入り込んでいる。社会全体が監視社会という枠組みに呑み込まれつつあるのだ。

それが証拠に、スパイウェアは広告やマーケティングといった真っ当なビジネスと密接にかかわっている。後述するアドウェアといわれるプログラムがそうだ。

その枠組みの中では、スパイウェアはコンピュータウイルスと働きは似ているものの、持っている意味合いはまったく異なる存在と言えるかもしれない。

ウイルスは派手な動きで人々を驚かす、破壊の帝王。しかしスパイウェアは監視社会の落とし子だ。こっそりとあなたのマシンに忍び込む、ネズミのような存在。知らず知らずのうちにプライバシーが囓られ、侵食されていく。

スパイが狙うものとは？

ご存じのようにコンピュータウイルスはコンピュータに感染し、ファイルを削除するなどの破壊活動を行う。そして他のコンピュータにも感染し、自己増殖を続けていく。インターネット経由で瞬く間に世界中の数万台、数百万台のパソコンなどに感染して破壊を続けていくさまは、一昨年の「Nimda」や昨年の「SQL Slammer」で嫌というほど見せつけられた。

これに対し、スパイウェアは何をするのだろうか。基本的な定義は、ユーザーの知らないうちにハードディスク内のデータを収集し、ネット経由で特定の場所にこっそり送信してしまうプログラムのことだ。インターネットブラウザーの閲覧履歴やCookieの中身、コンピュータのIPアドレス、OSの種類、ソフトウェアの使用回数などの個人データが収集されている。

これらはアドウェアなど、比較的穏便なスパイウェアの集めるデータだ。キーロガーなど犯罪性の高いスパイウェアともなると、ブラウザー上でタイプしたIDやパスワードやクレジットカード情報、住所、氏名、電話番号など危険性の高い個人データが流出する可能性がある。

スパイウェアは、アプリケーションとしてコンピュータのハードディスクにインストールされる。ということは、ディスク内のすべてのファイルが見られてしまうということだ。集められる情報は限りなく多い。

しかしスパイウェアは、破壊活動は行わない。また自己増殖や感染もしない。目的はあくまでも情報収集なのである。その点が、コンピュータウイルスとは根本的に異なっている。広義で言えば、冒頭の事件に出てきたキーロガーがそうだし、コンピュータウイルスの変種に含まれている「トロイの木馬」もそうだ。たとえば、その代表的な存在である「BackOrifice」は、侵入したコンピュータに対してアプリケーションの実行やファイルの削除、レジストリーの変更、パスワードの入手などの操作ができる。破壊活動が可能な点はウイルスに似ているが、みずから増殖して他のコンピュータに感染することはせずに、情報収集を主に行うという性格は、スパイウェアに限りなく近い。

また、コンピュータウイルスがアンチウイルスソフトやワクチンソフトによって駆除できるのに対し、スパイウェアは基本的にアンチウイルスソフトでは駆除できない。ワクチンソフトのパターンファイルに含まれていない——という定義の仕方もある。これは一面真実なのだが、間違っている点もある。BackOrificeなどのトロイの木馬は、パターンファイルに含まれているからだ。

「トロイの木馬」との区別

では、トロイの木馬とスパイウェアを区別するものは何なのだろうか？

それは、結局「誰が作って、誰が仕込んでいるか」という点だ。スパイウェアの多くは、マーケティングツールと称して一応は真っ当な企業がリリースしている。それに対して、たとえばBackOrificeを開発して配布しているのは、ハッカー集団の「Cult of the Dead Cow」だ。

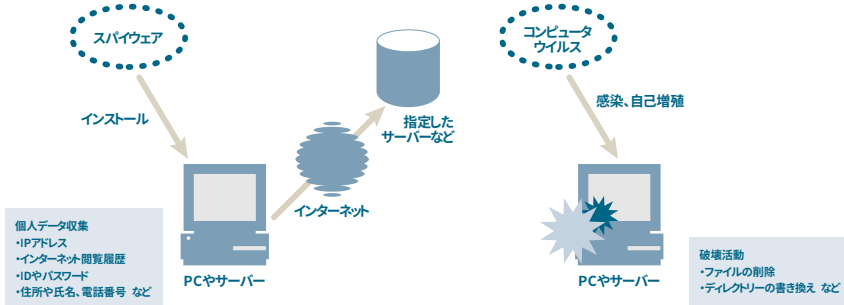
国内のワクチンソフトメーカーの社員は語る。

「アドウェアなどのスパイウェアとコンピュータウイルスを分けるのは、作る側がオフィシャルな企業かどうかという点だけで、動作内容によって区別しているわけではない。アドウェアはソフトのインストールの際に利用規約が掲示されているし、非合法とは言えない。こうしたソフトまでワクチンで駆除してしまうことには問題がある」

「それでは、その“真っ当なマーケティング会社”がどれだけ信用できるのか？」最後はそういう議論に落ち着くのかもしれない。だがユーザーの側から見れば、どの会社が信用できて、どの会社が犯罪まがいなことをしているのかなど、どうやって判断すればいいというのか。アダルトサイトを運営している会社がマーケティングの材料だと言ってスパイウェアをユーザーのパソコンに送り込んだ場合、その信用度を推し量るのはとても難しい。

結局はユーザーの側から見れば、悪意のあるスパイウェアも、マーケティングツールであるアドウェアも、どちらも「自分を監視している薄気味の悪い存在」という意味ではまったく変わりはないのだ。

■ スパイウェアとウィルスの目的と活動



種類	スパイウェア	コンピュータウイルス
目的	個人データの収集	破壊活動
侵入経路	アプリケーションのインストール	感染と自己増殖
開発元	合法的マーケティング・広告企業や非合法な開発者	非合法な開発者
防御・駆除方法	スパイウェア駆除ツール	ワクチンソフト

どのような悪だくみを働くのか

スパイの種別とその活動

アドウェアが猛威を振るうわけ

以上のように、スパイウェアは大きく分ければ、きわめて「犯罪性の高いプログラム」と、マーケティングツールとして企業が利用規約にその存在を記載したうえで提供している「アドウェア」の2つに区分される。そしてここ数年、疫病のような勢いで広がりつつあるのは、アドウェアだ。

そもそもアドウェアがこれほどまでに蔓延するようになった背景には、インターネットの広告モデルの迷走がある。バナー広告から始まったネットの広告は、ネットの普及と反比例するようにクリックするユーザーが減少していき、途中で何度もビジネスモデルの軌道修正を迫られた。そんな中で注目を集めるようになったのが、ユーザー層を思い切り絞り込んだターゲット指向型の広告だ。その最右翼は、最近ますます人気を集めつつある検索エンジンを使ったPPC（Pay Per Click）広告モデルだ。そしてアドウェアというスパイウェアの一種も、広告やマーケティング業界の中でその存在感をひそかに高めつつある。いわば陰の主役とでもいうべき存在だ。

P2Pファイル交換と握手

アドウェアが台頭してきたのには、大きく分けて2つの要因がある。まず常時かつ高速な接続を実現するブロードバンドの普及がある。第二に、そのインフラをベースにしたP2Pファイル交換サービスの流行だ。

単純なバナー広告では、ユーザーをターゲットにするのに限界がある。不特定多数を相手にした広告というビジネスモデルは、すでに成り立たない。ではどうすれば特定の趣味や志向を持った人に対して、うまく広告を発信することができるのだろうか――。

そんな悩みを抱えていた広告業界の前に現れたのが、P2Pファイル交換だった。ファイル交換企業の側は、ナプスター崩壊後の時代の中で、収益を上げるモデルを確立できずに苦闘を続けていた。

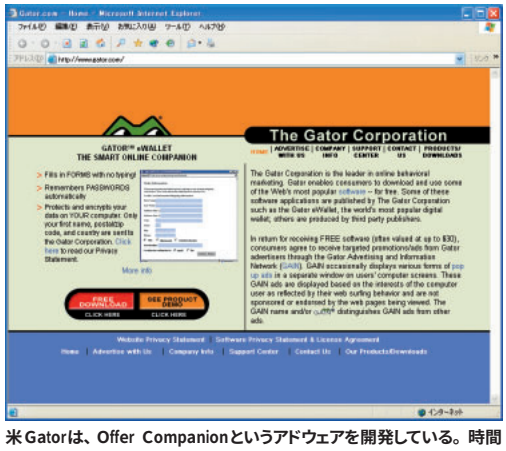
「そうだ、無料でファイル交換サービスを提供する代わりに、ターゲット広告をユーザーに受け入れてもらえばいい！」

そんな発想で、誰が言い出したのかは今となってはわからないが、広告業界とP2Pファイル交換はめでたく縁結びした。そしてその仲を取り持ったのが、アドウェアだったのだ。P2Pファイル交換ソフトをダウンロードしてパソコンにインストールすると、同時にアドウェアもインストールされる。アドウェアのデータによって配信された広告の代金の一部がファイル交換サービスを提供している企業に環流され、収益の源泉となる。

当初は性別や年齢、職業、趣味などをユーザーに入力させ、それに合わせた広告を表示させるというプリミティブなシステムだった。しかし、ただでさえ広告にうさん臭さを感じている海千山千のファイル交換ユーザーたちが、素直に個人データを入力するとは考えにくい。面倒だからと間違った情報を適当に入力するユーザーが相次ぐ。そこでサービス提供者の側は知恵を絞った。「ユーザーが見て回るウェブサイトの履歴を見て、それに合わせた広告を配信すればいい」。

オンラインソフトやサービスに潜む

その発想から、アドウェアはきわめて精巧なスパイウェアへと進化し始めた。ユーザーが何も入力しなくとも、インターネ



米Gatorは、Offer Companionというアドウェアを開発している。時間をかけてダウンロードされ、電子メールアドレスやウェブの巡回の習慣などの個人データをGator.comに送信する。

XUPITERは、インターネットエクスプローラのツールバーを乗っ取ってしまう。ウィルスとして登録しているワクチンソフトもあるほどだ。

ットブラウザーの履歴をこと細かに収集し、そこからユーザーの興味に適合した広告を送り込む。ユーザーがみずからの意志で趣味や買いたいものを入力するのと比べ、自分でも気づいていなかったような潜在意識化の習慣や志向までをも浮かび上がらせてしまう可能性さえ持っている。きわめて巧妙かつ効率の良いターゲッティングを実現してしまったわけだ。

さらにアドウェアはファイル交換だけでなく、ダウンローダーや翻訳、動画再生、検索ツールなどオンラインソフトのさまざまな分野へと浸透している。今ではオンラインソフトやサービスの収益モデルとして、デファクトスタンダードの地位を固めそうな勢いだ。オンラインソフトをインストールしようとすると、たいていアドウェアがおまけに付いてくる、といった状況が現実になりつつある。世の中で動いているパソコンの半数にスパイウェアがこっそり潜んでいるという試算もあるほどだ。

そしてこのどこかの段階でアドウェアは、スタンドアローンで情報を収集するツールから、インターネット経由で個人データを外部に送信するネットワークアプリケーションへと変貌を遂げてしまっている。後者の方が、プライバシー侵害の危険性が高いのは当然だ。何しろ、アドウェアはバックグラウンドで動くアプリケーションとしてハードディスクにインストールされている。つまり、ハードディスクの中身を自由自在に読めてしまうのだ。

もちろん、ファイル交換の無償ソフトをインストールする際に、利用規約をよく読めば「ユーザーの情報をサーバーに送信することを認める」といった記載があることに気づくはずだ。だがたいていのユーザーは、利用規約なんていう長文で面倒なものは読まない。自分でも気づかないままに、スパイウェアをインストールしてしまう結果になっている。そして、この点が大きな批判を浴びる原因となっている。米国ではプライバシー保護団体や消費者団体の間に、広範な反スパイウェア運動が巻き起こっている。「誰も読みもしない利用規約に記載しているだけでは、アカウンタビリティー(説明責任)を果たしたとは言えない」という主張だ。アドウェアと犯罪的なスパイウェアを区別するのは「ユーザーに対して事前の承諾があるかないかである」という考え方もある。だが、小さな文字の利用規約にこっそり書いただけで承諾を得られたと決めてしまうアドウェアは、犯罪的なスパイウェアとほとんど変わらないのではないかというわけだ。これらの団体は、きちんとみずからの意志でアドウェアの導入を承認したユーザー以外にはインストールさせない――つまりオプトイン方式でのインストールを求めている。

■ スパイウェアの種類と特徴

スパイウェアの種類	感染経路	特徴	代表的なソフトや開発元
アドウェア	ファイル交換サービスやダウンローダー、動画再生、翻訳などの無償ソフトにバンドル	利用規約でデータ外部送信の承認をとった上でインストールされる。合法的企業が提供している	Cydoor、Gator、Alexa、Xupiterなど
トロイの木馬	HTMLメールのスクリプトを使った感染など	サーバープログラムをターゲットに感染させ、クライアントから遠隔操作してさまざまなデータを引き出す	BackOrifice2000(ハッカー集団のCult of the Dead Cowが開発・配布)など
キーロガー	HTMLメールのスクリプトを使った感染、直接のインストールなど	ユーザーがキーボードでタイプした内容をすべて記録し、ログを外部送信する	WinWhatWhere、Windows Keylogger、Ghost Keyloggerなど
パスワードクラックツール	HTMLメールのスクリプトを使った感染、直接のインストールなど	ダイヤルアップネットワークなどにユーザーが保存したID、パスワードを取り出し、外部送信する	Ferretなど

手口はより巧妙に進化

そして、アドウェア＝スパイウェアは、今も進化を続けている。たとえば、Cookieを積極的に使った情報収集の仕組みがそうだ。

Cookieというのはご存じのように、ウェブサーバーが送信した情報をユーザー側のパソコンのハードディスクに自動保存しておき、次に同じウェブサイトを訪問した際にこの自動保存されていた情報をウェブサーバーに送信する機能だ。そもそもの目的は、毎回ログイン作業を繰り返さなくてもすむように、ユーザーの認証を管理することによって入力の手間を省くためのものだった。だが最近はこのCookieを悪用した手口も登場してきている。スクリプトを使い、ハードディスクから個人情報を集めてCookie経由で送信する。あるいはユーザーがどのバナー広告を見て、そのうちのどれをクリックしたかといったデータを送信することもできる。

あるいは、特定のウェブサイトをブラウザーで表示すると「ダウンロードしますか?」というメッセージを表示するというパターンも出現している。OKをクリックすると、アドウェアが自動的にダウンロードされ、ActiveXを使って勝手にインストールされる。以前、アダルトサイトなどで利用者にダウンロードを促し、国際電話やダイヤルQ2回線経由のダイアルアップ接続をインストールしてしまう悪質なプログラムがあった。コンピュータリテラシーの低い初心者をうまく騙す手口だったが、それと同じような手法だと言える。さらに最近は、ユーザーの確認画面さえ現れず、サイトを表示すると同時にダウンロードとインストールを始めてしまうという恐ろしいケースさえ出現している。

ここまで来ると、犯罪的なスパイウェアとの境界はほとんどなくなってくる。キータイプをこっそり記録したり、パスワードを抜き出したり、あるいはどんなアプリケーションを起動したかなどをユーザーのパソコンの操作を記録したりするスパイウェアと、マーケティングのためと称するアドウェアは限りなく融合していく。

いずれにせよ、問題は同じだ。スパイウェアやアドウェアがハードディスクのどこを見て、どんなデータを集め、そしてそれをどこに送っているのか――そうした情報は、ユーザー側にはいっさい明らかにされない。そして勝手にシステムに常駐し、ユーザーの個人情報を外部に流し続けているのだ。

スパイの息の根を止める武器を装備しろ！

無料でも確実に仕留める2大ソフトウェア

「SpyBot」と「Ad-aware 6」で倒せ

海外製のソフトでも安心

ここまでで、スパイウェアの脅威や正体がつかめただろう。次はいよいよスパイをあぶり出して仕留めよう。

スパイウェアはアプリケーションの形式やインターネット一時ファイル（Cookie）、レジストリーの改変などのあらゆる手段でPC内に忍び込む。これらを手動で探し出して除去するのは大変だ。そこでスパイウェアの検索や除去に特化したソフトウェアの出番だ。除去専用ソフトならわずか数ステップで、あやしいスパイたちを一網打尽にできる。今回はスパイウェア除去ソフトの中から代表格のソフトを2つ紹介する。両者とも海外製のソフトウェアだが操作は比較的簡単で、日本語に対応しているソフトもあるので、苦手意識を持たずに使用できるだろう。

まずは、除去ソフトの老舗と言えるLAVASOFT社製の「Ad-aware 6」だ。このソフトは、個人使用に限って無料のStandard（Personal）版、有料のPlus版（26.95ドル）とProfessional版（39.95ドル）の3種類がある。ここではStandard版を中心に紹介する。なお、Standard版には、英語が苦手でも日本語化できるツールが存在する。今回は残念ながら掲載の許諾をいただけなかったので紹介は割愛するが、インターネットでAd-awareを調べればきっと見つかるだろう。もし、そのツールを使うなら同梱の文書をよく読んで自己責任で利用してほしい。

もう1つは、無料で利用できるPepiMK Software製の「SpyBot-Search & Destroy」（以下SpyBot）で、最近は対スパイウェアの定番になりつつある。こちらは標準で日本語メニュー化ができるうえ、ヘルプも日本語化できる。また、easyとadvancedの2つのモードがあるため、初心者は手軽に扱えてベテランは細かく設定をカスタマイズできる。

両ソフトともに機能はほぼ共通しており、手動操作では困難なメモリーに常駐するタイプのスパイウェアでさえも除去できる。インターネット経由で常にスパイウェアの最新定義ファイルを更新することも可能だ。また、広告付きの無料ソフトなどはスパイウェアを除去すると起動できなくなることがあるが、両ソフト共に除去実行前にバックアップを取り、不具合が生じた場合に必要なデータを復旧する機能もある。

併用でさらに完璧に仕留める

どちらが優れているかは一概には言い難い。一般にはAd-awareはスパイウェアの発見率に、SpyBotは除去率に定評がある。好みに応じて使い分けるのもいいし、併用して確実にスパイウェアの除去を狙うのもいい。ただし併用時の注意もある。前述したお互いのバックアップデータをスパイウェアと認識することがあるのだ。併用するなら、お互いのデータを無視するように設定しよう。

さて、簡単にスパイウェアを除去できるとは言っても少し注意が必要だ。単一のファイルのスパイウェアなら指示どおりの削除で問題はない。しかし、レジストリーに関連した項目の変更は、最悪の場合にシステムが起動しなくなることもある。レジストリーに関連するスパイウェアは、インターネットなどで情報を入手してから除去してほしい。SpyBotならデフォルトの設定だけの除去で十分な効果がある。またメモリー常駐型など、スパイウェアの種類によっては「使用中のため除去できないもの」もある。このようなときは、ウィンドウズをセーフモードで起動してからスパイウェア除去ソフトを使おう。これらのスパイウェア除去ソフトにファイアーウォールソフトを組み合わせると、より堅牢な環境を作りだせる。

では、さっそくスパイを退治しよう！　2つのツールの使い方を紹介していくが、それぞれ下記のURLからソフトをダウンロードしておいてほしい。

SpyBot-Search & Destroy

対応OS：ウィンドウズ95/98/Me/NT4.0/2000/XP
価格：無料（寄付を受け付けている）

トップページ
URL http://security.kolla.de/

ダウンロード
URL http://security.kolla.de/index.php?lang=en&page=download

Ad-aware 6 Standard

対応OS：ウィンドウズ98/Me/NT4.0/2000/XP
価格：無料（個人使用限定）

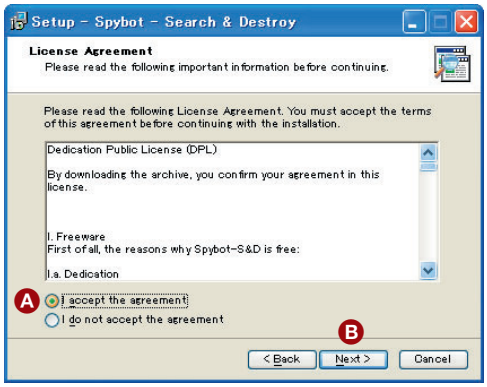
日本語トップページ
URL http://www.lsfileserv.com/japanese/

ダウンロード
URL http://www.lsfileserv.com/japanese/support/download/

I 日本語も使えるSpyBot-S&Dで楽々排除

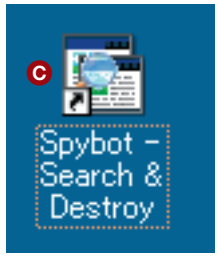
■インストールと日本語環境設定

1



インストールは、ダウンロードした「SpyBotsd12.exe」をダブルクリックして、ウィザードに従うだけの単純なものだ。途中、ライセンス合意の確認があるので「I accept the agreement」をチェックAする。あとは「Next」ボタンBを押していけば完了する。

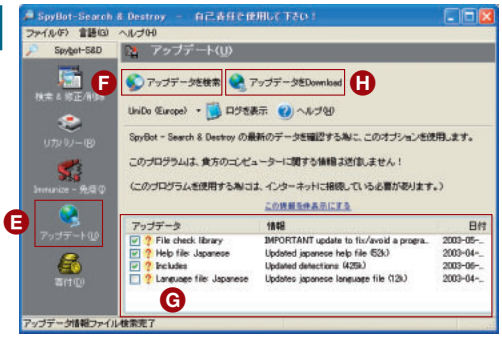
2



次にデスクトップに作成されたSpyBotのアイコンCをダブルクリックして起動しよう。この場合、easyモードで起動することになる。初回起動時にはウィザード画面が登場するので、日本の国旗を選択Dすれば日本語化できる。

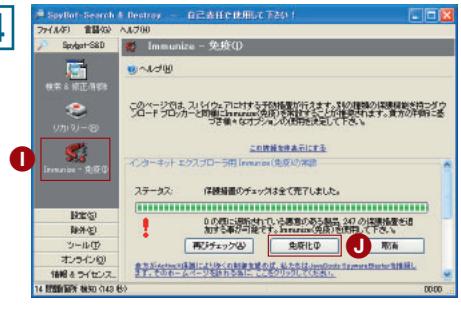
easyモードは操作が簡単で検出と除去に特化しており、advancedモードは細かく設定を変えて検出と除去ができる。

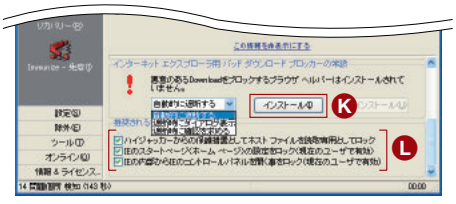
3



今度は画面左側のアップデートアイコンEをクリックして画面を切り替えよう。「アップデータを検索」Fをクリックすると、画面下にアップデーター覧Gが登場する。ここで「File check library」「Help file: Japanese」「Includes」の3つを選んで、「アップデートをDownload」Hをクリックしよう。これでSpyBot本体のアップデート、ヘルプファイルの日本語化、定義ファイルの更新が完了し、SpyBotがadvancedモードで再起動する。easyモードを使いたいならさらに再起動してもいいだろう。

4





最後に、より対策を強固にするには、画面左の「Immunize-免疫」アイコンIをクリックして画面を切り替えよう。「インターネットエクスプローラ用Immunize(免疫)の常設」欄で「免疫化」ボタンJをクリックし、その後に、さらに下へスクロールして「インターネットエクスプローラ用バッドダウンロードブロッカーの常設」欄で、メニューから遮断方法を選択して「インストール」ボタンKをクリックする。また、advancedモードで起動している場合は「推奨される様々な保護措置」も適宜チェックLしておこう。

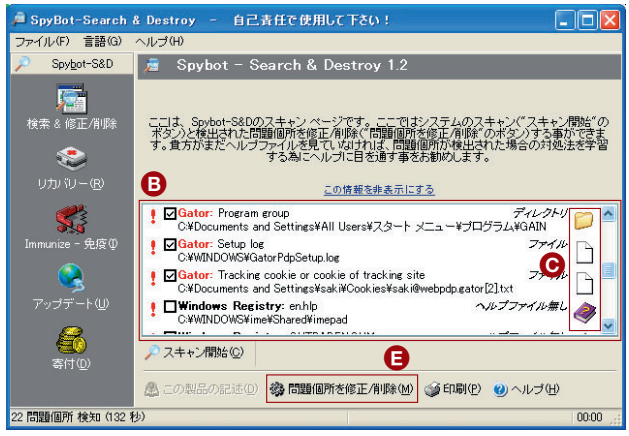
免疫化すると、ブラウザーの弱点をついてスパイウェアをインストールする悪質なウェブサイトにアクセスしても、ある程度防御してくれる。

■スキャンと削除、復旧

1

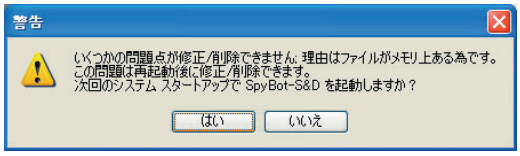
SpyBotを起動し、起動画面の「スキャン開始」ボタンAをクリックする(画面はeasyモード)。

2



スキャンが終了すると、スパイウェアの一覧Bが登場する。要注意のファイルには赤文字ですでにチェックマークが付いている。赤字のリストはほぼスパイウェアに間違いない。心配な場合は、このリスト内のアイコンCをシングルクリックして、その項目の詳細な情報Dを確認する。確認したら「問題個所を修正/削除」ボタンEをクリックするとチェックマークの付いたファイルが削除される。

3



2を実行した後に、メモリー上で実行されているスパイウェアは削除できないことがある。警告ウィンドウの指示に従って「はい」をクリックすると、次回のシステム起動時に自動的にSpyBotが起動してスキャンを開始し、問題のスパイウェアを除去する。

4

ここまでの除去作業をした後に、一部のソフトが動かなくなるなどの不具合が生じたときには、SpyBotの起動画面の「リカバリー」アイコンFをクリックする。除去したデーター覧Gが登場するので、該当するデータにチェックHをして「チェックした項目を修復」ボタンIを押すと、不具合が修正される。

赤字で表示されているものは、ほぼなにも考えずに削除してしまって差し支えない。しかし、赤字で表示されずに黒の太字で表示されているファイルは、どのようなファイルなのか詳しく調べてから削除した方がいい。レジストリーファイルやキーの場合は、最悪システムが起動しなくなることもあるからだ。あくまでも自己責任での利用になる。レジストリーの知識に自信がない人はそのまま残しておいてもいいだろう。

■便利な設定

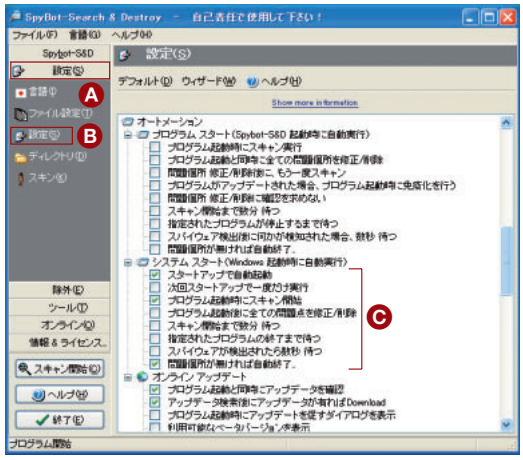
標準の設定のままでも十分に使えるが、さらに便利に使うには設定を変えてみよう。PCの起動時に自動的にスパイウェアを検索するように設定しておくと、常にクリーンな状態に保てる。また、SpyBotは標準設定では起動ドライブのみしかスキャンしない。そのため外部メディアや増設したハードディスクをスキャンする方法も紹介する。

●スタートアップ時の自動実行

1

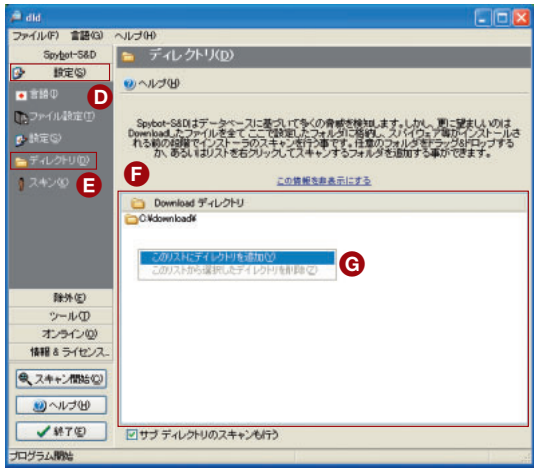
ウィンドウズのスタートメニューから、SpyBotをadvancedモードで起動する。

2



「設定」タブボタンAをクリックして、「設定」アイコンBをクリックしよう。「オートメーション」の「システムスタート」で、「スタートアップで自動起動」「プログラム起動時にスキャン開始」「問題個所がなければ自動終了」の3つにチェックを付ける(C)と、システム起動時にスパイウェアの検知を自動実行してくれる。

●外部メディアや増設ハードディスクのスキャン

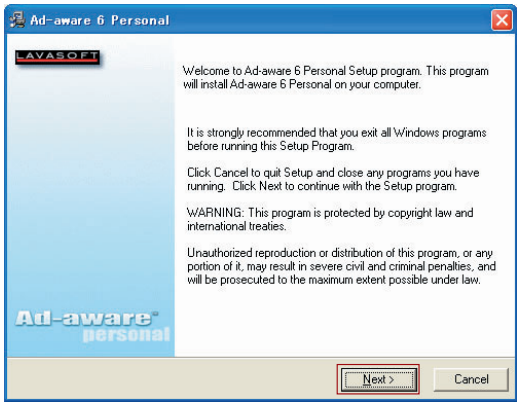


「設定」タブDの「ディレクトリ」アイコンEをクリックし、「Downloadディレクトリ」の欄Fに、目的のドライブやフォルダをドラッグする。もしくは、この欄で右クリックしてメニューから追加するG。

II Ad-aware 6で根こそぎ排除

■インストールと定義ファイルの更新

1

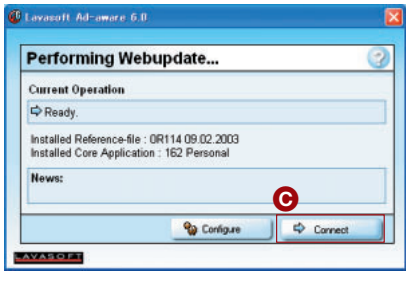


ダウンロードした「aaw6.exe」をダブルクリックして、画面の指示に従って順次「Next」ボタンを押していくだけで、インストールは完了する。

2

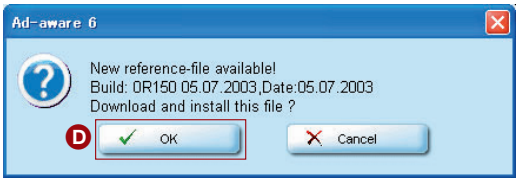
Ad-awareを起動して、起動画面で地球アイコンAもしくは画面下の「Check for updates now」Bの文字をクリックする。

3



「Performing Webupdate」のウィンドウが登場するので「Connect」Cボタンを押す。

4



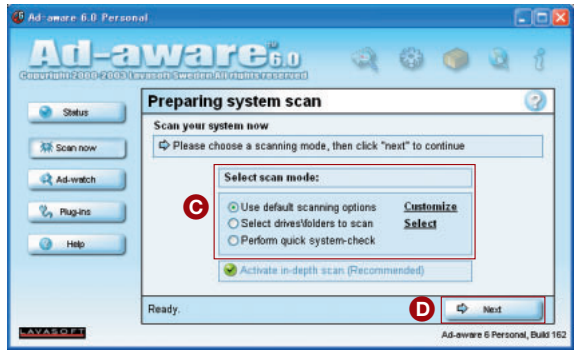
最新データが存在すれば図のようなアラートが登場するので「OK」Dボタンを押すと最新定義ファイルに更新される。

■スキャンと削除、復旧

1

Ad-awareの起動画面左側の「Scan now」Ⓐもしくは画面下部の「Start」Ⓑをクリックする。

2



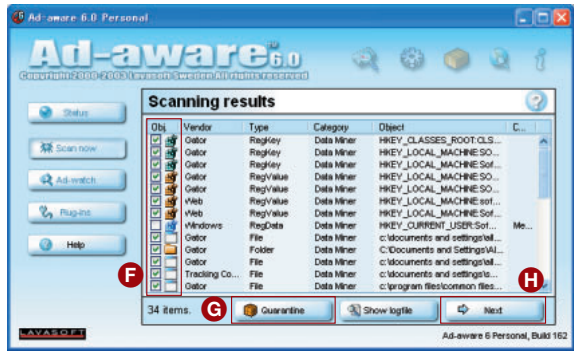
「Preparing system scan」画面に切り替わったら、スキャンモードを選ぶⒸ。「Use default scanning options」は次ページの「外部メディアや増設ハードディスクのスキャン」の設定と共通しており、外部メディア以外の特定のフォルダを指定するものだ。「Select drives \ folders to scan」は「Select」をクリックして、任意のドライブやフォルダーをスキャンするモード「Perform quick system-check」はウィンドウズフォルダー以下のフォルダーとメモリー、レジストリーをスキャンする高速モードだ。「Next」Ⓓをクリックするとスキャンが開始される。

3

スキャンが終了し、スパイウェアが見つかると、虫のアイコンと赤い文字で注意してくれる。「Next」ボタンⒺで「Scanning results」画面に移動しよう。

P125の2にある「General Options」の設定で「Automatically quarantine objects prior to removal」（スパイウェアの自動バックアップ機能）のチェックをはずしていなければ、そのまま「Next」Ⓗボタンをクリックしよう。

4



リストアップされたスパイウェアから排除するものにチェックⒻしていく。いったん「Quarantine」ボタンⒼをクリックしてバックアップを作成してから「Next」ボタンⒽをクリックしよう。これでスパイウェアの削除は完了する。

5

スパイウェアを排除したあとに動かなくなってしまうソフトがあった場合は、Ad-awareの起動画面で画面上部の箱型のアイコンⒾか「Open quarantine-list」Ⓙをクリックして、隔離したスパイウェアの画面に移動する。

6

隔離オブジェクト一覧Ⓚの中から、復旧させたいバックアップを選択して「Restore」ボタンⓁをクリックすると、不具合が修正される。

■便利な設定

Ad-awareにも、SpyBotと同様にシステムのスタートアップ時に自動的に起動してスパイウェアを検出してくれる便利な機能がある。このほか、外部メディアや増設したハードディスク、特定のフォルダーでのスパイウェアのスキャン方法も紹介する。

●スタートアップ時の自動実行

1

Ad-aware 6を起動し、起動画面上部の歯車アイコンAから設定画面の「General Options」を呼びだそう。ほかの画面になっていた場合は、2左側の「General」ボタンBでも呼び出せる。

2

「Run at Windows start up」Cにチェックをして、「Customize」Dの文字をクリックする。

3

「Startup Settings」の画面になるので、「Startup scan mode」Eを好みに合わせて設定する。「No automated scanning」は自動的にスキャンさせない設定。「Use my default scan setting」は、「Customize」Fで特定のフォルダーのみをスキャンするようにカスタマイズできる。また、「Perform quick system check」では高速スキャンが可能。これらのスキャンモードを設定し、システムスタートアップ時にスパイウェアを自動的に削除してAd-awareを終了するなら、「Startup action」Gの2つの項目をチェックし、「Proceed」(H)をクリックすればすべての設定が完了する。

SpyBotとAd-awareの2つともスタートアップに登録が可能だ。この場合、Ad-awareが先に起動し、そのスキャン中にSpyBotが起動してスキャンし始める。検知したスパイウェアの隔離方法により不具合が生じることがあるので、スタートアップで自動実行するのは、どちらか一方にしておこう。

●外部メディアや増設ハードディスクのスキャン

設定画面の「Scanning」ボタンIをクリックして、「Click here to select drives + folders」Jを選んでドライブやフォルダーを指定する。また、「Scan within archives」Kをチェックすると、アーカイブに潜んでいるスパイウェアも検出できる。設定したらLをクリックすると完了する。

有償版との差は？

Ad-aware 6には有料バージョンのPlus版（26.95ドル）とProfessional版（39.95ドル）がある。Plus版ではブラウザーでのポップアップ広告のブロックやレジストリーの書きかえなどを、常駐して監視する「Ad-Watch」機能がある。Professional版はPlus版にさらに機能が追加されており、ファイルの実行プロセスなどをリアルタイムで監視する機能が加わったり、プラグインを使って一段と機能を追加できたりする。

Plus版から利用可能な常駐監視機能「Ad-Watch」

［インターネットマガジン　バックナンバーアーカイブ］ ご利用上の注意

このPDFファイルは、株式会社インプレスR&D（株式会社インプレスから分割）が1994年～2006年まで発行した月刊誌『インターネットマガジン』の誌面をPDF化し、「インターネットマガジン　バックナンバーアーカイブ」として以下のウェブサイト「All-in-One INTERNET magazine 2.0」で公開しているものです。

http://i.impressRD.jp/bn

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、URL、団体・企業名、商品名、価格、プレゼント募集、アンケートなど）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真の撮影者、イラストの作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は収録されていない場合があります。
- このファイルやその内容を改変したり、商用を目的として再利用することはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用する際は、出典として媒体名および月号、該当ページ番号、発行元（株式会社インプレスR&D）、コピーライトなどの情報をご明記ください。
- オリジナルの雑誌の発行時点では、株式会社インプレス R&D（当時は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

このファイルに関するお問い合わせ先
株式会社インプレスR&D
All-in-One INTERNET magazine 編集部
im-info@impress.co.jp