bitdefender

ANTIVIRUS 2008

ユーザガイド

BitDefender Antivirus 2008
ユーザガイド

発行 2008.04.14

法的表示


bitdefender

目次

ライセンスおよび保証

この契約条件に同意いただけない場合は、ソフトウェアをインストールしないでください。 "同意する"、"OK"、"続ける"、"はい"、を選ぶか、ソフトウェアをインストールするか使用すると、その方法を問わずお客様はこの契約条件を完全に理解し、同意したとみなされます。

これらの条件は、関連図書および購入いただいたライセンスによって提供されたアプリケーションのすべてのアップデートおよびアップグレード、図書内に記載されたすべての関連するサービス契約、そしてこれらのすべてのコピーを含む、お客様にライセンスされた家庭用 BitDefender Solutions および Services に適用されます。

このライセンス契約は、国際著作権法および国際協定によって保護されている、コンピュータソフトウェアおよびサービスを含み、場合により関連するメディア、印刷物、および"オンライン"あるいは電子的な図書も含む、上記の BITDEFENDER のソフトウェア製品（以下、"BitDefender"）を使用するための、お客様（個人あるいは法人を問わず）と BITDEFENDER の間で交わされる法的効力のある契約です。BitDefender をインストール、複製、あるいは使用することで、お客様は、この契約の内容に従うことに同意したとみなされます。

この契約条件に同意いただけない場合は、BitDefender をインストールまたは使用しないでください。

BitDefender ライセンス. BitDefender は、著作権法および国際著作権協約および他の知的財産法および協定で保護されています。BitDefender は、使用権をライセンスされるのであって、販売されているわけではありません。

ライセンスの許諾。BITDEFENDER は、お客様に、そしてお客様だけに、BitDefender を使うための、以下の非独占的で、限定され、移転できない、有償のライセンスを許諾します。

アプリケーションソフトウェア。お客様は、ライセンスされたユーザの総数まで、必要な台数のコンピュータに BitDefender をインストールして使うことができます。またバックアップの目的で、１個のコピーを追加で作成することができます。

デスクトップユーザライセンス。このライセンスは、ネットワークサービスを提供していない単独のコンピュータにインストールできる BitDefender ソフトウェアに適用されます。それぞれの管理ユーザは、このソフトウェアを単独のコンピュータにインストールすると共に、他のデバイスにバックアップ目的で１個のコピーを追

加で作成できます。許可される管理ユーザの数は、ライセンスで許可されたユーザの数です。

ライセンス条件。ここで許諾されたライセンスは、BitDefender を購入いただいた日から始まり、購入いただいたライセンスの期限で終了します。

期限。この製品は、ライセンスの期限が切れると同時に、その機能が動作しなくなります。

アップグレード。BitDefender がアップグレード版の場合、お客様は、BITDEFENDER によってアップグレード可能と明記された BITDEFENDER を使うための正式なライセンスを所有していなければなりません。アップグレード版の BitDefender は、お客様がアップグレードの権利を持つ製品を置き換える、あるいは補足するものです。アップグレード後の製品は、このライセンス契約条件に沿ってのみ使用が可能です。BitDefender が、お客様に単一の製品としてライセンスされたソフトウェアパッケージの一部分をアップグレードする場合、BitDefender はその単一パッケージの一部としてのみ使用あるいは転送が可能で、ライセンスされたユーザの総数以上に使う目的で分割はできません。この契約条件は、オリジナルの製品あるいはアップグレード後の製品に関して、お客様と BITDEFENDER の間に存在する事前に交わされた契約を置き換え、それに取って代わります。

著作権。BitDefender に関するすべての権利、資格、および所有権、および（BitDefender に付随する画像、写真、ロゴ、アニメーション、ビデオ、オーディオ、ミュージック、テキスト、"アプレット"を含むが、それに限定されない）BitDefender に関するすべての著作権、関連印刷物、および BitDefender のすべての複製は、BITDEFENDER が所有しています。BitDefender は、著作権法および国際協定の規定で保護されています。お客様は BitDefender をその他のあらゆる著作物と同様に扱わなければなりません。BitDefender に付随する印刷物をコピーすることはできません。BitDefender が存在するメディアや形態に関わらず、作成されたすべての複製に対し、オリジナルの状態のままの著作権の記述を作成し、含めなければなりません。BitDefender ライセンスを、サブライセンス、貸与、販売、リース、共有することはできません。BitDefender の、解析、再コンパイル、逆アセンブル、派生的作品の作成、改造、翻訳、ソースコードを表示しようとするあらゆる行為は禁止されています。

限定保証。BITDEFENDER は、お客様が BitDefender を入手してから30日間、BitDefender が配布されるメディアに不具合がないことを保証します。この保証に違反があった場合のお客様への救済措置は、BITDEFENDER が独自の判断で、受け取った不良メディアを交換するか、BitDefender のためにお客様が支払った金額を返金

するか、どちらかのみです。BITDEFENDER は、BitDefender に不具合やエラーがないこと、またはそうしたエラーが修正されることを保証しません。BITDEFENDER は、BitDefender がお客様の要望を満たすことも保証しません。

この契約に明記されていない限り、BITDEFENDER は、明示的または黙示的に関わらず、その提供する製品、改良、関連するメンテナンスあるいはサポート、その他の素材（有形無形に関わらず）あるいはサービスについて、その他のすべての保証を放棄します。BITDEFENDER は、商品性、特定の目的への適応性、称号、不具合の有無、データの正確さ、含まれる情報の正確さ、システムとの統合性、および規則、法律、取引の過程、一般慣行、あるいは商習慣の中で生じたものであっても、第三者のソフトウェア、スパイウェア、アドウェア、Cookie、電子メール、文書、広告、あるいはそれらに類するものをフィルタリング、無効化、あるいは除去することによる第三者の権利侵害に対する（ただし、ここに列記した内容に限定されない）暗示的な保証を含む、あらゆる暗示的な保証および条件を放棄することをここに明記します。

損害に対する免責。BitDefender を使用、試験、あるいは評価するすべての使用者は、BitDefender の品質および動作のすべてのリスクを負います。どのような場合も、BITDEFENDER は、BITDEFENDER がそのような損害の存在や可能性について助言を受けていたとしても、BitDefender の使用、動作、あるいは送信（ただし、ここに列記した内容に制限されない）によって起きた、直接あるいは間接のあらゆる種類の損害に対して責任を負いません。州によっては、付随的、または結果的に生じる損害について、責任の放棄あるいは制限を認めない場合がありますので、上記の制限あるいは除外はお客様に適用されない可能性もあります。いずれの場合でも、BITDEFENDER の責任は、お客様が BITDEFENDER を購入するために払った金額を超えることはありません。上記の免責および制限条項は、お客様が BitDefender の使用、評価、試験に同意したかに関わらず適用されます。

ユーザへの重要なお知らせ。. このソフトウェアは、フォールト・トレラントではなく、フェイルセーフな動作あるいは操作を必要とする危険環境で使用するために設計されておらず、またその使用も想定していません。このソフトウェアは、航空機の航行操作、核施設、通信システム、兵器システム、直接あるいは間接の生命維持システム、航空管制、あるいは動作不良が死、重度の身体障害あるいは財産損害につながるあらゆる用途や施設では使用できません。

一般。この契約は、ルーマニアの法律および国際著作権規定および協定に準拠しています。これらのライセンス条件から起きた紛争の裁定を行う唯一の管轄および裁判地は、ルーマニアの裁判所とします。

BitDefender の使用にかかる価格、経費、および手数料は、お客様への事前の通知なく変更される場合があります。

この契約の内容の一部が無効な場合でも、その無効性が、この契約の他の部分の有効性に影響することはありません。

BitDefender および BitDefender ロゴは、BITDEFENDER の商標です。この製品で、あるいはそれに関連して使われるその他の商標は、それぞれの所有者の所有物です。

お客様が契約条件のいずれかに違反した場合は、このライセンスは即座に解除されます。解除されても、BITDEFENDER あるいはその代理店からの返金はありません。製品の使用にかかる守秘義務および各種制限の条件は、解除以降も有効です。

BITDEFENDER は、諸条件をいつでも改訂することができ、改訂された内容と共に配布されるバージョンのソフトウェアには自動的に適用されます。諸条件の一部が、無効で強制不能と分かった場合も、他の条件は有効で強制可能であり、その正当性には影響しません。

この諸条件の翻訳内容が他の言語の解釈と異なったり矛盾する場合は、BITDEFENDER によって発行された英語版の内容が常に優先します。

BITDEFENDER への連絡は、5, Fabrica de Glucoza street, 72322-Sector 2, Bucharest, Romania, あるいは 電話番号：40-21-2330780 または FAX：40-21-2330763、電子メールアドレス：office@bitdefender.comへお願いします。

はじめに

このガイドは、お使いのパーソナルコンピュータのセキュリティ・ソリューションとしてBitDefender Antivirus 2008を選択されたすべてのお客様を対象にしています。この図書に記載された情報は、コンピュータについて詳しいお客様だけでなく、Windows を使えれば誰でも理解できるでしょう。

この図書では、BitDefender Antivirus 2008、その開発メーカと開発者について説明し、そのインストールを手順を追って解説し、その設定の仕方を説明します。BitDefender Antivirus 2008の使い方や、アップデート、テスト、カスタマイズする方法についても記載します。BitDefender を最大限有効利用する方法が分かるはずです。

その内容が、お客様にとって楽しく、有意義であることを願っています。

1. この図書で使われている決まり事

1.1. 字体の決まり事

この図書では、内容を読みやすくするためにいくつかの字体を使っています。その内容を、次の表にまとめました。

見た目	説明
sample syntax	構文の例は、monospacedの文字で記載されています。
http://www.bitdefender.com	URL リンクは、http あるいは ftp サーバ上の外部の場所を表しています。
support@bitdefender.com	電子メールアドレスが、連絡先としてテキストに挿入されています。
「はじめに」 (p. xii)	これは、この文書内の別の場所を示す内部リンクです。
filename	ファイルおよびディレクトリは、monospaced フォントを使って記載されています。

見た目	説明
option	すべての製品オプションは、strong文字で記載されています。
sample code listing	コードリストは、monospaced文字で記載されています。

1.2. 警告

警告は、テキスト内の注意書きで、現在の段落に関係する追加情報にお客様の注意を惹くよう、見た目で区別されています。

注意

注意は、ちょっとした意見のようなものです。無視しても構いませんが、注意では、関連する話題についての特別な機能やリンクなど、重要な情報が提供される場合があります。

重要項目

お客様が注意すべき内容で、読み飛ばしていけません。通常、緊急ではなくても、重要な情報が提供されます。

警告

これは、お客様が注意深く扱う必要のある重大な情報です。内容に従って、損することはあり得ません。非常な危険を伴う内容を含みますので、よく読んで理解しておいてください。

2. この図書の構造

この図書は、いくつかの大きな主題に分かれています。 さらに、技術用語を説明する用語集も用意されています。

インストール. BitDefender をワークステーションにインストールするステップバイステップな解説です。BitDefender Antivirus 2008をインストールするための、分かりやすいチュートリアルとなります。正しいインストールの必須条件からはじまり、インストール操作すべてを順を追って説明します。最後に、BitDefender をアンインストールしなければならない場合のため、削除操作についても説明しています。

基本的な管理. BitDefender の基本的な管理とメンテナンスの説明です。

詳細なセキュリティ管理. BitDefender が提供するセキュリティ機能の詳細な説明です。 この章では、詳細設定コンソールにあるすべてのオプションについて説明します。 お使いのコンピュータをウイルス、スパイウェア、Rootkit などあらゆる種類のマルウェアの脅威から効率よく守るために、すべての BitDefender モジュールを設定し使用する方法について解説します。

BitDefender Rescue CD. BitDefender Rescue CD の説明です。この起動可能な CD が提供する機能を理解し、使えるようになるでしょう。

問い合わせ先. 予期しない事態が起きた時、相談するための連絡先です。

用語集. 用語集では、この文書の中で出会う専門用語あるいは一般的でない用語を説明します。

3. コメントのお願い

この図書をよりよくするために、お客様のご意見、ご感想をお待ちしております。内容については、可能な限り調べて検査しています。しかし、最高の文書を提供できるように、この図書内でお客様が見つけた問題点、あるいは改良できる点があれば、教えてください。

電子メールをdocumentation@bitdefender.comへ送ってください。

重要項目
いただいたメールを間違いなく処理できるように、この文書の内容に関するすべての電子メールは、必ず英語で書いてください。

インストール

1. BitDefender Antivirus 2008のインストール

このユーザガイドのBitDefender Antivirus 2008のインストールの項では、以下の内容を扱っています：

■システム要項
■インストール手順
■初回設定ウィザード
■アップグレード
■BitDefender の修復あるいは削除

1.1. システム要項

製品が正常に機能するよう、インストールする前に、お使いのコンピュータで次のオペレーティングシステムが実行されており、その他の必要システム環境が満たされていることを確認してください：

■動作環境：Windows 2000 SP4 / XP SP2 32b & 64b / Vista 32b & 64b; Internet Explorer 6.0（以降）

Windows 2000

■800 MHz以上のプロセッサ
■最小256 MBのRAMメモリ（512 MB推奨）
■最小60 MBのハードディスク空き容量

Windows XP

■800 MHz以上のプロセッサ
■最小256 MBのRAMメモリ（１GB推奨）
■最小60 MBのハードディスク空き容量

Windows Vista

■800 MHz以上のプロセッサ
■最小512 MBのRAMメモリ（１GB推奨）
■最小60 MBのハードディスク空き容量

BitDefender Antivirus 2008の試用版は、BITDEFENDER のウェブサイト http://www.bitdefender.comからダウンロードできます。

1.2. インストール手順

Setup ファイルを見つけてダブルクリックしてください。すると、手順にそって設定が行えるウィザードが起動します。

設定ウィザードを起動する前に、BitDefender はより新しいインストールパッケージがないか確認します。新しいバージョンがあれば、ダウンロードするように促されます。新しいバージョンをダウンロードするにははいをクリックし、Setup ファイル内のバージョンをインストールするにはいいえをクリックしてください。なお、Intego の Dual Protection をご購入のお客様は、そのまま Setup ファイル内のバージョンをインストールして後日アップデートを行うか、代理店に連絡して新しいインストーラを入手してください。

インストール手順

次の手順に従って、BitDefender Antivirus 2008をインストールしてください：

1. 次へ進むには次へをクリックし、インストールを中止するにはキャンセルをクリックしてください。
2. 次へをクリックしてください。

   お使いのコンピュータに他のアンチウイルス製品がインストールされていると、BitDefender Antivirus 2008がその旨警告します。 該当する製品をアンインストールするには、削除をクリックしてください。 検出された製品を削除せずにインストールを続けるには、次へをクリックしてください。

警告

BitDefender をインストールする前に、検出された他のアンチウイルス製品をアンインストールすることを強くお薦めします。１台のコンピュータで２つ以上のアンチウイルス製品を同時に実行すると、システムが使用不能となる場合があります。

3. ライセンス契約を読んで、同意するを選び、次へをクリックしてください。条件に同意いただけない場合は、キャンセルをクリックしてください。インストール処理は途中で破棄され、Setup を終了します。
4. デフォルトでは、BitDefender Antivirus 2008は C:¥Program Files¥BitDefender¥BitDefender 2008 にインストールされます。 インストール先のパスを変更するには、参照をクリックし、BitDefender Antivirus 2008をインストールしたいフォルダを選択してください。

   次へをクリックしてください。
5. インストール処理に関するオプションを選択してください。 いくつかは、デフォルトで選択されています：
   - ■「お読みください」ファイルを開く - インストールの最後で、「お読みください」ファイルを開きます。
   - ■デスクトップにショートカットを作成 - インストールの最後で、BitDefender Antivirus 2008のショートカットをお使いのデスクトップに作成します。
   - ■インストールが完了したらCDを取り出す - インストールの最後で、CDを取り出します；このオプションは、CDから製品をインストールした場合にだけ表示されます。
   - ■Windows Defender を無効にする - Windows Defender を無効にします；このオプションは、Windows Vista でのみ表示されます。

   製品のインストールを開始するには、インストールをクリックしてください。

   重要項目

   インストール中に、ウィザードが表示されます。ウィザードは、お使いのBitDefender アンチウイルス 2008の登録、BitDefender アカウントの作成、重要なセキュリティタスクを実行するための BitDefender の設定を手引きします。ウィザードの手順を完了して、次の手順に進んでください。
6. 終了をクリックしてください。 設定ウィザードがインストールを完了するために、お使いのシステムを再起動するよう促される場合があります。 できるだけ早く、実行することをお勧めします。

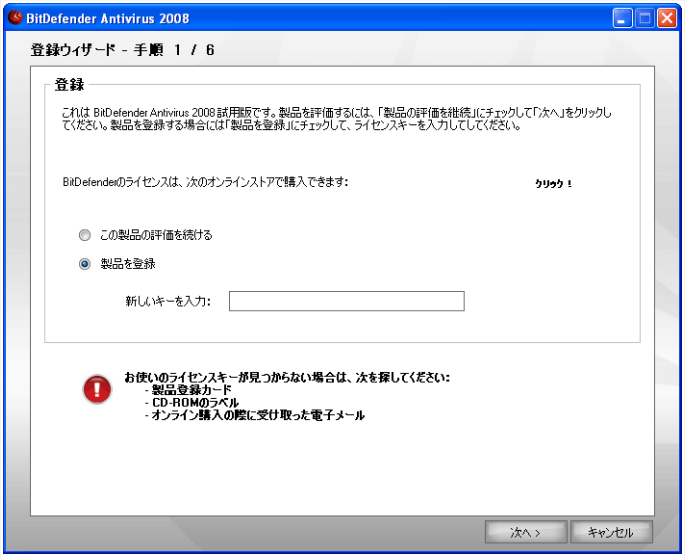
   インストール先としてデフォルト設定を使った場合、BitDefenderという名前の新しいフォルダがProgram Filesに作成され、その中にBitDefender 2008というサブフォルダがあります。

1.3. 初回設定ウィザード

インストール処理中に、ウィザードが表示されます。ウィザードは、お客様のBitDefender アンチウイルス 2008の登録、BitDefender アカウントの作成、重要なセキュリティタスクを実行するための BitDefender の設定を手引きします。

このウィザードの完了は必須ではありません。しかし時間の節約と、BitDefender アンチウイルス 2008をインストールする前にお使いのシステムが安全であることを確認するためにも、ウィザードを完了させることをお勧めします。

1.3.1. 手順1/6 - BitDefender アンチウイルス 2008を登録



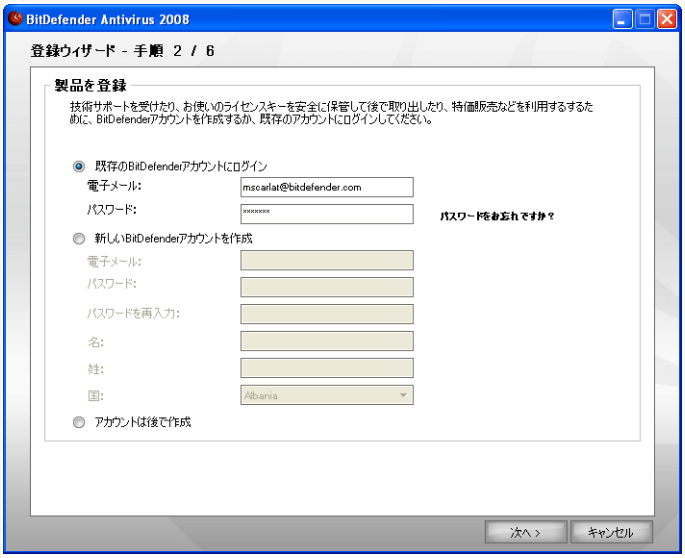
登録

製品を登録 を選択すると、BitDefender アンチウイルス 2008を登録できます。ライセンスキーを新しいキーを入力欄に入力してください。

製品の評価を続けるには、製品の評価を継続を選択してください。

次へをクリックしてください。

1.3.2. 手順2/6 - BitDefenderアカウントを作成



アカウントの作成

BitDefender アカウントを持っていません

BitDefender の無償技術サポートおよび他の無料サービスを受けるには、アカウントが必要です。

注意
アカウントを後日作成される場合は、該当するオプションを選択してください。

新しい BitDefender アカウントを作成を選択し、必要な情報を入力してください。ご入力いただいたデータの機密は守られます。

■電子メール - お使いの電子メールアドレスをご入力ください。

■パスワード - 上で指定したユーザの有効なパスワードを入力してください。

注意
パスワードは、半角英数字で４文字以上にしてください。

■パスワードを再入力 - 上で入力したパスワードを再度入力してください。

■名 - お名前をご入力ください。

■姓 - 苗字をご入力ください。

■国 - お住まいの国名を選択してください。

注意
今入力した電子メールアドレスとパスワードを使用し、http://myaccount.bitdefender.com から皆さんのアカウントにログインしてください。

アカウントを正常に作成するには、まずお使いの電子メールアドレスを有効にしなければなりません。電子メールアドレスを確認し、BitDefender 登録サービスから送られる電子メールの指示に従ってください。

次へをクリックしてください。

すでに BitDefender アカウントを持っています

皆さんが既に BitDefender アカウントを登録されていれば、BitDefender は自動でそのアカウントを検出します。 その場合は、そのまま次へをクリックしてください。

既に有効なアカウントをお持ちで、BitDefender がそれを検出しなかった場合は、既存の BitDefender アカウントにログインを選択し、アカウントの電子メールアドレスとパスワードをご入力ください。

注意
入力したパスワードが誤っていた場合、次へをクリックするとパスワードの再入力を求められます。 Okをクリックしてパスワードを再入力するか、キャンセルをクリックしてウィザードを終了してください。

パスワードを忘れたら、お使いのパスワード忘れた場合？をクリックし、表示をご参照ください。

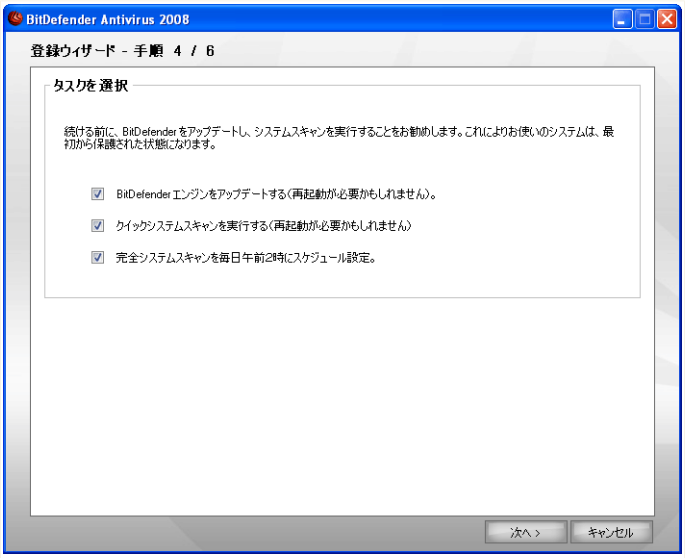
次へをクリックしてください。

1.3.3. 手順3/6 - リアルタイムウイルスレポート（RTVR）について

RTVRの情報

次へをクリックして続けるか、キャンセルをクリックしてウィザードを終了してください。

1.3.4. 手順4/6 - 実行するタスクを選択



タスクを選択

お使いのシステムのセキュリティのために重要なタスクを実行するよう、BitDefenderアンチウイルス 2008を設定してください。

次のオプションが指定できます：

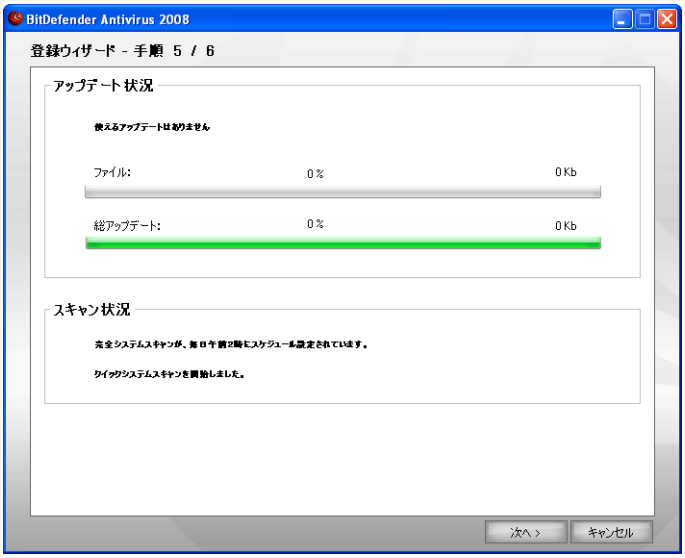
■BitDefender エンジンをアップデート（再起動が必要な場合があります） - お使いのコンピュータを最新の脅威から守るために、次の手順で BitDefender エンジンのアップデートが実行されます。
■クイックシステムスキャンを実行（再起動が必要な場合があります） - 次の手順で、WindowsおよびProgram Filesフォルダ内のお使いのファイルが感染していないことを BitDefender が確認するため、クイックシステムスキャンが実行されます。
■毎日午前２時に完全システムスキャンを実行 - 毎日午前２時に完全システムスキャンを実行します。

重要項目
お使いのシステムのセキュリティ万全にするためにも、次の手順へ進む前に、これらのオプションを有効にしておくことをお勧めします。

最後のオプションだけを選択するか、あるいはオプションを１つも選択していない場合、次の手順はスキップされます。

次へをクリックして続けるか、キャンセルをクリックしてウィザードを終了してください。

1.3.5. 手順5/6 - タスクが完了するまでお待ちください

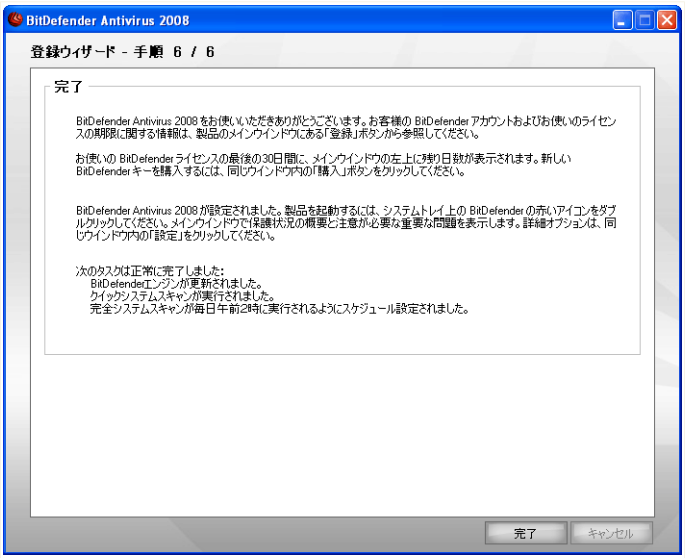


タスクの状況

タスクが完了するまでお待ちください。前の手順で選択したタスクの状況が確認できます。

次へをクリックして続けるか、キャンセルをクリックしてウィザードを終了してください。

1.3.6. 手順6/6 - 概要を表示



終了

これが設定ウィザードの最後の手順です。

ウィザードを完了し、インストール処理に進むには、終了をクリックしてください。

1.4. アップグレード

アップグレードの方法は、次から選べます：

■以前のバージョンを削除せずにインストール - v8以降では、Internet Security は除外

Setup ファイルをダブルクリックし、「インストール手順」 (p. 3)画面に表示されるウィザードをご利用ください。

重要項目

インストール処理中に、Filespy サービスが原因のエラーメッセージが表示されます。OKをクリックしてインストールを続けてください。

■以前のバージョンをアンインストールし、新しいバージョンをインストール – BitDefender 全バージョン用

「インストール手順」 (p. 3)に解説されている通り、まずお使いの以前のバージョンを削除しなければなりません。続いてコンピュータを再起動し、新しいバージョンをインストールしてください。

重要項目

BitDefender v8 以降からアップグレードする場合、事前に BitDefender 設定、友達一覧、迷惑メール送信者一覧を保存しておくことをお勧めします。 アップグレード処理が完了したら、それらを読み込んでください。

1.5. BitDefender を修復あるいは削除

BitDefender アンチウイルス 2008を修復あるいは削除したい場合、Windowsスタートメニューから次のように選択してください：スタート → プログラム → BitDefender 2008 → 修復、削除。

次へをクリックすると、選択について確認されます。次の選択が行える新しいウインドウが開きます：

■修復 – 以前の Setup でインストールされたすべてのプログラムコンポーネントを再インストールします。

BitDefender の修復を選ぶと、新しいウインドウが開きます。 修復をクリックすると、修復処理が開始します。

メッセージが表示されたらコンピュータを再起動し、その後、インストールをクリックしてBitDefender アンチウイルス 2008を再インストールしてください。

インストール処理が完了したら、新しいウインドウが開きます。 終了をクリックしてください。

■削除 – インストールされているすべてのコンポーネントを削除します。

注意
クリーンに再インストールする場合は、削除を選択することをお勧めします。

BitDefender の削除を選ぶと、新しいウインドウが開きます。

重要項目
BitDefender を削除すると、以降はウイルスやスパイウェアなどのマルウェアの脅威から保護されません。 BitDefender のアンインストール後、Windows Defender を有効にするには、該当するチェックボックスを選択してください。 このオプションは Windows Vista でのみ使えます。

削除をクリックすると、お使いのコンピュータからのBitDefender アンチウイルス 2008の削除を開始します。

削除処理中に、フィードバックを送るためのダイアログが表示されます。 OKをクリックして、５つ以下の簡単な質問で構成されたオンラインのアンケートに回答してください。 アンケートに回答したくない場合、キャンセルをクリックしてください。

削除処理が完了したら、新しいウインドウが開きます。 終了をクリックしてください。

注意
削除処理が完了したら、Program FilesからBitDefenderフォルダを削除することをお勧めします。

BitDefender の削除中にエラーが起きました

BitDefender の削除中にエラーが起きたら、削除処理は中止され、新しいウインドウが開きます。 UninstallTool を実行をクリックして、BitDefender を完全に削除してください。 アンインストールツールは、自動削除処理で削除されなかったすべてのファイルと registry キーを削除します。

基本的な管理

2. はじめに

BitDefender をインストールすれば、お使いのコンピュータは保護されます。いつでも BitDefender Security Center を開いて、システムのセキュリティ状態を確認し、予防措置を講じ、製品を完全に設定することができます。

BitDefender Security Center を開くには、Windows スタートメニューから、スタート → プログラム → BitDefender 2008 → BitDefender Antivirus 2008を選ぶか、あるいはシステムトレイ内の BitDefender アイコンをダブルクリックしてください。

BitDefender Security Center

The BitDefender Security Center には、２つの画面があります：

■状態画面：お使いのコンピュータのセキュリティの脆弱性についての情報を表示し、その修正を手助けします。お使いのコンピュータに影響する問題がいくつあるか簡単に確認できます。対応する赤いすべての問題を修正ボタンをクリックす

ることで、お使いのコンピュータの脆弱性は、その場で解決されるか、簡単に修正するための手順が案内されます。また、４種類のセキュリティのカテゴリに対応して４つの状況ボタンが表示されます。緑の状態ボタンは、危険がないことを意味します。黄あるいは赤のボタンは、中位あるいは高いセキュリティの危険を表します。修正するには、その黄/赤のボタンをクリックし、修正ボタンを一つずつクリックするか、すべてを修正をクリックします。灰色は、設定されていないコンポーネントを表します。

■クイックタスク画面：お使いのシステムを安全に保ち、データを守ります。

さらに BitDefender Security Center には、いくつかの便利なショートカットがあります。

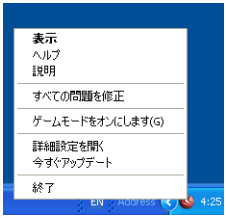
リンク	説明
購入	製品を購入するためのページを開きます。
マイアカウント	お客様の BitDefender アカウントのページを開きます。
登録	登録ウィザードを開きます。
ヘルプ	ヘルプファイルを開きます。
サポート	BitDefender のサポートウェブページを開きます。
設定	詳細設定画面を開きます。
履歴	BitDefender の履歴&イベントを記載したウインドウを開きます。

2.1. システムトレイ内の BitDefender アイコン

製品全体を素早く管理するために、システムトレイ上の BitDefender アイコンを使うこともできます。

アイコンをダブルクリックすると、BitDefender Security Center が開きます。アイコンを右クリックすると、BitDefender 製品を素早く管理できるコンテキストメニューが呼び出せます。

表示 - BitDefender Security Center を開きます。



BitDefender アイコン

■
■ヘルプ - ヘルプファイルを開きます。
■説明 - BitDefender のウェブページを開きます。
■すべての問題を修正 - セキュリティの脆弱性を除去する手助けをします。
■ゲームモードをオン/オフにする - ゲームモード をオン / オフにします。
■詳細設定を開く - 詳細設定画面を利用できるようにします。
■今すぐアップデート - すぐにアップデートを開始します。 アップデート状況を表示するウインドウが新たに開きます。
■終了 - アプリケーションを終了します。

ゲームモードがオンのときには、G という文字が BitDefender アイコンの上に表示されます。

お使いのシステムに影響する重大な問題がある場合、エクスクラメーションマーク (!) が BitDefender アイコン上に表示されます。 マウスカーソルをアイコン上に移動すると、お使いのシステムに影響する問題の数を確認できます。

2.2. スキャン処理バー

スキャン処理バーは、お使いのシステム上のスキャン処理をグラフに視覚化したものです。

緑のバー（ファイル領域）は1秒間にスキャンされたファイルの数を、0から50の範囲で表示します。

処理バー

注意
スキャン処理バーは、リアルタイム保護が無効だとファイル領域上に赤いバツ印を表示して知らせます。

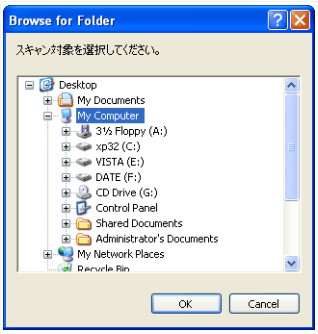
スキャン処理バーを使ってオブジェクトをスキャンできます。スキャンしたいオブジェクトをドラッグして、バーの上にドロップしてください。　詳細については、「ドラッグ&ドロップスキャン」 (p. 72)を参照してください。

グラフィカルなインタフェースを表示したくなければ、右クリックして隠すを選んでください。

2.3. BitDefender の手動スキャン

特定のフォルダを素早くスキャンするには、BitDefender の手動スキャンを使ってください。

BitDefender の手動スキャンを使うには、Windows のスタートメニューから、スタート → プログラム → BitDefender 2008 → BitDefender 手動スキャンと選んでください。 次のウインドウが開きます：



BitDefender の手動スキャン

フォルダを参照し、スキャンしたいフォルダを選び、OKをクリックすれば完了です。　BitDefender Scanner　が表示され、スキャン処理を手引きします。

2.4. ゲームモード

新しいゲームモードは、ゲームの処理への影響を最小限にするよう、保護設定を一時的に変更します。 ゲームモードをオンにすると、次の設定が適用されます：

■BitDefender の警告とポップアップ表示がすべて無効になります。

■BitDefenderリアルタイム保護レベルは、消極的に設定されています。

ゲームモードがオンのときには、G という文字が BitDefender アイコンの上に表示されます。

2.4.1. ゲームモードを使用

ゲームモードは、次の方法のいずれかで使えるようになります：

■システムトレイの BitDefender アイコンを右クリックし、ゲームモードをオンにするを選択します。

■Alt+Gキー（デフォルトのホットキー）を押します。

重要項目
ゲームが終わったらゲームモードをオフにしてください。ゲームモードをオンにするのと同じやり方でオフにできます。

2.4.2. ゲームモードのホットキーを変更

ホットキーを変更するには、次の手順で行ってください：

1. BitDefender Security Center の設定 をクリックし、設定コンソールを開きます。

   注意
   または、システムトレイ内の BitDefender アイコンを右クリックし、詳細設定を開くを選択してください。

2. 詳細をクリックしてください。
3. ゲームモードのホットキーを有効オプションから、希望するホットキーを選択してください。

   ■使用するキーは、次の中から希望するものにチェックします：Control キー(Ctrl)、Shift キー(Shift)、Alternate キーAlt)。

   ■編集欄で、使用したい文字キーに対応する文字を入力します。

   例えば、Ctrl+Alt+Dホットキーを使用するには、Ctrl、Altにチェックして、Dを入力します。

注意
ゲームモードのホットキーを有効のチェックマークを外すと、ホットキーは使えなくなります。

3. セキュリティの状態

セキュリティの状態画面には、お使いのコンピュータの脆弱性を系統的に整理し、使いやすい一覧として表示します。BitDefender アンチウイルス 2008では、問題がお使いのコンピュータのセキュリティに影響する際は、いつでも知ることができます。

セキュリティの状態を表す４種類のボタンがあります：

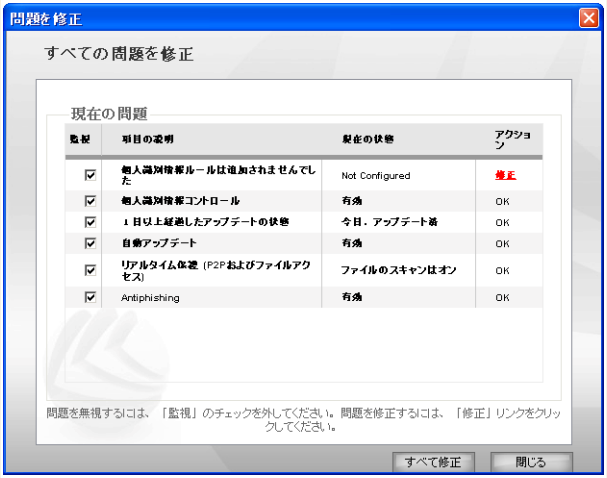
■アンチウイルス
■アンチフィッシング
■個人識別情報コントロール
■アップデート

その左には、お使いのシステムセキュリティに影響する問題の数と、赤いすべての問題を修正ボタンがあります。

４つの状態ボタンは、現在の保護のレベルに応じて、緑、黄、赤、あるいは灰色で表示されます。

■緑は、お使いのコンピュータの危険度が低いことを意味します。
■黄は、お使いのコンピュータの危険度が中位であることを意味します。
■赤 は、お使いのコンピュータの危険度が高いことを意味します。
■灰色は、設定されていないコンポーネントを表します。

セキュリティの問題を修正するのは面倒ではなく、すべての問題を修正ボタンをクリックするだけで実行されます。 新しいウインドウが開きます。



セキュリティの問題

セキュリティの問題一覧とその状態の簡単な説明が表示されます。

特定の問題だけを修正するには、対応する修正ボタンをクリックしてください。その場で修正されるか、ウィザードの手順に従うことで修正されます。すべての問題を修正する場合はすべて修正ボタンをクリックし、対応するウィザードの手順に従ってください。

設定コンソールを使うには、Security Center の下部にある設定リンクをクリックしてください。 コンテキストヘルプが表示され、これらの問題と修正方法について詳しく伝えます。

重要項目

すべての問題には、それぞれチェックボックスがあり、デフォルトではすべてチェックされています。特定の問題をセキュリティの危険度の算出対象から除外するには、対応するチェックボックスのチェックを外してください。お使いのコンピュータがさらされているセキュリティの危険を高める可能性がありますから、このオプションは注意してご使用ください。

問題を後で修正するなら、閉じるをクリックします。

3.1. アンチウイルスの状態ボタン

アンチウイルスの状態ボタンが緑なら、心配することは何もありません。もしボタンが黄、赤、あるいは灰色なら、お使いのコンピュータは、中位から高い危険にさらされています。

状態ボタンの色は、お使いのコンピュータの安全に影響する設定をしたときだけでなく、重要なタスクを見落とした場合にも変化します。例えば、前回のシステムスキャンが古いと、セキュリティの状態ボタンは黄になります。非常に古いと、赤になります。

次の表は、セキュリティの危険度を算出する際に対象となる要素についての情報を表示します。

問題	色
前回のシステムスキャンが古い	黄
前回のシステムスキャンが非常に古い	赤
リアルタイム保護が無効	赤
アンチウイルス保護レベルの設定が消極的	黄

問題を修正するには、次の手順で行ってください：

1. アンチウイルスの状態ボタンをクリックしてください。
2. 一つずつ修正するには修正ボタンをクリックし、すべてを一括して修正するにはすべてを修正ボタンをクリックしてください。
3. 問題がその場で修正されない場合、ウィザードに沿って修正してください。

3.2. アンチフィッシングの状態ボタン

アンチフィッシングの状態ボタンが緑なら、心配することは何もありません。ボタンが赤のときは、お使いのコンピュータが高いセキュリティの危険にさらされています。

次の表は、セキュリティの危険度を算出する際に対象となる要素についての情報を表示します。

問題	色
アンチフィッシング保護は有効です	緑
アンチフィッシング保護は無効です	赤

問題を修正するには、次の手順で行ってください：

1. アンチフィッシングの状態ボタンをクリックしてください。
2. 一つずつ修正するには修正ボタンをクリックし、すべてを一括して修正するにはすべてを修正ボタンをクリックしてください。
3. 問題がその場で修正されない場合、ウィザードに沿って修正してください。

3.3. 個人識別情報コントロール状態ボタン

個人識別情報コントロールの状態ボタンが緑なら、心配することは何もありません。ボタンが赤あるいは灰色なら、お使いのコンピュータが高いセキュリティの危険にさらされています。

次の表は、セキュリティの危険度を算出する際に対象となる要素についての情報を表示します。

問題	色
個人情報保護は設定されており、有効です	緑
個人情報保護は設定されていますが、無効です	赤
個人情報保護は設定されていません	灰色

問題を修正するには、次の手順で行ってください：

1. 個人識別情報コントロールの状態ボタンをクリックしてください。
2. 一つずつ修正するには修正ボタンをクリックし、すべてを一括して修正するにはすべてを修正ボタンをクリックしてください。
3. 問題がその場で修正されない場合、ウィザードに沿って修正してください。

3.4. アップデートの状態ボタン

アップデートの状態ボタンが緑なら、心配することは何もありません。ボタンが赤の時は、お使いのコンピュータが高いセキュリティの危険にさらされています。

次の表は、セキュリティの危険度を算出する際に対象となる要素についての情報を表示します。

問題	色
自動アップデートは有効です	緑
自動アップデートは無効です	赤
前回のアップデートは１日前です	赤

問題を修正するには、次の手順で行ってください：

1. アップデートの状態ボタンをクリックしてください。
2. 一つずつ修正するには修正ボタンをクリックし、すべてを一括して修正するにはすべてを修正ボタンをクリックしてください。
3. 問題がその場で修正されない場合、ウィザードに沿って修正してください。

4. クイックタスク

４つの状態ボタンの下には、クイックタスク画面があります。

4.1. セキュリティ

BitDefender には、お使いの BitDefender を最新に保ち、お使いのコンピュータをウイルスから守るためのセキュリティモジュールが付属します。

セキュリティモジュールに入るには、セキュリティタブをクリックしてください。

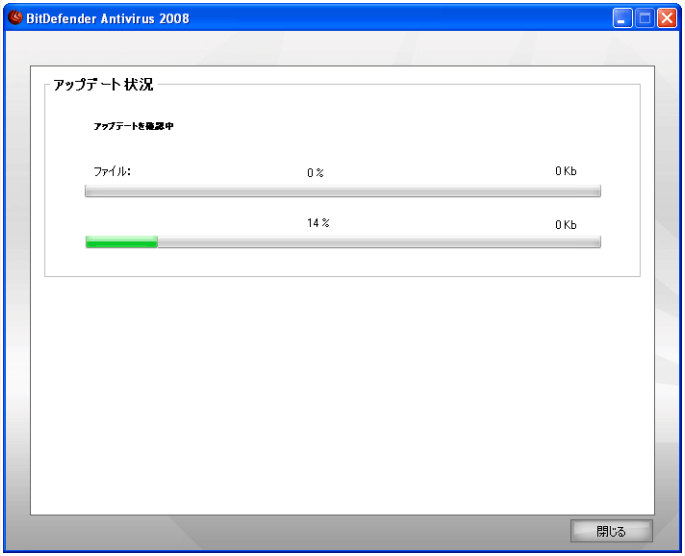
次のボタンが使えます：

■今すぐアップデート - すぐにアップデートを開始します。
■マイドキュメントをスキャン - お使いの書類と設定のクイックスキャンを開始します。
■ディープシステムスキャン - お使いのコンピュータ全体（アーカイブも含む）のスキャンを開始します。
■完全システムスキャン - お使いのコンピュータ全体（アーカイブは除く）のスキャンを開始します。

4.1.1. BitDefender のアップデート

毎日新しいマルウェアが生まれ、検出されています。そのため BitDefender を最新のマルウェアのシグネチャで更新することが重要です。

デフォルトでは、お使いのコンピュータの起動時、およびその後は１時間毎にアップデートをチェックします。 BitDefender をアップデートするには、今すぐアップデートをクリックしてください。 アップデート処理が開始され、次のようなウインドウが表示されます：



BitDefender のアップデート

このウインドウで、アップデート処理の状態を確認できます。

アップデート処理はその場で実行されます。つまりアップデートされるファイルは、順次上書きされていきます。この方法により、アップデート処理は製品の動作に影響せず、同時に脆弱性も除外されます。

このウインドウを閉じるには、閉じるをクリックしてください。　閉じてもアップデート処理は中止されません。

注意
ダイアルアップ接続でインターネットを利用しているなら、BitDefender　のアップデートを定期的に行うのがよいでしょう。

再起動を求められたらコンピュータを再起動してください。. 主要なアップデートでは、コンピュータの再起動を求められることがあります。 アップデートが再起動を必要とする際、毎回確認されたくなければ、確認せず、再起動を待機をチェックしてください。 それにより、次回アップデートが再起動を必要とする際には、皆さ

んがご自分でシステムを再起動するまではアップデート前のファイルを使って動作を継続します。

再起動をクリックすると、すぐにシステムを再起動します。

後でシステムを再起動するには、OKをクリックしてください。 できるだけ早くシステムを再起動することをお勧めします。

4.1.2. BitDefender によるスキャン

マルウェアを対象にお使いのコンピュータをスキャンするには、対応するボタンをクリックしてスキャンタスクを実行します。 次の表は、簡単な説明付きの使用可能なスキャンタスク一覧です：

タスク	説明
マイドキュメントをスキャン	現在のユーザの重要なフォルダをスキャンする場合は、このタスクをご使用ください：マイドキュメント、デスクトップ、スタートアップ。 これで、お使いの書類の安全、安全な作業スペース、アプリケーション起動時のクリーンな実行を確実にします。
ディープシステムスキャン	システム全体をスキャンします。 デフォルトの設定では、ウイルス、スパイウェア、アドウェア、Rootkitなど、お使いのシステムのセキュリティの脅威となるあらゆる種類のマルウェアをスキャンします。
完全システムスキャン	アーカイブを除く、システム全体をスキャンします。 デフォルトの設定では、ウイルス、スパイウェア、アドウェア、Rootkit など、お使いのシステムのセキュリティの脅威となるあらゆる種類のマルウェアをスキャンします。

注意

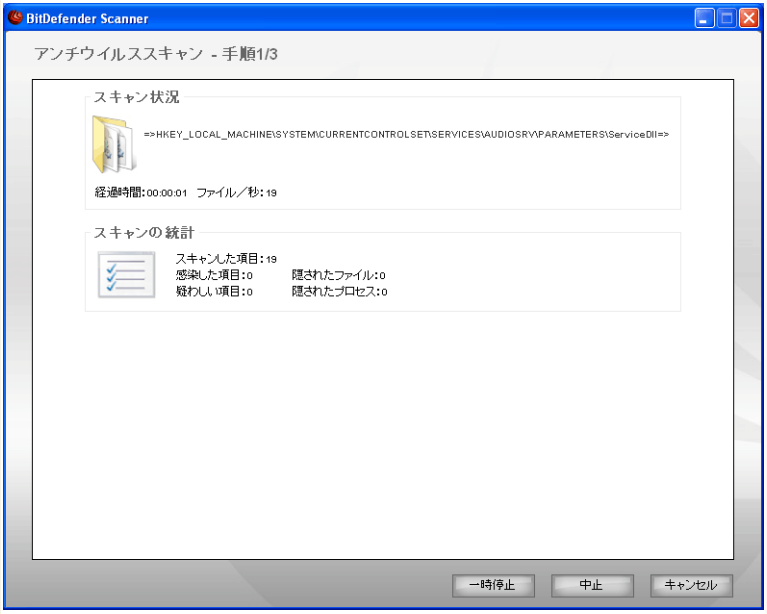
ディープシステムスキャンおよび完全システムスキャンのタスクは、システム全体を調べるため、スキャン処理には時間がかかります。ですから、これらのタスクは比較的暇なときに実行するか、できればシステムが使われていないときに実行することをお勧めします。

オンデマンドのスキャン処理を実行すると、クイックあるいは完全スキャンに関わらず、BitDefender Scanner が表示されます。

次の３つの手順に従って、スキャン処理を完了させてください。

手順1/3 - スキャン

BitDefenderは、選択したオブジェクトのスキャンを開始します。



スキャン

スキャンの状況および統計（スキャン速度、経過時間、スキャン済み／感染／疑わしい／隠された オブジェクトの数、など）を確認できます。

注意
スキャンの内容によっては、スキャン処理に時間がかかる場合があります。

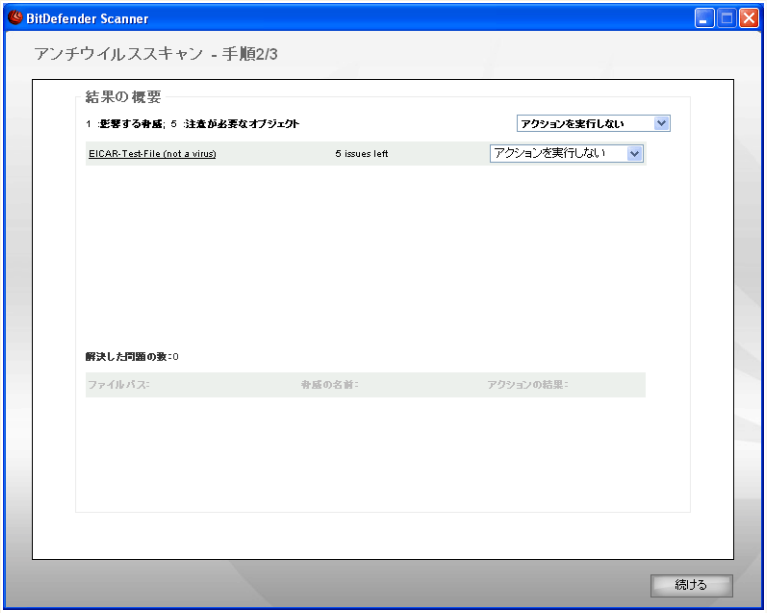
スキャン処理を一時停止するには、一時停止をクリックしてください。スキャンを再開するには、再開をクリックしてください。

停止&はいをクリックすれば、スキャンをいつでも停止できます。その後、ウィザードの最後の手順に移動します。

BitDefender がスキャンを完了するまでお待ちください。

手順2/3 - アクションを選択

スキャンが完了したら、スキャンの結果を表示するウインドウが新たに開きます。



アクション

お使いのシステムに影響する問題の数を確認できます。

感染したオブジェクトは、感染したマルウェアの数を基にグループ表示されます。感染したオブジェクトについて詳しい情報を参照するには、検出された脅威に対応するリンクをクリックします。

問題のそれぞれのグループごとに一括して実行されるアクションを選ぶか、問題ごとに個別のアクションを指定できます。

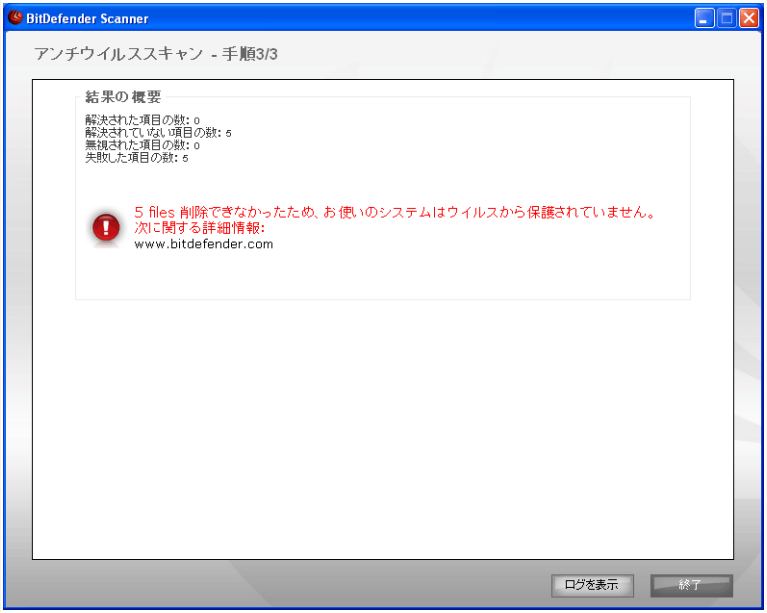
メニューには、次のオプションが表示されます：

アクション	説明
アクションなし	検出したファイルに対して、アクションを実行しません。
ウイルスを除去	感染したファイルからウイルスを除去します。
削除	疑わしいファイルを削除します。
可視にする	隠されたオブジェクトを表示させます。

指定したアクションを適用するには、続けるをクリックしてください。

手順3/3 - 結果を表示

BitDefender が問題の修正を完了したら、スキャンの結果が新しいウインドウに表示されます。



概要

結果の概要を確認できます。 レポートファイルは、対応するタスクのプロパティウインドウにあるログ画面に自動で保存されます。

重要項目
削除処理を完了するため、お使いのシステムを再起動するよう促される場合があります。

終了をクリックして、ウインドウを閉じてください。

BitDefender はいくつかの問題を解決できませんでした

多くの場合、BitDefender は検出した感染ファイルの感染除去、あるいは隔離を正常に行います。 ただし、解決できない問題も存在します。

解決できない問題があれば、www.bitdefender.comの BitDefender サポートチームにご相談ください。 サポート担当者がその問題の解決のお手伝いをします。

BitDefender はパスワード保護された項目を検出しました

パスワード保護された対象には次の２つの種類が含まれています：アーカイブおよびインストーラです。 それらは、感染したファイルを持っていて、さらに実行されない限りは、システムに実際の影響を与えることはありません。

これらの項目が安全であることを確認するには：

- パスワード保護された項目がアーカイブである場合は、ファイルを解凍して、それぞれのファイルをスキャンしてください。 スキャンしたいファイルあるいはフォルダを右クリックし、BitDefender アンチウイルス 2008を選択してください。
- パスワード保護された項目がインストーラである場合は、インストーラ実行前にリアルタイム保護 が有効になっていることをご確認ください。 インストーラが感染している場合、BitDefender は感染を検出し、隔離します。

BitDefender がこれらの対象を再び検出しないようにするには、それらをスキャン処理の例外に追加してください。 スキャンの例外に追加するには、 設定 をクリックして設定コンソールを開き、 アンチウイルス > 例外 と選択してください。 詳しくは、スキャンから除外されるオブジェクトをご参照ください。

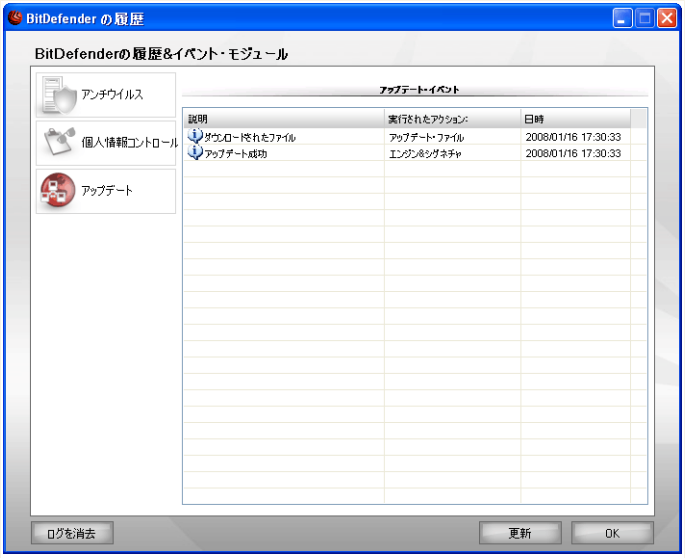
BitDefender は疑わしいファイルを検出しました

疑わしいファイルはヒューリスティック分析によって検出されたファイルであり、まだシグネチャが公開されていないマルウェアに感染している可能性があります。

スキャン中に疑わしいファイルが検出されると、それをBitDefender 研究所へ提出するように促されます。 OK をクリックすると、それらのファイルを BitDefender 研究所に送信します。

5. 履歴

BitDefender Security Center ウインドウの下部にある履歴リンクは、BitDefenderの履歴&イベントを表示する別のウインドウを開きます。このウインドウにはセキュリティ関連のイベントの概要が表示されます。例えば、アップデートが正常に完了したか、お使いのコンピュータでマルウェアが見つかったか、バックアップタスクでエラーがなかったか、などを簡単に確認できます。



イベント

BitDefender の履歴&イベントの表示内容を絞り込むために、左側に次のカテゴリが用意されています：

■アンチウイルス
■個人情報
■アップデート

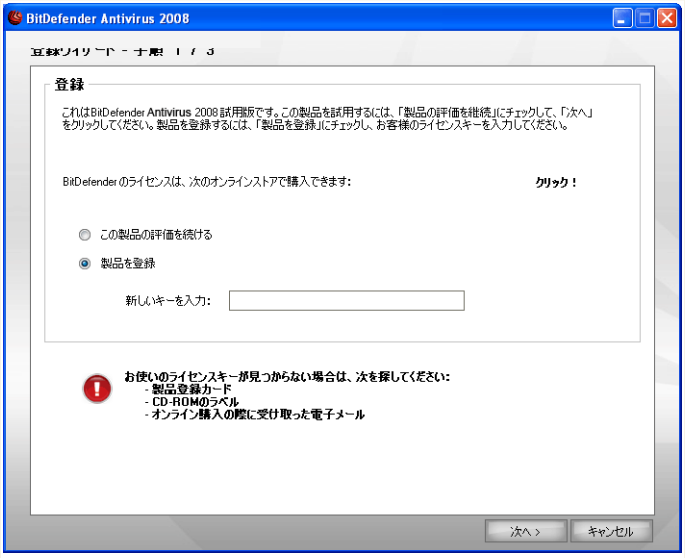
各カテゴリに、イベント一覧が用意されています。各イベントには次の情報が表示されます：簡単な説明、それが起きた際に BitDefender が実行したアクション、それが起きた日時。一覧内の特定のイベントの詳細情報を表示するには、イベントをダブルクリックしてください。

古いログを削除するにはログを削除をクリックしてください。最新のログを表示するには、更新をクリックしてください。

6. 登録

BitDefender アンチウイルス 2008 には30日間の試用期間が設けられています。BitDefender アンチウイルス 2008 を登録、ライセンスキーを変更、または BitDefender アカウントを作成するには、BitDefender Security Center ウインドウ上部にある 登録 リンクをクリックしてください。 登録ウィザードが表示されます。

6.1. 手順1/3 - BitDefender アンチウイルス 2008を登録



登録

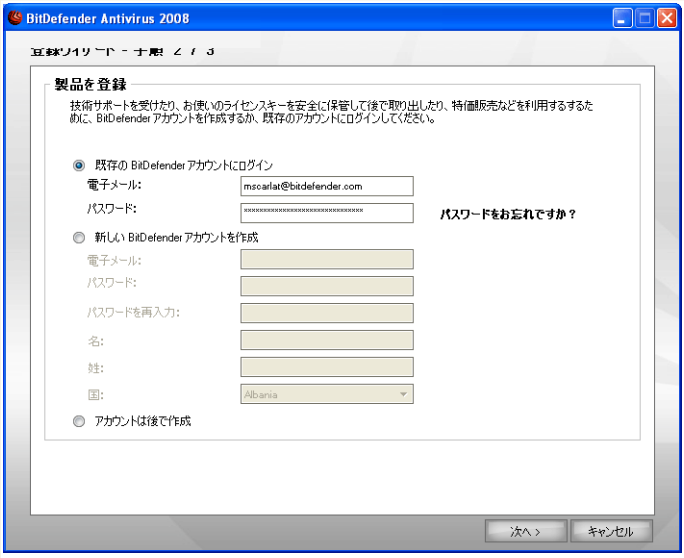
BitDefender ライセンスをお持ちでない場合は、 BitDefender オンラインストアからライセンスキーをご購入ください。

製品を登録 を選択すると、BitDefender アンチウイルス 2008を登録できます。ライセンスキーを新しいキーを入力欄に入力してください。

試用期間が残っており製品の評価を続ける場合、この製品の評価を続けるを選択してください。

次へをクリックしてください。

6.2. 手順2/3 - BitDefenderアカウントを作成



アカウントの作成

BitDefender アカウントを持っていません

BitDefender の無償技術サポートおよび他の無料サービスを受けるには、アカウントが必要です。

注意
アカウントを後日作成される場合は、該当するオプションを選択してください。

新しい BitDefender アカウントを作成を選択し、必要な情報を入力してください。ご入力いただいたデータの機密は守られます。

■電子メール - お使いの電子メールアドレスをご入力ください。

■パスワード - 上で指定したユーザの有効なパスワードを入力してください。

注意
パスワードは、半角英数字で４文字以上にしてください。

■パスワードを再入力 - 上で入力したパスワードを再度入力してください。

■名 - お名前をご入力ください。

■姓 - 苗字をご入力ください。

■国 - お住まいの国名を選択してください。

注意
今入力した電子メールアドレスとパスワードを使用し、http://myaccount.bitdefender.com から皆さんのアカウントにログインしてください。

アカウントを正常に作成するには、まずお使いの電子メールアドレスを有効にしなければなりません。電子メールアドレスを確認し、BitDefender 登録サービスから送られる電子メールの指示に従ってください。

次へをクリックしてください。

すでに BitDefender アカウントを持っています

皆さんが既に BitDefender アカウントを登録されていれば、BitDefender は自動でそのアカウントを検出します。 その場合は、そのまま次へをクリックしてください。

既に有効なアカウントをお持ちで、BitDefender がそれを検出しなかった場合は、既存の BitDefender アカウントにログインを選択し、アカウントの電子メールアドレスとパスワードをご入力ください。

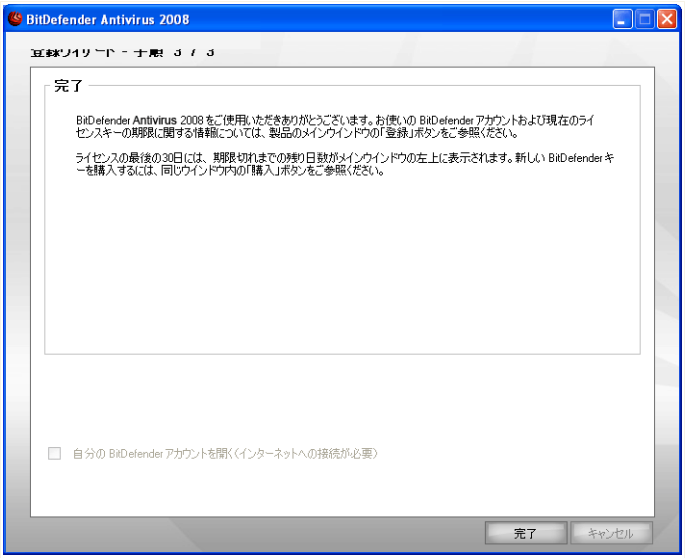
注意

入力したパスワードが誤っていた場合、次へをクリックするとパスワードの再入力を求められます。 Okをクリックしてパスワードを再入力するか、キャンセルをクリックしてウィザードを終了してください。

パスワードを忘れたら、お使いのパスワード忘れた場合？をクリックし、表示をご参照ください。

次へをクリックしてください。

6.3. 手順 3/3 - BitDefender アンチウイルス 2008を登録



概要

自分の BitDefender アカウントを開くを選択し、BitDefender アカウントをご入力ください。これにはインターネット接続が必要です。

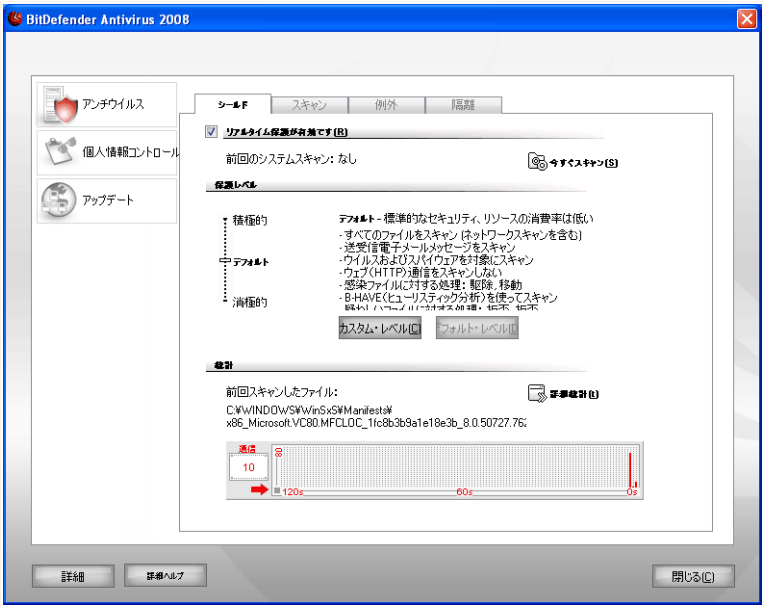
完了をクリックして、ウインドウを閉じてください。

詳細なセキュリティ管理

7. 設定コンソール

BitDefender アンチウイルス 2008には、BitDefender の詳細設定と管理が行える設定コンソールがあります。

設定コンソールを使うには、Security Center の下部にある設定リンクをクリックしてください。



設定コンソール

設定コンソールは、いくつかのモジュールに整理されています：アンチウイルス、個人情報、アップデートです。 これで、指摘されたセキュリティの問題の種類に応じて、BitDefender を簡単に管理できます。

設定コンソールの左側には、モジュールの選択肢が表示されます：

■アンチウイルス - ここからアンチウイルスモジュールを設定できます。

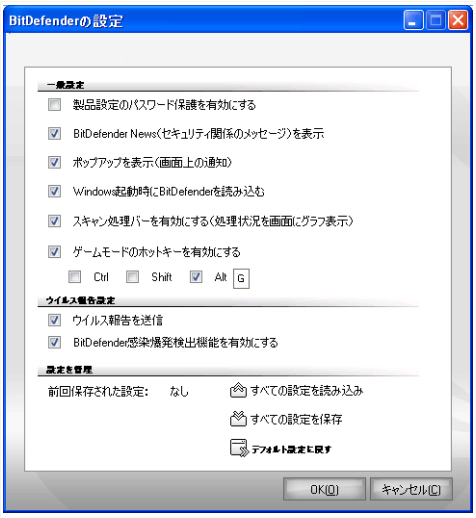
■個人情報 - ここから個人情報コントロールモジュールを設定できます。
■アップデート - ここからアップデートモジュールを設定できます。

画面の下方には、詳細ボタンが表示されます。 表示内容について詳しい情報を参照するには、このボタンをクリックします。

設定コンソールを使うには、Security Center の下部にある設定リンクをクリックしてください。 コンテキストヘルプは表示内容についての詳しい情報をお知らせします。

7.1. 一般設定

BitDefender アンチウイルス 2008の設定を行い、その設定を管理するには、詳細をクリックしてください。 新しいウインドウが開きます。



一般設定

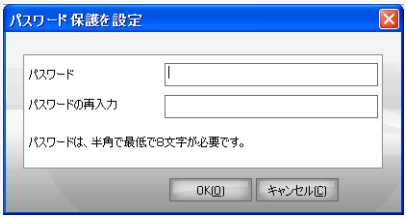
ここで、BitDefender の全体的な動作を設定できます。デフォルトでは、BitDefender は Windows の起動時に読み込まれ、タスクバーに最小化された状態で実行されます。

7.1.1. 一般設定

■製品設定のパスワード保護を有効にする - BitDefender の設定を保護するため、パスワード保護を有効にします。

注意
お客様以外にもこのコンピュータを使う管理者権限を持っているなら、BitDefender 設定をパスワードで保護することをお勧めします。

このオプションを選ぶと、次のウインドウが開きます：



パスワードを入力

パスワードをパスワード欄に入力し、同じパスワードをパスワードを再入力欄に再度入力して、OKをクリックしてください。

パスワードを設定したら、BitDefender の設定を変更しようとするたびにパスワード入力を求められます。 他のシステム管理者（もしいれば）も BitDefender の設定を変更するにはこのパスワードを入力する必要があります。

重要項目
パスワードを忘れたら、BitDefender の設定を変更するために製品の修復が必要です。

■BitDefender News（セキュリティ関連の通知）を表示 - BitDefender サーバが送信する、ウイルスの発生に関するセキュリティ通知を時折表示します。
■ポップアップ（画面上の通知）を表示 - 製品の状態に関するポップアップウインドウを表示します。
■Windows の起動時に BitDefender を読み込む - システム起動時に、自動で BitDefender を起動します。 このオプションを選択しておくことをお勧めします。
■スキャン処理バーを有効にする（処理状況を画面にグラフ表示） - スキャン処理バーを有効/無効にします。 スキャン処理バーを表示させたくない場合はこのチェックボックスのチェックを外してください。

注意
このオプションは、実行中の Windows ユーザアカウントのみで設定可能です。

■ゲームモードのホットキーを有効にする - キーボードのキーの組み合わせ（ホットキー）を使用してゲームモードを有効/無効にできるようにします。 デフォルトのホットキーはAlt+Gです。

ホットキーを変更するには：

1. 使用したいキーを次から選びます：Control キー(Ctrl)、Shift キー(Shift)、Alternate キー(Alt)。
2. 編集欄で、使用したい文字キーに対応する文字を入力します。

7.1.2. ウイルスレポートの設定

■ウイルスレポートを送信 - BitDefender 研究所へ、お使いのコンピュータで見つかったウイルスに関するレポートを送ります。ウイルス発生を監視するために使われます。

レポートにはお客様の氏名、IPアドレスなどの機密情報は含まれず、商用目的には利用されません。提供される情報にはウイルス名だけが含まれ、統計レポートの作成のみに使われます。

■BitDefender 爆発的発生検出機能を有効にする - BitDefender 研究所に、可能性のあるウイルス発生のレポートを送ります。

レポートにはお客様の氏名、IPアドレスなどの機密情報は含まれず、商用目的には利用されません。提供される情報にはウイルスと疑われるファイルだけが含まれ、新しいウイルスの特定にのみ使われます。

7.1.3. 設定を管理

BitDefender で行った設定を希望する場所へ保存あるいは希望する場所から読み込むには、 すべての設定を保存 / すべての設定を読み込みボタンを使用します。これにより、BitDefender 製品を再インストールしたり修復した後でも同じ設定を使うことができます。

重要項目
管理者権限を持つユーザだけが、設定の保存および読み込みを行えます。

デフォルトの設定を読み込むには、デフォルト設定に戻すをクリックしてください。

8. アンチウイルス

BitDefender は、お使いのコンピュータをあらゆる種類のマルウェア（ウイルス、トロイの木馬、スパイウェア、Rootkit など）から保護します。

マルウェアのシグネチャを基にする一般的なスキャンに加え、BitDefender はスキャンしたファイルに対してヒューリスティック分析を行います。ヒューリスティックスキャンの目的は、ウイルス定義ファイルが見つかる前に、特定のパターンとアルゴリズムから新しいウイルスを見つけることです。そのため擬陽性メッセージが表示されるかもしれません。そのようなファイルが検出されると、疑わしいファイルと判断されます。そのような場合、分析のためそのファイルを BitDefender 研究所へ送ってください。

BitDefenderが提供する保護は、２つのカテゴリに分類できます：

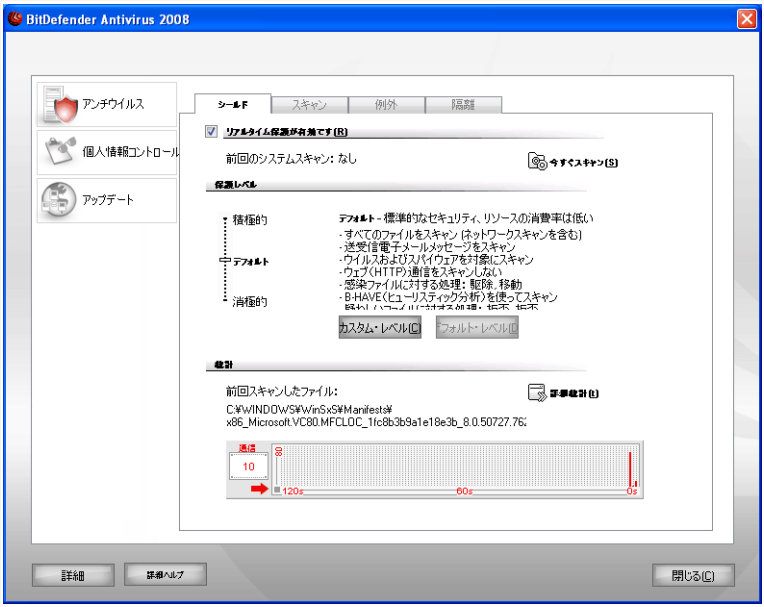
- オンアクセススキャン - お使いのシステムに新しいマルウェアが侵入するのを防ぎます。これは、リアルタイム保護とも呼ばれています - ファイルは使われる際、つまりアクセス時にスキャンされます。 例えば BitDefender は、お客様がWORD書類を開こうとした際に既知の脅威を対象に書類をスキャンし、電子メールなら受け取った際にスキャンします。
- オンデマンドスキャン - お使いのシステムに既に存在しているマルウェアの検出と除去を行います。 これはユーザの要求に応じて実行される従来のスキャン方式です - BitDefender がスキャンするドライブ、フォルダ、ファイルをお客様が指定します - そこでオンデマンドと呼んでいます。 スキャンタスクでは、カスタムスキャンを作成し、定期的に実行するようにスケジュールを組むことができます。

このガイドのアンチウイルスの項には、次のトピックが含まれています：

8.1. オンアクセススキャン

オンアクセススキャンは、すべてのアクセスされるファイル、電子メールメッセージ、インスタントメッセンジャ（ICQ、NetMeeting、Yahoo Messenger、MSN Messenger）経由の通信をスキャンすることでお使いのコンピュータをあらゆるマルウェアの脅威から保護するため、リアルタイム保護とも呼ばれています。

リアルタイム保護を設定し監視するには、設定コンソールのアンチウイルス>シールドをクリックしてください。 次のウインドウが開きます：



リアルタイム保護

重要項目
お使いのコンピュータがウイルスに感染しないように、リアルタイム保護は常に有効にしてください。

画面の下部には、スキャンされたファイルおよび電子メールメッセージに関するリアルタイム保護の統計が表示されます。これらの統計について詳細な情報を記載したウインドウを表示するには、詳細統計をクリックしてください。

クイックシステムスキャンを開始するには、今すぐスキャンをクリックしてください。

8.1.1. 保護レベルを設定

必要なセキュリティに応じて、保護レベルを選択できます。スライダをドラッグして、適切な保護レベルに設定してください。

３つの保護レベルがあります：

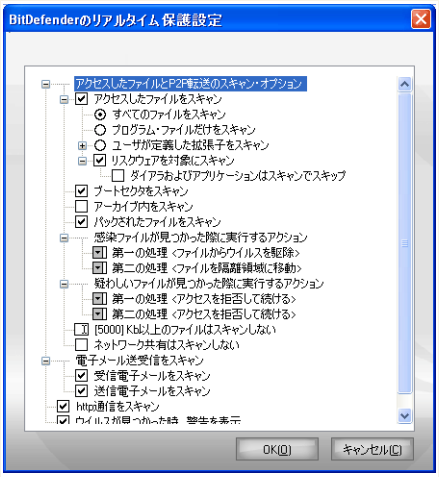
保護レベル	説明
消極的	基本的に必要なセキュリティはカバーします。リソース消費レベルは低いです。 ウイルスを対象にプログラムおよび受信メールメッセージだけスキャンします。従来のシグネチャ方式のスキャンに加え、ヒューリスティック分析も使用されます。感染ファイルに対するアクションは次の通りです：ファイルを感染除去/アクセス拒否。
デフォルト	標準的なセキュリティを提供します。リソース消費レベルは低いです。 すべてのファイルと受信&送信メールメッセージが、ウイルスおよびスパイウェアを対象にスキャンされます。従来のシグネチャ方式のスキャンに加え、ヒューリスティック分析も使用されます。感染ファイルに対するアクションは次の通りです：ファイルを感染除去/アクセス拒否。
積極的	高いセキュリティを提供します。リソース消費レベルは中位です。 すべてのファイルと受信&送信メールメッセージ、ウェブ通信が、ウイルスおよびスパイウェアを対象にスキャンされます。従来のシグネチャ方式のスキャンに加え、ヒューリスティック分析も使用されます。感染ファイルに対するアクションは次の通りです：ファイルを感染除去/アクセス拒否。

デフォルトのリアルタイム保護設定を適用するには、デフォルトレベルをクリックしてください。

8.1.2. カスタム保護レベル

経験豊富なユーザは、BitDefender が提供するスキャン設定をさらに活用したいと思うかもしれません。 スキャナは特定のファイル拡張子だけをスキャンしたり、特定のマルウェアを検索したり、アーカイブを除外したりするように設定できます。これでスキャン時間を減らし、スキャン中のお使いのコンピュータの動作を改善することができます。

リアルタイム保護もカスタムレベルをクリックすれば、カスタマイズできます。次のウインドウが開きます：



シールド設定

スキャンオプションは、Windows でメニューを辿るような、拡張可能なメニューに整理されています。 オプションを開くには "+" のついたボックスをクリックし、オプションを閉じるには "-" のついたボックスをクリックしてください。

注意
"+" 記号がついていても開けないスキャンオプションがあります。これは、それらのオプションがまだ選択されていないからです。選択すれば開けるようになります。

■アクセスされたファイルおよびP2P通信のスキャンオプション - アクセスされたファイルおよびインスタントメッセンジャ（ICQ、NetMeeting、Yahoo Messenger、MSN Messenger）による通信をスキャンします。続いて、スキャンしたいファイル形式を選択してください。

オプション		説明
アクセスされるファイルをスキャン	すべてのファイルをスキャン	ファイル形式に関わらず、すべてのアクセスされるファイルがスキャンされます。
	プログラムファイルのみをスキャン	プログラムファイルだけがスキャンされます。これは、以下の拡張子を持つファイルだけがスキャンされます：.exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml; .nws。
	ユーザが指定した拡張子のみをスキャン	ユーザが指定した拡張子を持つファイルだけがスキャンされます。これらの拡張子は ";" で区切ってください。
	リスクウェアを対象にスキャン	リスクウェアを対象にスキャンします。 検出されたファイルは感染ファイルとして扱われます。このオプションが有効だと、アドウェアコンポーネントを含むソフトウェアは動作しなくなる場合があります。 これらの種類のファイルをスキャン対象から除外するには、ダイアラおよびアプリケー

オプション		説明
		ションをスキャンから除外を選択してください。
起動セクタをスキャン		システムの起動セクタをスキャンします。
アーカイブ内部をスキャン		アクセスされるアーカイブがスキャンされます。このオプションがオンだと、コンピュータの処理速度が遅くなります。
圧縮ファイルをスキャン		すべての圧縮ファイルがスキャンされます。
第一のアクション		感染ファイルあるいは疑わしいファイルに対する第一のアクションをドロップダウンメニューから選択してください。
	アクセスを拒否して続ける	感染ファイルが検出されたら、このファイルへのアクセスは拒否されます。
	ファイルを感染除去	感染したファイルからウイルスを除去します。
	ファイルを削除	警告なしで、感染ファイルを即座に削除します。
	ファイルを隔離領域へ移動	感染ファイルを隔離領域へ移動します。
第二のアクション		第一のアクションが失敗した際に、感染ファイルに対して実行される第二のアクションをドロップダウンメニューから選択してください。
	アクセスを拒否して続ける	感染ファイルが検出されたら、このファイルへのアクセスは拒否されます。
	ファイルを削除	警告なしで、感染ファイルを即座に削除します。
	ファイルを隔離領域へ移動	感染ファイルを隔離領域へ移動します。
サイズが [x] Kb以上のファイルはスキャンしない		スキャンされるファイルの最大サイズを入力してください。サイズが0 Kbだと、サイズに

オプション	説明
	関わらず、すべてのファイルがスキャンされます。
ネットワーク共有をスキャンしない	このオプションが有効だと、ネットワーク接続の速度を向上させるために、BitDefenderはネットワーク共有をスキャンしません。 お使いのネットワークがアンチウイルスソリューションで守られている場合にだけ、このオプションを有効にすることをお勧めします。

■電子メール通信をスキャン - 電子メール通信をスキャンします。

次のオプションが指定できます：

オプション	説明
受信メールをスキャン	すべての受信電子メールメッセージをスキャンします。
送信メールをスキャン	すべての送信電子メールメッセージをスキャンします。

■http 通信をスキャン - http 通信をスキャンします。

■ウイルスが見つかったときに警告を表示 - ファイルあるいは電子メールメッセージ内でウイルスが見つかった際に、警告ウインドウが開きます。

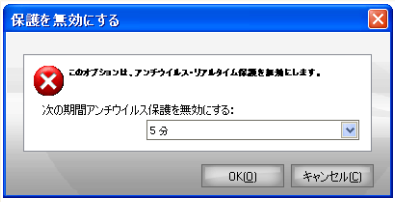
感染ファイルについては、警告ウインドウにウイルス名、そのパス、BitDefenderが実行したアクション、ウイルスに関する詳細情報を確認できる BitDefender サイトへのリンクが表示されます。感染電子メールについては、送信者と宛先の情報も警告ウインドウで表示されます。

疑わしいファイルが検出された場合は、そのファイルを分析するため BitDefender 研究所へ送れるよう、警告ウインドウからウィザードを起動できます。この報告に対する情報を受け取れるよう、お使いの電子メールアドレスも入力できます。

変更を保存してウインドウを閉じるには、OKをクリックしてください。

8.1.3. リアルタイム保護を無効にする

リアルタイム保護を無効にしようとすると、警告ウインドウが開きます。



リアルタイム保護を無効にする

リアルタイム保護を無効にする期間をメニューから選択する必要があります。リアルタイム保護は、5、15、30分間、1時間、永久に、あるいはシステム再起動まで、無効にすることができます。

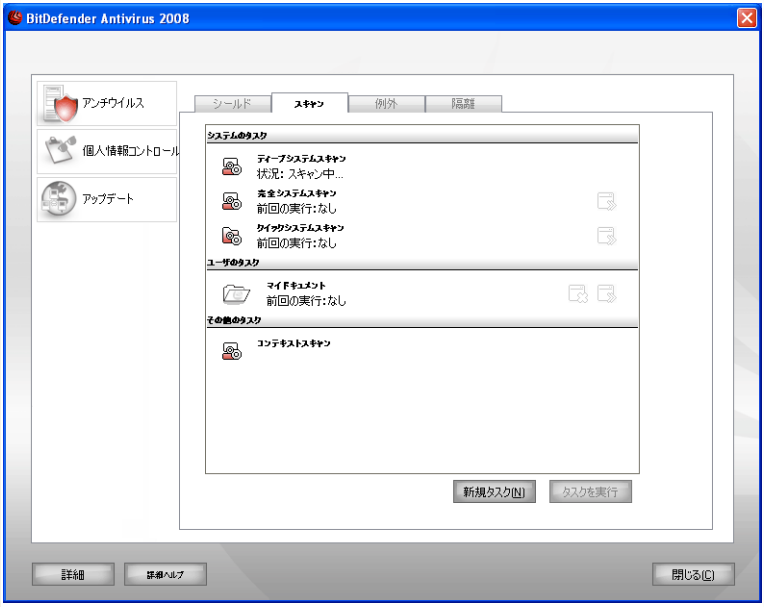
警告
これはセキュリティ上の重要な判断を必要とします。リアルタイム保護を無効にする場合は、できるだけ短期間にすることをお勧めします。リアルタイム保護が無効だと、マルウェアの脅威から保護されません。

8.2. オンデマンドスキャン

BitDefender の主な目的は、お使いのコンピュータをウイルスから守ることです。これはお使いのコンピュータへの新しいウイルスの侵入を防ぎ、お使いの電子メールメッセージや、ダウンロードおよびお使いのシステムへコピーされる新しいファイルをスキャンすることによって実現されます。

BitDefender をインストールいただく前に、お使いのシステムにすでにウイルスが存在している可能性もあります。ですから、BitDefender をインストールしたら、既に存在するウイルスを対象にお使いのコンピュータをスキャンしておくとよいでしょう。また、ウイルスを対象にお使いのコンピュータを頻繁にスキャンするのもよい考えです。

オンデマンドスキャンを設定し、実行するには、設定コンソールのアンチウイルス>スキャンをクリックしてください。 次のウインドウが開きます：



スキャンタスク

オンデマンドスキャンは、スキャンタスクに基づいています。スキャンタスクでは、スキャンオプションおよびスキャンされるオブジェクトを指定します。 デフォルトのタスクあるいは独自のスキャンタスク（ユーザが指定したタスク）を実行することで、いつでもコンピュータをスキャンできます。また、定期的、あるいは作業の邪魔にならないようシステムが使われていないときに実行するよう設定できます。

8.2.1. スキャンタスク

BitDefender には、一般的なセキュリティの問題に対応するため、デフォルトで作成されたいくつかのタスクが用意されています。独自にカスタマイズしたスキャンタスクを作成することもできます。

各タスクには、タスクを設定し、スキャン結果を確認するプロパティウインドウがあります。詳細については、「スキャンタスクを設定」 (p. 60)をご参照ください。

スキャンタスクには３つのカテゴリがあります：

■システムタスク - デフォルトのシステムタスク一覧が用意されています。次のタスクが利用できます：

デフォルトタスク	説明
ディープシステムスキャン	システム全体をスキャンします。 デフォルトの設定では、ウイルス、スパイウェア、アドウェア、Rootkit など、お使いのシステムのセキュリティの脅威となるあらゆる種類のマルウェアをスキャンします。
完全システムスキャン	アーカイブを除く、システム全体をスキャンします。デフォルトの設定では、ウイルス、スパイウェア、アドウェア、Rootkit など、お使いのシステムのセキュリティの脅威となるあらゆる種類のマルウェアをスキャンします。
クイックシステムスキャン	Windows、プログラムファイル、そしてすべてのユーザフォルダをスキャンします。 デフォルトの設定では、Rootkit 以外のすべての種類のマルウェアをスキャンしますが、メモリ、レジストリ、Cookie はスキャンしません。

注意
ディープシステムスキャンおよび完全システムスキャンのタスクは、システム全体を調べるため、スキャン処理には時間がかかります。ですから、これらのタスクは比較的暇なときに実行するか、できればシステムが使われていないときに実行することをお勧めします。

■ユーザタスク - ユーザが指定したタスクを一覧できます。

マイドキュメントという名前のタスクが用意されています。 現在のユーザの重要なフォルダをスキャンする場合は、このタスクを使ってください：マイドキュメント、デスクトップ、スタートアップ。これで、お使いの書類の安全、安全な作業環境、起動されるアプリケーションの安全を確認できます。

■その他のタスク　－　その他のスキャンタスク一覧があります。これらのスキャンは、このウインドウから実行できないその他の種類のスキャンタスクです。設定を変更するほか、スキャンレポートを表示することが可能です。

各タスクの右には３つのボタンがあります：

■ スケジュール　－　選択したタスクに後日実行するためのスケジュールが設定されています。このボタンをクリックすると、プロパティウインドウ、タスクのスケジュールを確認し編集できるスケジューラタブが開きます。
■ 削除　－　選択したタスクを削除します。

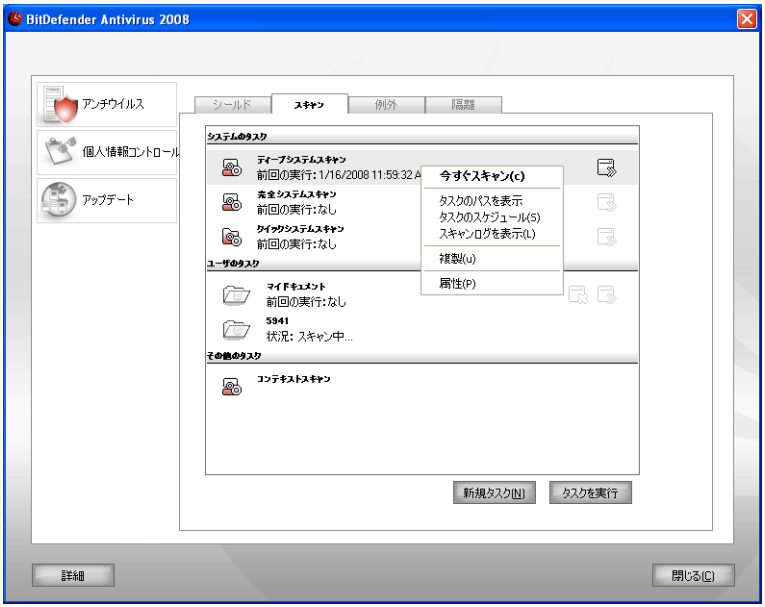
注意
システムタスクには使えません。システムタスクを削除することはできません。

■ 今すぐスキャン－選択したタスクを実行して、即座にスキャンを開始します。

各タスクの左に、タスクを設定し、スキャンログを表示するプロパティボタンがあります。

8.2.2. ショートカットメニューを使う

各タスクには、ショートカットメニューが用意されています。選択したタスクを右クリックすれば開けます。



ショートカットメニュー

ショートカットメニューには、次のコマンドが用意されています：

■今すぐスキャン - 選択したタスクを実行し、即座にスキャンを開始します。
■スキャン対象を変更 - プロパティウインドウ、および選択したタスクのスキャン対象を変更できるスキャンパスタブを開きます。

> **注意**
> システムタスクの場合、スキャン対象を確認することしかできませんので、このオプションはタスクパスを表示に置き換わります。

■タスクスケジュール - プロパティウインドウ、および選択したタスクをスケジュール設定できるスケジュールタブを開きます。
■スキャンログを表示 - プロパティウインドウ、および選択したタスクの実行後のレポートを確認するスキャンログタブを開きます。
■複製 - 選択したタスクを複製します。

注意
これは、複製したタスクの設定を編集できるので、新規タスクを作成する際に便利です。

■削除 – 選択したタスクを削除します。

注意
システムタスクには使えません。システムタスクを削除することはできません。

■プロパティ – プロパティウインドウ、および選択したタスクの設定を変更できる概要タブを開きます。

注意
その他のタスクカテゴリの特殊性により、この場合は、プロパティおよびスキャンログを表示オプションだけが使えます。

8.2.3. スキャンタスクを作成

スキャンタスクを作成するには、次のいずれかの方法を使えます：

■既存のタスクを複製し、名前を変更して、プロパティウインドウで必要な変更を加えてください。
■新規タスクをクリックして新規タスクを作成し、設定を行ってください。

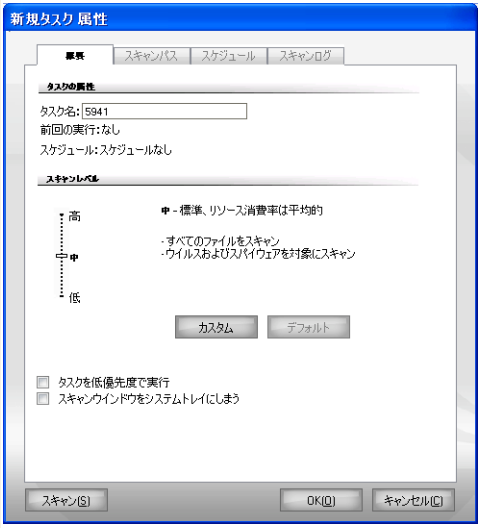
8.2.4. スキャンタスクを設定

各スキャンタスクには、スキャンオプション設定、スキャン対象設定、タスクスケジュール、レポート表示をするためのプロパティウインドウがあります。 このウインドウを開くには、タスクの右に表示される開くボタンをクリックしてください（あるいはタスクを右クリックし、開くをクリックしてください）。

注意
ログの表示およびログタブの詳細については、「スキャンログを表示」（p. 79）をご参照ください。

スキャン設定を行う

特定のスキャンタスクのスキャンオプションを設定するには、右クリックしてプロパティを選択してください。 次のウインドウが開きます：



概要

ここでは、タスクに関する情報（名前、前回の実行、およびスケジュールの状態）を確認し、スキャン設定を設定できます。

スキャンレベルの選択

スキャン設定は、スキャンレベルを選択することで簡単に設定できます。スライダをドラッグして、ご希望のスキャンレベルを設定してください。

３つのスキャンレベルがあります：

保護レベル	説明
低	適度な検出効率を提供します。リソース消費のレベルは低いです。

保護レベル	説明
	プログラムは、ウイルスだけを対象にスキャンされます。従来のシグネチャ方式のスキャンに加え、ヒューリスティック分析も併用されます。
中	良好な検出効率を提供します。リソース消費レベルは中程度です。 すべてのファイルが、ウイルスとスパイウェアを対象にスキャンされます。従来のシグネチャ方式のスキャンに加え、ヒューリスティック分析も併用されます。
高	高い検出効率を提供します。リソース消費レベルは高いです。 すべてのファイルとアーカイブが、ウイルスおよびスパイウェアを対象にスキャンされます。従来のシグネチャ方式のスキャンに加え、ヒューリスティック分析も併用されます。

スキャン処理に関する、一連の一般的なオプションも用意されています：

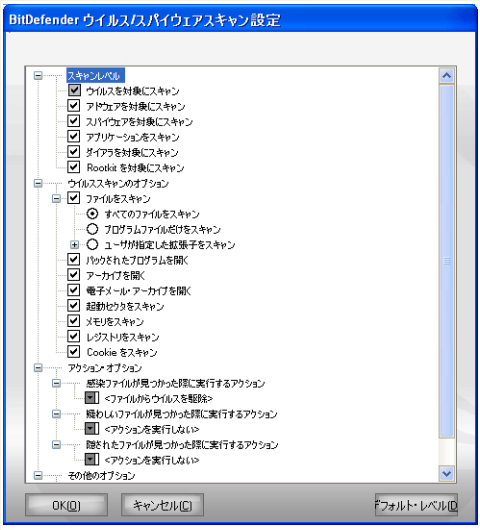
オプション	説明
タスクを低優先度で実行	スキャン処理の優先順位を下げます。他のプログラムがより高速で実行されますが、スキャン処理が完了するまでの時間が長くなります。
スキャンウインドウをシステムトレイにしまう	スキャンウインドウをシステムトレイにしまいます。BitDefender アイコンをダブルクリックすれば開きます。

変更を保存してウインドウを閉じるには、OKをクリックしてください。タスクを実行するには、スキャンをクリックしてください。

スキャンレベルをカスタマイズ

経験豊富なユーザは、BitDefender が提供するスキャン設定をさらに活用したいと思うかもしれません。 スキャナは特定のファイル拡張子だけをスキャンしたり、特定のマルウェアを検索したり、アーカイブを除外したりするように設定できます。これでスキャン時間を減らし、スキャン中のお使いのコンピュータの動作を改善することができます。

独自のスキャンオプションを設定するには、カスタムをクリックしてください。新しいウインドウが開きます。



スキャン設定

スキャンオプションは、Windows でメニューを辿るような、拡張可能なメニューに整理されています。 オプションを開くには "+" のついたボックスをクリックし、オプションを閉じるには "-" のついたボックスをクリックしてください。

スキャンオプションは、４つのカテゴリに分類されています：

■スキャンレベル
■ウイルススキャンのオプション
■アクションオプション
■その他のオプション

■スキャンレベルカテゴリで希望するオプションを選択して、BitDefender にスキャンさせたいマルウェアの種類を指定してください。

次のオプションが指定できます：

オプション	説明
ウイルスを対象にスキャン	既知のウイルスを対象にスキャンします。 BitDefender は不完全なウイルス本体も検出しますので、お使いのシステムのセキュリティに影響する可能性のあるあらゆる脅威を除去できます。
アドウェアを対象にスキャン	アドウェアを対象にスキャンします。検出されたファイルは、感染ファイルとして処理されます。このオプションが有効だと、アドウェアコンポーネントを含むソフトウェアは正常に動作しなくなるかもしれません。
スパイウェアを対象にスキャン	スパイウェアを対象にスキャンします。検出されたファイルは、感染ファイルとして処理されます。
アプリケーションをスキャン	アプリケーション（.exeおよび.dllファイル）をスキャンします。
ダイアラを対象にスキャン	通話料の高額な番号へダイアルするアプリケーションを対象にスキャンします。検出されたファイルは、感染ファイルとして処理されます。このオプションが有効だと、ダイアラコンポーネントを含むソフトウェアは正常に動作しなくなる可能性があります。
Rootkit を対象にスキャン	一般に Rootkit として知られる、隠されたオブジェクト（ファイルおよびプロセス）をスキャンします。

■スキャンするオブジェクトの種類（アーカイブ、電子メールメッセージなど）および他のオプションを指定してください。ウイルススキャンのオプションカテゴリの特定のオプションを選択することで指定できます。

次のオプションが指定できます：

オプション		説明
ファイルをスキャン	すべてのファイルをスキャン	アクセスしようとするすべてのファイルが、その種類に関わらずスキャンされます。
	プログラムファイルのみをスキャン	プログラムファイルだけがスキャンされます。つまり、次の拡張子を持つファイルだけ

オプション		説明
		です：exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml、およびnws。
	ユーザが指定した拡張子のみをスキャン	ユーザが指定した拡張子を持つファイルだけがスキャンされます。これらの拡張子は ";" で区切ってください。
パックされたプログラムを開く		パックされたファイルをスキャンします。
アーカイブを開く		アーカイブの内部をスキャンします。
電子メールアーカイブを開く		メールアーカイブの内部をスキャンします。
起動セクタをスキャン		システムの起動セクタをスキャンします。
メモリをスキャン		ウイルスおよび他のマルウェアを対象に、メモリをスキャンします。
レジストリをスキャン		レジストリ項目をスキャンします。
Cookie をスキャン		Cookie ファイルをスキャンします。

■検出された感染/疑わしい/隠されたファイルに対して実行されるアクションをアクションオプションカテゴリで指定してください。各カテゴリに、異なるアクションを指定できます。

・検出された感染ファイルに対するアクションを選択してください。　次のオプションが指定できます：

アクション	説明
なし（オブジェクトは記録）	感染ファイルに対してアクションは実行されません。これらのファイルは、レポートファイルに記載されます。

アクション	説明
ファイルからウイルスを駆除	感染したファイルからウイルスを除去します。
ファイルを削除	警告なしで、感染ファイルを即座に削除します。
隔離領域へ移動	感染ファイルを隔離領域へ移動します。

- 検出された疑わしいファイルに対するアクションを選択してください。 次のオプションが指定できます：

アクション	説明
なし（オブジェクトは記録）	疑わしいファイルに対してアクションは実行されません。これらのファイルは、レポートファイルに記載されます。
ファイルを削除	警告なしに、疑わしいファイルを即座に削除します。
隔離領域へ移動	疑わしいファイルを隔離領域へ移動します。

注意
ファイルは、ヒューリスティック分析によって疑わしいと判断されます。それらのファイルは、BitDefender 研究所へ送ってください。

- 検出された隠されたオブジェクト（Rootkit）に対するアクションを選択してください。 次のオプションが指定できます：

アクション	説明
なし（オブジェクトは記録）	隠されたファイルに対してアクションは実行されません。これらのファイルは、レポートファイルに記載されます。
隔離領域へ移動	隠されたファイルを隔離領域へ移動します。
可視にする	隠されたファイルを確認できるように可視にします。

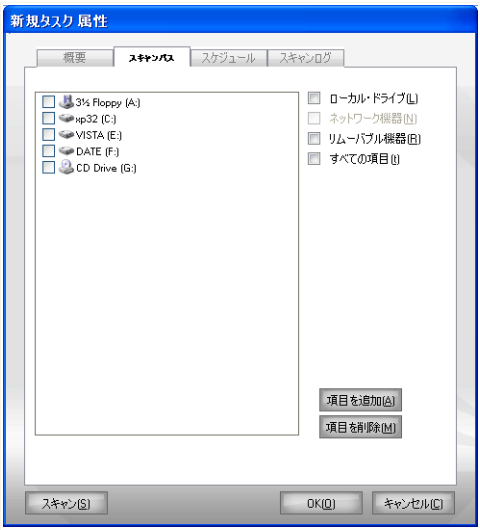
注意
検出されたファイルを無視するように指定するか、選択したアクションが失敗したら、スキャンウィザードでアクションを選択しなければなりません。

■スキャン処理が完了後、すべての疑わしいファイルを BitDefender 研究所へ提出するか確認するには、他のオプションカテゴリにある疑わしいファイルは BitDefender 研究所へ提出をチェックしてください。

デフォルトをクリックすると、デフォルト設定が読み込まれます。 変更を保存してウインドウを閉じるには、OKをクリックしてください。

スキャンの対象を設定

特定のユーザのスキャンタスクのスキャン対象を設定するには、タスクを右クリックし、スキャン対象を変更を選択してください。 次のウインドウが開きます：



スキャンの対象

ローカル、ネットワーク、およびリムーバブルドライブの一覧と、以前追加したファイルかフォルダがあればそれが表示されます。チェックされたすべての項目が、タスク実行時にスキャンされます。

この画面には、次のボタンが表示されます：

■項目を追加 - スキャンしたいファイル/フォルダを選択するファイル閲覧ウインドウが開きます。

注意
ファイル/フォルダをドラッグ&ドロップして一覧に追加することもできます。

■項目を削除 - スキャンされるオブジェクトの一覧から、以前選択したファイル/フォルダを削除します。

注意
削除できるのは後から追加したファイル/フォルダだけで、BitDefender が自動的に"見つけた"ファイルは削除できません。

上記のボタン以外に、スキャン対象場所を素早く選択するいくつかのオプションがあります。

■ローカルドライブ - ローカルドライブをスキャンします。
■ネットワークドライブ - すべてのネットワークドライブをスキャンします。
■リムーバブルドライブ - CD-ROM、フロッピーディスクユニットなどのリムーバブルドライブをスキャンします。
■すべての項目 - ローカル、ネットワーク、リムーバブルに関わらず、すべてのドライブをスキャンします。

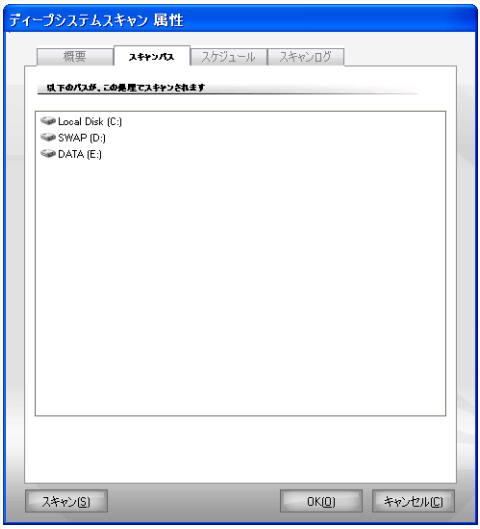
注意
お使いのコンピュータ全体をスキャンするには、すべての項目チェックボックスを選択してください。

変更を保存してウインドウを閉じるには、OKをクリックしてください。タスクを実行するには、スキャンをクリックしてください。

システムタスクのスキャン対象を表示

システムタスクカテゴリのスキャンタスクのスキャン対象は、変更できません。 スキャン対象の確認だけができます。

特定のシステムタスクのスキャン対象を表示するには、タスクを右クリックし、タスクのパスを表示を選択してください。 例えば完全システムスキャンでは、次のウインドウが開きます：



完全システムスキャンのスキャン対象

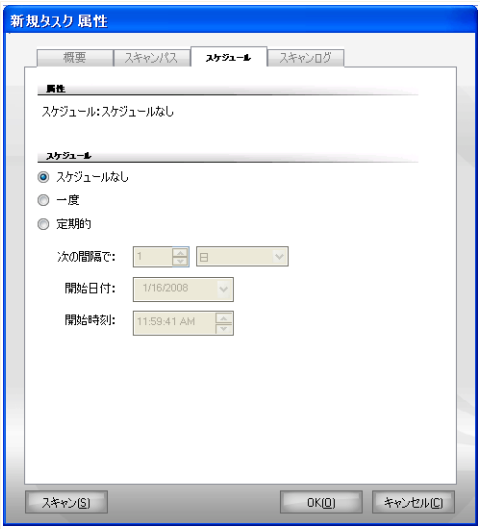
完全システムスキャンおよびディープシステムスキャンはすべてのローカルドライブをスキャンしますが、クイックシステムスキャンではWindowsおよびプログラムファイルフォルダだけをスキャンします。

OKをクリックして、ウインドウを閉じてください。 タスクを実行するには、スキャンをクリックしてください。

スキャンタスクをスケジュール

複雑なタスクの場合、スキャン処理に時間がかかるため、他のプログラムはすべて終了しておいた方が無難です。そのため、そのようなタスクは、お客様がコンピュータを使っておらず、アイドル状態になった際に実行するよう設定するのが理想です。

特定のタスクのスケジュールを表示するか編集するには、タスクを右クリックして、タスクのスケジュールを選んでください。 次のウインドウが開きます：



スケジュール

スケジュール設定されたタスクがあれば、表示されます。

タスクのスケジュールを設定するには、次のオプションのいずれかを選択してください：

- スケジュールなし – ユーザが要求した場合にだけタスクを起動します。
- 一度 – 特定の日時に一度だけスキャンを起動します。開始日付/時刻欄で開始日時を指定してください。
- 定期的 – 指定した日時から、特定の間隔（時間、日、週、月、年）で定期的にスキャンを起動します。

特定の間隔でスキャンを繰り返すには、定期的を選び、次の間隔で：ボックスに、この処理の頻度を表す分／時間／日／週／月／年の数を入力してください。また開始日付/時刻欄で開始日時を指定してください。

変更を保存してウインドウを閉じるには、OKをクリックしてください。タスクを実行するには、スキャンをクリックしてください。

8.2.5. スキャンするオブジェクト

スキャン処理を起動する前に、BitDefender およびそのマルウェアシグネチャが最新であることを確認してください。古いシグネチャデータベースでお使いのコンピュータをスキャンすると、前回のアップデート以降に登場したマルウェアをBitDefender が検出できない可能性があります。前回のアップデート実行日時を確認するには、設定コンソールでアップデート>アップデートをクリックしてください。

注意
BitDefender が完全なスキャンをするには、開かれているすべてのプログラムを終了する必要があります。特に、お使いの電子メールクライアント（例えば、Outlook、Outlook Express、Eudora）を終了することが重要です。

スキャン方式

BitDefender には４種類のオンデマンドスキャンが用意されています：

- 即座にスキャン - システム/ユーザタスクからスキャンタスクを実行します。
- コンテキストスキャン - ファイルあるいはフォルダを右クリックし、BitDefender アンチウイルス 2008を選択してください。
- ドラッグ&ドロップによるスキャン - ファイルあるいはフォルダをスキャン処理バーへドラッグ&ドロップしてください。
- 手動スキャン - BitDefender 手動スキャンを使って、スキャンするファイルあるいはフォルダを直接選択してください。

即座にスキャン

お使いのコンピュータあるいはその一部をスキャンする際、デフォルトのスキャンタスクまたは独自のスキャンタスクを実行できます。 これを「即座にスキャン」と呼びます。

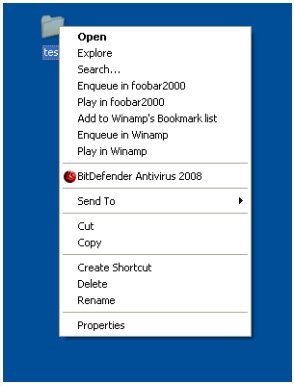
スキャンタスクを実行するには、次の方法のいずれかを使ってください：

■一覧内で希望するスキャンタスクをダブルクリックしてください。
■タスクごとの 今すぐスキャンボタンをクリックしてください。
■タスクを選び、タスクを実行をクリックしてください。

BitDefender スキャナが表示され、スキャンが開始されます。 詳細については、「BitDefender Scanner」 (p. 74)をご参照ください。

コンテキストスキャン

新しいスキャンタスクを作成せずにファイルあるいはフォルダをスキャンするには、コンテキストメニューを使います。 これを「コンテキストスキャン」と呼びます。



コンテキストスキャン

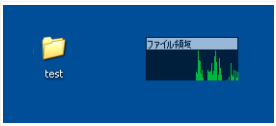
スキャンしたいファイルあるいはフォルダを右クリックし、BitDefender アンチウイルス 2008を選択してください。

BitDefender スキャナが表示され、スキャンが開始されます。 詳細については、「BitDefender Scanner」 (p. 74)をご参照ください。

コンテキストスキャンタスクのプロパティウインドウで、スキャンオプションの編集やレポートファイルを確認できます。

ドラッグ&ドロップスキャン

スキャンしたいファイルあるいはフォルダをスキャン処理バーへ次のようにドラッグ&ドロップしてください。



ファイルをドラッグ

ファイルをドロップ

BitDefender スキャナが表示され、スキャンが開始されます。 詳細については、「BitDefender Scanner」 (p. 74)をご参照ください。

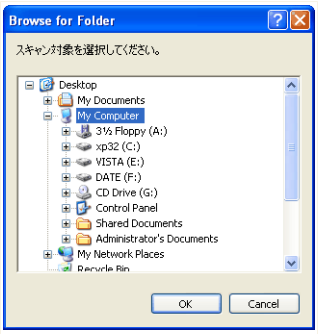
手動スキャン

手動スキャンとは、スタートメニューの BitDefender プログラムグループにある BitDefender 手動スキャンオプションを使って、スキャンするオブジェクトを直接選択することです。

注意
手動スキャンは Windows がセーフモードで実行されていても使えるので便利です。

BitDefender でスキャンするオブジェクトを選択するには、Windows スタートメニューでスタート → プログラム → BitDefender 2008 → BitDefender 手動スキャンのように選択してください。

次のウインドウが開きます：



手動スキャン

スキャンしたいオブジェクトを選び、OKをクリックしてください。

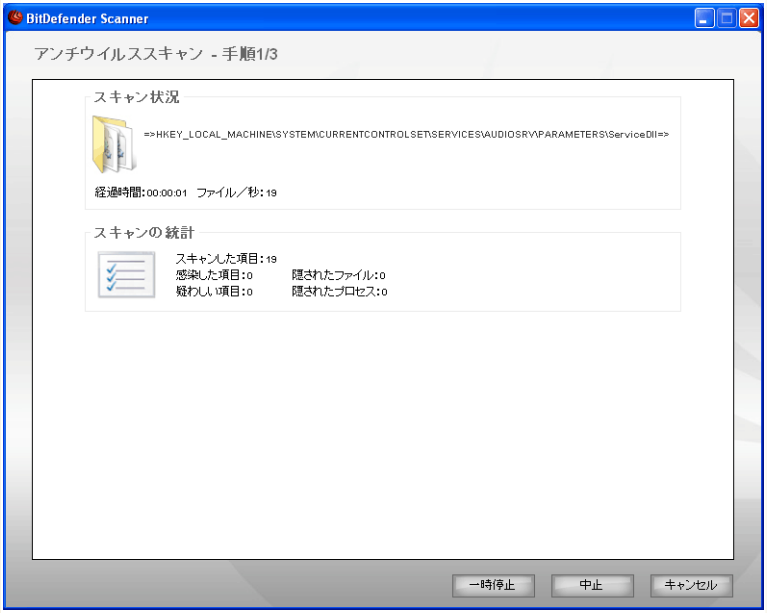
BitDefender スキャナが表示され、スキャンが開始されます。 詳細については、「BitDefender Scanner」 (p. 74)をご参照ください。

BitDefender Scanner

オンデマンドスキャン処理を開始すると、BitDefender スキャナが表示されます。次の３つの手順に従って、スキャン処理を完了させてください。

手順1/3 - スキャン

BitDefenderは、選択したオブジェクトのスキャンを開始します。



スキャン

スキャンの状況および統計（スキャン速度、経過時間、スキャン済み／感染／疑わしい／隠された オブジェクトの数、など）を確認できます。

注意
スキャンの内容によっては、スキャン処理に時間がかかる場合があります。

スキャン処理を一時停止するには、一時停止をクリックしてください。スキャンを再開するには、再開をクリックしてください。

停止&はいをクリックすれば、スキャンをいつでも停止できます。その後、ウィザードの最後の手順に移動します。

BitDefender がスキャンを完了するまでお待ちください。

手順2/3 - アクションを選択

スキャンが完了したら、スキャンの結果を表示するウインドウが新たに開きます。

アクション

お使いのシステムに影響する問題の数を確認できます。

感染したオブジェクトは、感染したマルウェアの数を基にグループ表示されます。感染したオブジェクトについて詳しい情報を参照するには、検出された脅威に対応するリンクをクリックします。

問題のそれぞれのグループごとに一括して実行されるアクションを選ぶか、問題ごとに個別のアクションを指定できます。

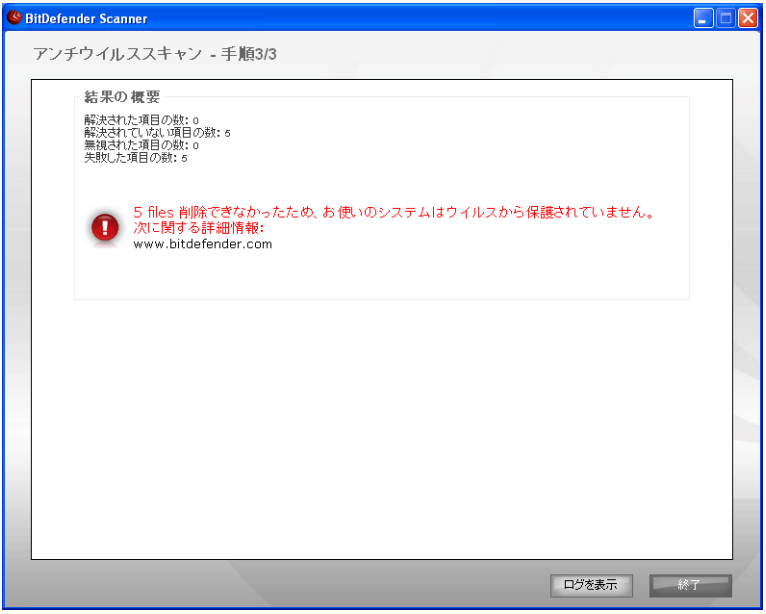
メニューには、次のオプションが表示されます：

アクション	説明
アクションなし	検出したファイルに対して、アクションを実行しません。
ウイルスを除去	感染したファイルからウイルスを除去します。
削除	疑わしいファイルを削除します。
可視にする	隠されたオブジェクトを表示させます。

指定したアクションを適用するには、続けるをクリックしてください。

手順3/3 - 結果を表示

BitDefender が問題の修正を完了したら、スキャンの結果が新しいウインドウに表示されます。



概要

結果の概要を確認できます。 レポートファイルは、対応するタスクのプロパティウインドウにあるログ画面に自動で保存されます。

重要項目
削除処理を完了するため、お使いのシステムを再起動するよう促される場合があります。

終了をクリックして、ウインドウを閉じてください。

BitDefender はいくつかの問題を解決できませんでした

多くの場合、BitDefender は検出した感染ファイルの感染除去、あるいは隔離を正常に行います。 ただし、解決できない問題も存在します。

解決できない問題があれば、www.bitdefender.comの BitDefender サポートチームにご相談ください。 サポート担当者がその問題の解決のお手伝いをします。

BitDefender はパスワード保護された項目を検出しました

パスワード保護された対象には次の２つの種類が含まれています：アーカイブおよびインストーラです。 それらは、感染したファイルを持っていて、さらに実行されない限りは、システムに実際の影響を与えることはありません。

これらの項目が安全であることを確認するには：

- パスワード保護された項目がアーカイブである場合は、ファイルを解凍して、それぞれのファイルをスキャンしてください。 スキャンしたいファイルあるいはフォルダを右クリックし、BitDefender アンチウイルス 2008を選択してください。
- パスワード保護された項目がインストーラである場合は、インストーラ実行前にリアルタイム保護 が有効になっていることをご確認ください。 インストーラが感染している場合、BitDefender は感染を検出し、隔離します。

BitDefender がこれらの対象を再び検出しないようにするには、それらをスキャン処理の例外に追加してください。 スキャンの例外に追加するには、 設定 をクリックして設定コンソールを開き、 アンチウイルス > 例外 と選択してください。 詳しくは、スキャンから除外されるオブジェクトをご参照ください。

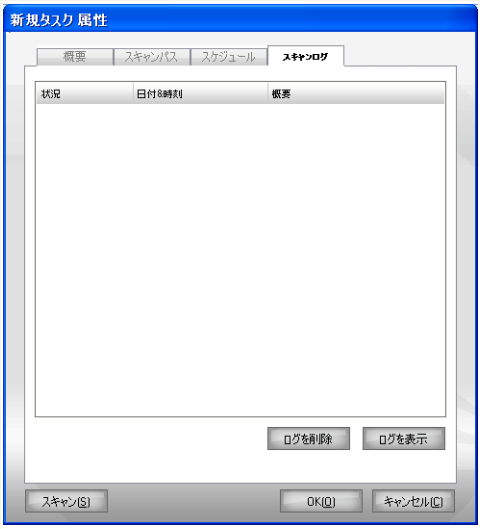
BitDefender は疑わしいファイルを検出しました

疑わしいファイルはヒューリスティック分析によって検出されたファイルであり、まだシグネチャが公開されていないマルウェアに感染している可能性があります。

スキャン中に疑わしいファイルが検出されると、それをBitDefender 研究所へ提出するように促されます。 OK をクリックすると、それらのファイルを BitDefender 研究所に送信します。

8.2.6. スキャンログを表示

タスク実行後にスキャンの結果を表示するには、タスクを右クリックして、スキャンログを表示を選択してください。 次のウインドウが開きます：



スキャンログ

タスクが実行されるたびに生成されるレポートファイルを表示できます。

ファイルごとに、記録されたスキャン処理の状況に関する情報、スキャンが実行された日時、スキャン結果の概要が提供されます。

２つのボタンがあります：

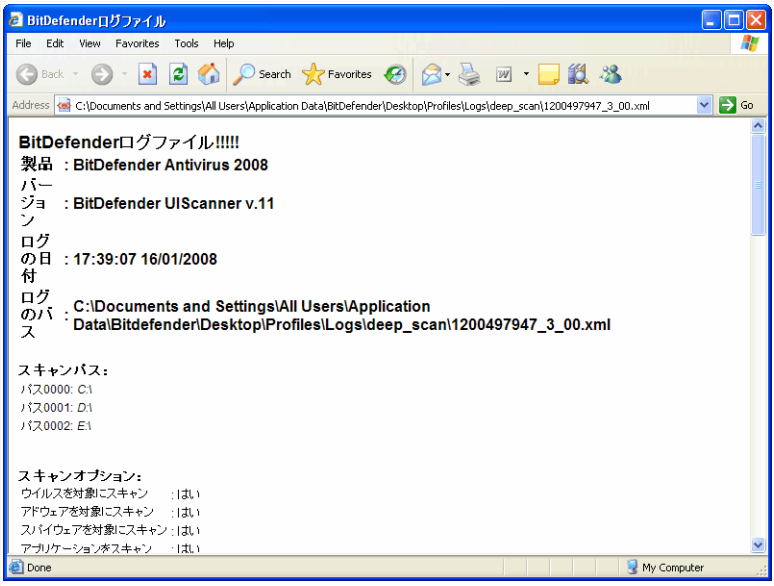
■ログを削除 – 選択したスキャンログを削除します。
■ログを表示 – 選択したスキャンログを表示します。 スキャンログは、お使いのデフォルトウェブブラウザで開かれます。

注意
ファイルを右クリックしてショートカットメニューから対応するオプションを選び、ファイルを表示や削除することもできます。

変更を保存してウインドウを閉じるには、OKをクリックしてください。タスクを実行するには、スキャンをクリックしてください。

スキャンログの例

次の図は、スキャンログの例です：



スキャンログの例

スキャンログには、スキャンオプション、スキャン対象、見つかった脅威、その脅威に対して実行されたアクション、などのスキャン処理の詳細情報が記載されています。

8.3. スキャンから除外されるオブジェクト

特定のファイルをスキャンから除外しなければならない場合があります。例えば、オンアクセススキャンからEICAR試験ファイルを除外したり、オンデマンドスキャンから.aviファイルを除外したいことがあるでしょう。

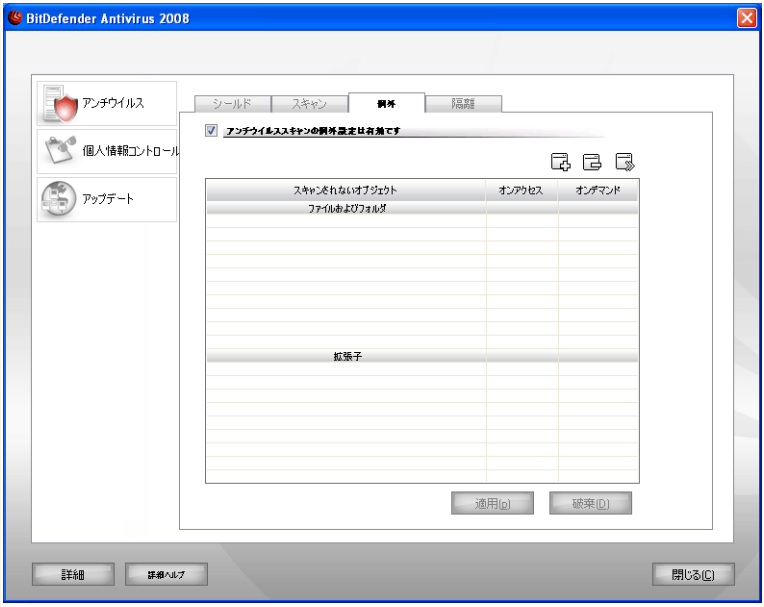
BitDefender では、オンアクセスあるいはオンデマンドスキャン、またはその両方でオブジェクトを除外することができます。この機能は、スキャン時間を減らし、お客様の他の作業への影響を回避することが目的です。

スキャンからは、２種類のオブジェクトが除外できます：

■パス － 指定したパスが示すファイルあるいはフォルダ（その中のすべてのオブジェクトを含む）がスキャンから除外されます。
■拡張子 - 指定した拡張子を持つすべてのファイルがスキャンから除外されます。

注意
オンアクセススキャンから除外されたオブジェクトは、お客様、アプリケーションのどちらによってアクセスされた場合でも、一切スキャンされません。

スキャンから除外されるオブジェクト確認し管理するには、設定コンソールでアンチウイルス>例外をクリックしてください。 次のウインドウが開きます：



例外

スキャンから除外されるオブジェクト（ファイル、フォルダ、拡張子）を確認できます。各オブジェクトについて、オンアクセス、オンデマンド、あるいはその両方で除外されるのか確認できます。

注意
ここで指定された例外は、コンテキストスキャンには適用されません。

表から項目を削除するには、削除ボタンをクリックしてください。

表内の項目を編集するには、対象を選択して、編集ボタンをクリックしてください。 除外される拡張子あるいはパス、それらが除外されるスキャン形式を、必要に応じて変更できる新しいウインドウが開きます。必要な変更を加えたら、OKをクリックしてください。

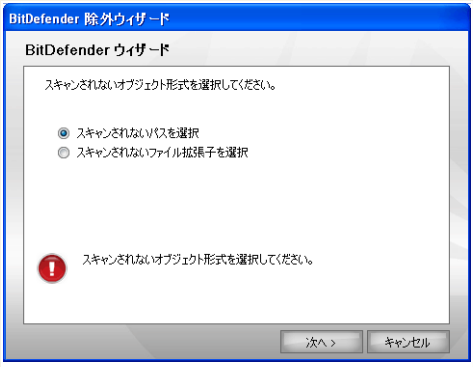
注意
オブジェクトを右クリックし、ショートカットメニューのオプションを選んでも、それを編集したり削除したりできます。

適用をクリックしてルール一覧で行った変更をまだ保存していなければ、破棄をクリックして以前の状態へ戻すことができます。

8.3.1. スキャンからパスを除外

スキャンからパスを除外するには、追加ボタンをクリックしてください。 表示される設定ウィザードにより、手順を追ってスキャンからパスを除外できます。

手順1/3 - オブジェクト形式を選択

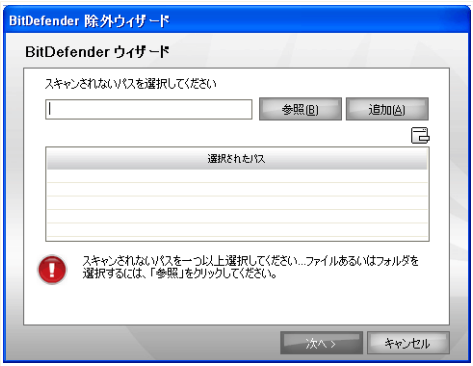


オブジェクト形式

スキャンからパスを除外するオプションを選択してください。

次へをクリックしてください。

手順2/3 - 除外するパスを指定



除外されるパス

スキャンから除外するパスを指定するには、次のいずれの方法を使ってください：

- 参照をクリックし、スキャンから除外したいファイルあるいはフォルダを選択したら、追加をクリックしてください。
- スキャンから除外したいパスを編集欄に入力し、追加をクリックしてください。

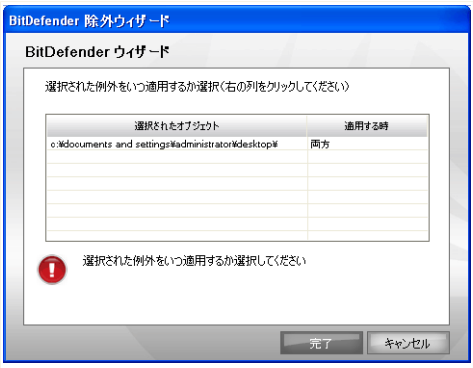
注意
指定したパスが存在しないと、エラーメッセージが表示されます。OKをクリックし、パスが正しいかどうか確認してください。

パスを追加すると、一覧に表示されます。パスは好きな数だけ追加できます。

表から項目を削除するには、削除ボタンをクリックしてください。

次へをクリックしてください。

手順3/3 - スキャン方式を選択



スキャン方式

スキャンから除外されるパス、およびその除外されるスキャン方式が記載された一覧が表示されます。

デフォルトでは、選択されたパスはオンアクセスおよびオンデマンドスキャンの両方から除外されます。除外を適用する対象を変更するには、右の列をクリックし、一覧から希望する対象オプションを選択してください。

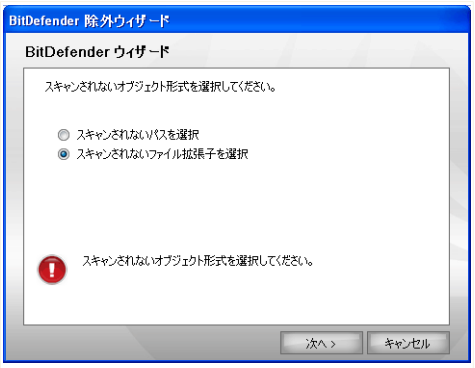
終了をクリックしてください。

適用をクリックして、変更を保存してください。

8.3.2. スキャンから拡張子を除外

スキャンから拡張子を除外するには、 追加ボタンをクリックしてください。 表示される設定ウィザードにより、手順を追ってスキャンから拡張子を除外できます。

手順1/3 - オブジェクト形式を選択

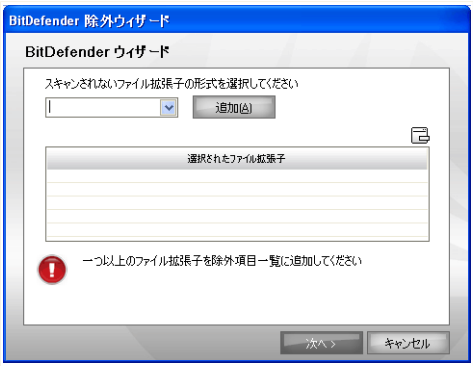


オブジェクト形式

スキャンから拡張子を除外するオプションを選択してください。

次へをクリックしてください。

手順2/3 - 除外される拡張子を指定



除外される拡張子

スキャンから除外される拡張子を指定するには、次のいずれかの方法を使ってください：

■スキャンから除外したい拡張子をメニューから選び、追加をクリックしてください。

注意
メニューには、お使いのシステムに登録されたすべての拡張子が一覧されます。拡張子を選んだ際に、その説明があれば表示されます。

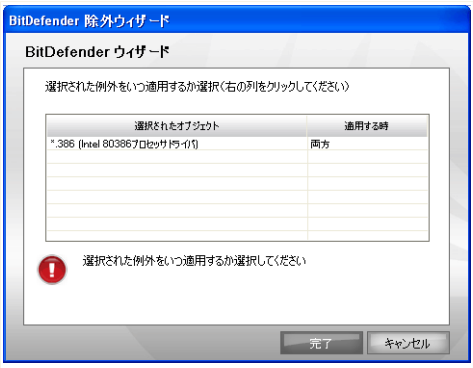
■スキャンから除外したい拡張子を編集欄に入力し、追加をクリックしてください。

拡張子を追加すると、一覧に表示されます。拡張子は、好きな数だけ追加できます。

表から項目を削除するには、削除ボタンをクリックしてください。

次へをクリックしてください。

手順3/3 - スキャン方式を選択



スキャン方式

スキャンから除外される拡張子、およびその除外されるスキャン方式が記載された一覧が表示されます。

デフォルトでは、選択した拡張子はオンアクセスおよびオンデマンドスキャンの両方で除外されます。除外を適用する対象を変更するには、右の列をクリックし、一覧から対象オプションを選択してください。

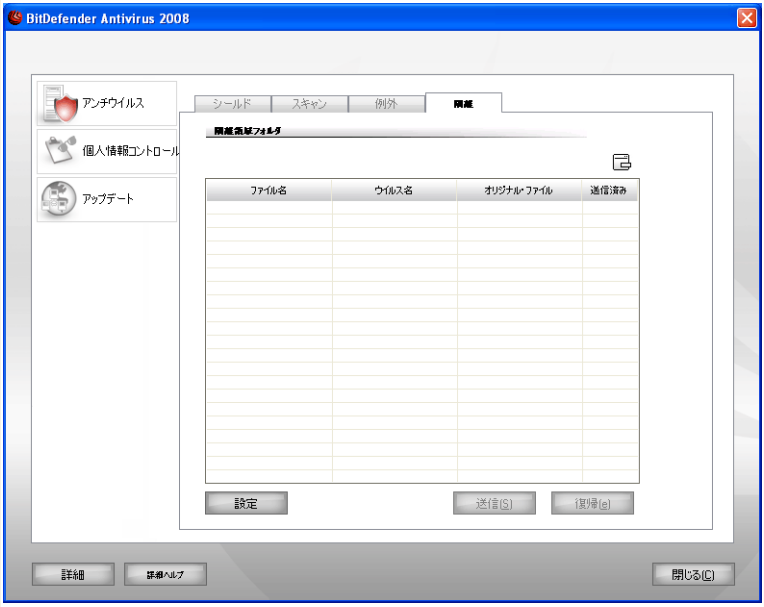
終了をクリックしてください。

適用をクリックして、変更を保存してください。

8.4. 隔離領域

BitDefender では、感染あるいは疑わしいファイルを、隔離領域と呼ぶ安全な場所に隔離することができます。これらのファイルを隔離領域に隔離することで、感染の危険はなくなり、同時にそれらのファイルをさらに分析するために BitDefender 研究所へ送ることが可能となります。

隔離されたファイルの表示と管理、および隔離領域の設定をするには、設定コンソールでアンチウイルス>隔離領域をクリックしてください。



隔離領域

8.4.1. 隔離されたファイルを管理

隔離領域画面には、これまでに隔離されたすべてのファイルの一覧が記載されています。各ファイルには、その名前、検出されたウイルス名、その元の場所へのパス、提出日が表示されます。

注意
ウイルスが隔離領域にあれば、実行したり読み出されたりできないため、悪さをすることはありません。

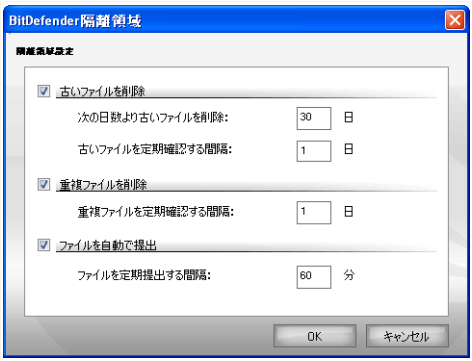
各領域から選択したファイルを削除するには、削除ボタンをクリックしてください。選択したファイルを元の場所へ戻すには、復旧をクリックしてください。

送信をクリックすれば、隔離領域で選択したファイルを BitDefender 研究所へ送ることができます。

コンテキストメニュー. 隔離されたファイルを簡単に管理できるように、コンテキストメニューが用意されています。前出したものと同じオプションが使えます。また更新を選択して、隔離領域がメンを更新することもできます。

8.4.2. 隔離領域設定を構成

隔離領域の設定をするには、設定をクリックしてください。 新しいウインドウが開きます。



隔離領域設定

隔離領域設定を使えば、BitDefender が次のアクションを自動で実行するように設定できます：

古いファイルを削除します。. 古い隔離されたファイルを自動で削除するには、対応するオプションをチェックしてください。 隔離されたファイルを削除するため、経過した日数と、BitDefender が古いファイルを確認する頻度を指定する必要があります。

注意
デフォルトでは、BitDefender は、古いファイルを毎日確認し、10日以上経過したファイルを削除します。

重複ファイルを削除します。. 重複する隔離されたファイルを自動で削除するには、対応するオプションをチェックしてください。 重複ファイルを確認する間隔を日数で指定する必要があります。

注意
デフォルトでは、BitDefender は、重複する隔離されたファイルを毎日確認します。

ファイルを自動で提出します。. 隔離されたファイルを自動で提出するには、対応するオプションをチェックしてください。 ファイルを提出する頻度を指定する必要があります。

注意
デフォルトでは、BitDefender は、隔離されたファイルを60分毎に自動で提出します。

変更を保存してウインドウを閉じるには、OKをクリックしてください。

9. 個人情報コントロール

BitDefender は、お使いのシステム上で、スパイウェアが動作しそうな多くの"ホットスポット"を監視し、お使いのシステムおよびソフトウェアに加えられた変更を確認しています。これはハッカーが、お客様のプライバシーを侵害し、クレジットカード番号などの個人情報をお使いのコンピュータからハッカーへ送出するためにインストールするトロイの木馬および他のツールをブロックするために有効です。

また BitDefender は、お客様が訪問するウェブサイトもスキャンし、フィッシングの脅威が検出されたら警告します。

このユーザガイドの個人情報コントロールの項には、次の内容が記載されています：

■個人情報コントロールの状態
■詳細設定 - 個人識別情報をコントロール
■詳細設定 - レジストリをコントロール
■詳細設定 - Cookieをコントロール
■詳細設定 - スクリプトをコントロール
■システム情報
■アンチフィッシングツールバー

9.1. 個人情報コントロールの状態

個人情報コントロールを設定し、その処理に関連した情報を表示するには、設定コンソールの個人情報>状態をクリックしてください。 次のウインドウが開きます：

個人情報コントロールの状態

9.1.1. 個人情報コントロール

重要項目
データの盗難を防ぎ、お客様のプライバシーを守るために、個人情報コントロールは有効にしておいてください。

個人情報コントロールは、５つの重要なコントロール機能を使ってお使いのコンピュータを守ります：

■個人識別情報をコントロール - すべての発信HTTPおよびSMTP通信を、お客様が個人識別情報画面で作成したルールに従ってフィルタリングすることで、お客様の機密データを保護します。

注意
画面の下には、個人識別情報コントロールの統計が表示されます。

■レジストリをコントロール - プログラムが Windows 起動時に実行できるようにレジストリ項目を変更しようとする度に、お客様の許可を要求します。

■Cookie をコントロール - 新しいウェブサイトが Cookie を設定しようとする度に、お客様の許可を要求します。

■スクリプトをコントロール - ウェブサイトがスクリプトあるいは他のアクティブなコンテンツを実行しようとする度に、お客様の許可を要求します。

これらのコントロールの設定を行うには、詳細設定をクリックしてください。

保護レベルを設定

必要なセキュリティに応じて、保護レベルを選択できます。スライダをドラッグして、適切な保護レベルに設定してください。

３つの保護レベルがあります：

保護レベル	説明
消極的	レジストリをコントロールだけが有効です。
デフォルト	レジストリをコントロールおよび個人識別情報をコントロールが有効です。
積極的	レジストリをコントロール、個人識別情報をコントロール、およびスクリプトをコントロールが有効です。

保護レベルを編集するには、カスタムレベルをクリックしてください。 開かれるウインドウで、有効にしたい保護オプションを選択し、OKをクリックしてください。

スライダの位置をデフォルトのレベルに戻すには、デフォルトレベルをクリックしてください。

9.1.2. アンチフィッシング保護

フィッシングは、ソーシャルエンジニアリングの技術を使い、人々をだまして個人情報を提供させるインターネット上の犯罪行為です。

多くの場合、フィッシングは、立派な、広く認知された企業からと偽った、大量に送信された電子メールメッセージから始まります。こうした詐欺メッセージは、フィッシングのターゲットに合致する受信者の数人だけでいいので、個人情報を漏らしてくれることを期待して送信されます。

フィッシングのメッセージには、通常、お客様のオンラインアカウントに関連した問題が書かれています。そして個人情報を要求する公式なウェブサイト（実際には、偽装サイト）を開かせるためにメッセージ内に記載されたリンクをクリックさせようとします。例えば、ユーザ名やパスワードなどのアカウント情報を確認するよう促して、銀行口座やカード番号を入力させようとします。 場合によっては、念を押すために、お客様のアカウントが既に停止されたか、記載されたリンクを使わなければ停止されると脅します。

フィッシングには、アカウント情報をお使いのコンピュータから直接盗むためにトロイの木馬によるキーロガーなどのスパイウェアが使われることもあります。

フィッシングの主な標的は、eBay および PayPal、あるいはオンラインサービスを提供する銀行など、オンラインの支払いサービスの顧客です。 最近では、成り済ましに使う個人識別データを入手するために、ソーシャルネットワークサイトのユーザが標的となることもあります。

インターネットを閲覧中のフィッシングから身を守るには、アンチフィッシングを有効にしておいてください。 これにより BitDefender は、お客様が各ウェブサイトを表示する前にスキャンし、フィッシングの脅威があれば警告します。 BitDefender にスキャンさせないウェブサイトのホワイトリストを作成することもできます。

Internet Explorer に統合された BitDefender アンチフィッシングツールバーを使って、アンチフィッシング保護およびホワイトリストを簡単に管理することもできます。 詳細については、「アンチフィッシングツールバー」 (p. 112)を参照してください。

9.2. 詳細設定 - 個人識別情報コントロール

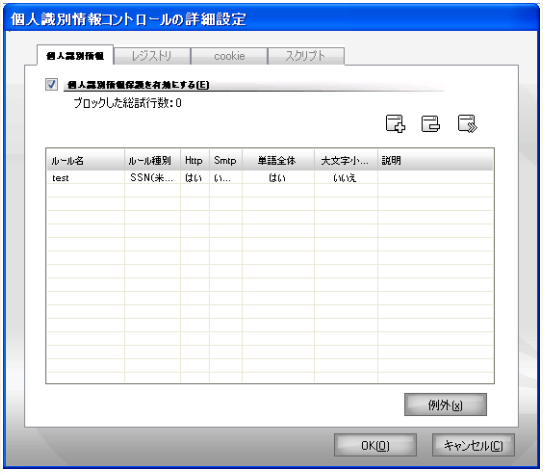
機密データを安全に保管することは、すべての人の関心事です。データの盗難は、インターネットのコミュニティが育つのと同じ早さで増え、人々をだまして個人情報を提供させる新しい技術が次々と登場しています。

個人識別情報コントロールは、機密データの安全な保管を手助けします。HTTPおよびSMTP通信を、お客様が指定した特定の文字列を対象にスキャンします。一致する文字列が見つかると、そのウェブページあるいは電子メールはブロックされます。

システムを使う他のユーザに、お客様が設定したルールを見られないよう、マルチユーザに対応しています。

個人情報ルールは、個人識別情報画面で設定できます。 この画面を呼び出すには、個人情報コントロールの詳細設定 ウインドウを開き、個人識別情報タブをクリックしてください。

注意
個人情報コントロールの詳細設定ウインドウを開くには、設定コンソールの個人情報>状態をクリックし、詳細設定をクリックしてください。



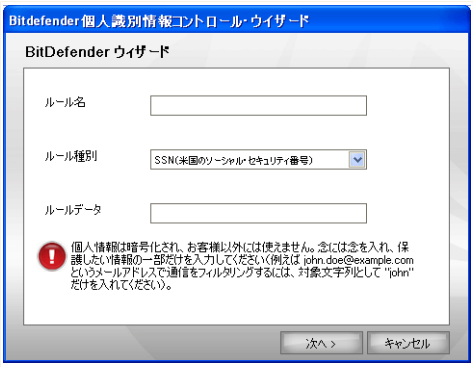
個人識別情報コントロール

9.2.1. 個人識別情報のルール

ルールは、手動で入力する必要があります（追加ボタンをクリックし、ルールの要素を選択してください）。設定ウィザードが表示されます。

設定ウィザードには、３つの手順があります。

手順1/3 - ルールの形式とデータを設定



ルールの形式およびデータを設定

ルール名を編集フィールドに入力してください。

次の内容を設定する必要があります：

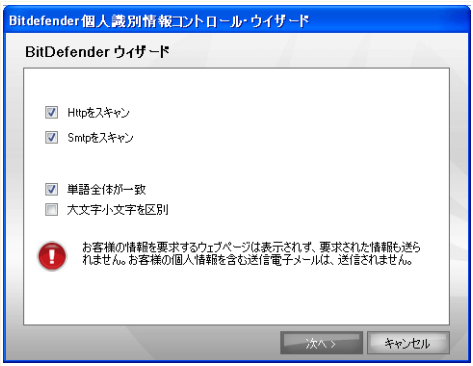
■ルールの形式 - 住所、名前、クレジットカード、PIN（個人識別番号）、社会保障番号、などのルールの形式を選択してください。
■ルールのデータ - ルールのデータを入力してください。

注意
入力した内容が３文字以下だと、データを確認するように促されます。メッセージやウェブページを間違ってブロックしないように、最低でも３文字は入力するようにお勧めします。

入力されたすべてのデータは暗号化されます。さらに安全を図るため、保護したいデータの全体は入力しないでください。

次へをクリックしてください。

手順2/3 - 通信を選択



通信を選択

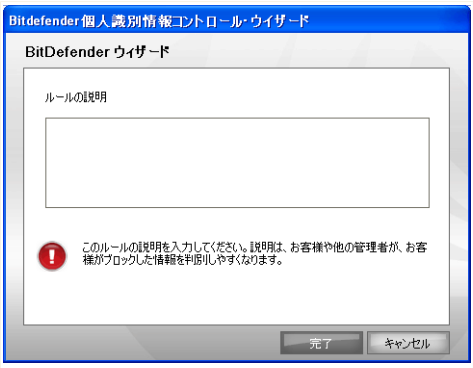
BitDefender にスキャンさせたい通信形式を選択してください。 次のオプションが指定できます：

■HTTPをスキャン - HTTP（ウェブ）通信をスキャンし、ルールのデータと一致する送信データをブロックします。
■SMTPをスキャン - SMTP（メール）通信をスキャンし、ルールのデータと一致する送信電子メールをブロックします。

ルールのデータが単語全体と一致した場合にだけ、あるいはルールのデータと検出された文字列の大文字小文字が一致した場合にだけ、ルールが適用されるように指定できます。

次へをクリックしてください。

手順3/3 - ルールの説明



ルールの説明

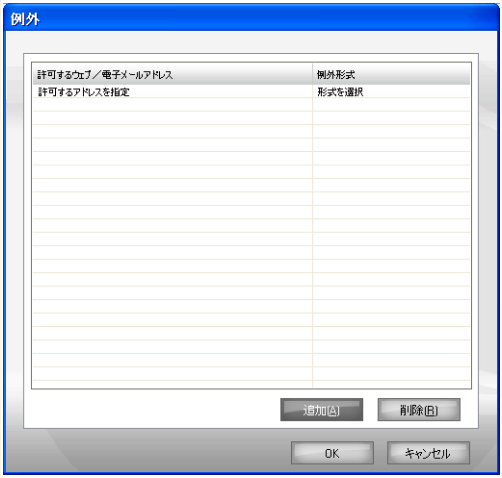
ルールの簡単な説明を編集フィールドに入力してください。

終了をクリックしてください。

9.2.2. 例外を指定

特定の個人識別情報ルールで、例外を指定する必要がある場合があります。 お使いのクレジットカード番号がHTTP（ウェブ）で送信されるのを防ぐルールを作成した場合を考えてみましょう。この場合、お使いのユーザアカウントからクレジットカード番号がウェブサイトへ送信される度に、対象となるページはブロックされます。例えば、安全と分かっているオンラインストアで靴を買おうとするならば、対応するルールに例外として指定しなければなりません。

例外を管理するためのウインドウを開くには、例外をクリックしてください。



例外

例外を追加するには、次の手順を実行してください：

1. 表に新しい項目を追加するために、追加をクリックしてください。
2. 許可するアドレスを指定をダブルクリックし、例外として追加したいウェブアドレスかメールアドレスを入力してください。
3. 形式を選択をダブルクリックし、上で入力したアドレスに対応するオプションをメニューから選択してください。
   ■ウェブアドレスを指定したら、HTTPを選択してください。
   ■電子メールアドレスを指定したら、SMTPを選択してください。

一覧から例外を削除するには、それを選択し、削除をクリックしてください。

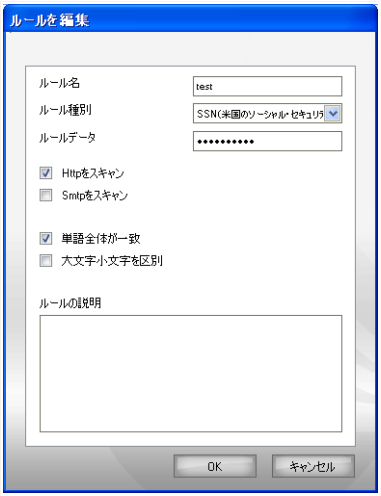
OKをクリックして、変更を保存してください。

9.2.3. ルールを管理

ルール一覧が表に表示されます。

ルールを削除するには、それを選択し、 削除ボタンをクリックしてください。ルールを一時的に無効とするには、対応するチェックボックスのチェックを外してください。

ルールを編集するには、それを選択し、 編集ボタンをクリックするか、それをダブルクリックしてください。新しいウインドウが開きます。



ルールを編集

ここで、ルールの名前、説明、内容（形式、データ、通信）を変更できます。OKをクリックして、変更を保存してください。

変更を保存してウインドウを閉じるには、OKをクリックしてください。

9.3. 詳細設定 - レジストリコントロール

Windows オペレーティングシステムの非常に重要な部分に、レジストリがあります。これは Windows がその設定、インストールされたプログラム、ユーザ情報などを保管する場所です。

レジストリは、Windows起動時にどのプログラムを自動で起動させるか指定するためにも使われます。ウイルスは、ユーザがコンピュータを再起動した際に、自動で起動されるようにレジストリを利用することが多くあります。

レジストリコントロールは、Windows レジストリを監視します - これは、トロイの木馬を検出するために効果的です。この機能は、Windows の起動時に実行されるようにプログラムがレジストリを編集しようとすると、お客様に警告を発します。

レジストリ警告

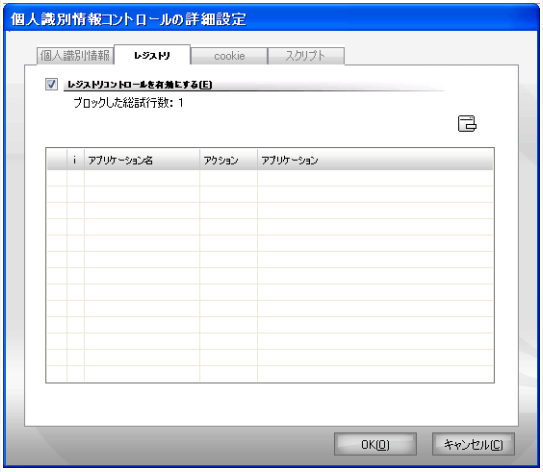
いいえをクリックしてこの変更を拒否するか、はいをクリックして許可することができます。

BitDefender にお客様の設定を覚えさせるには、このプログラムには常にこのアクションを適用にチェックしてください。 このようにルールが作成され、このプログラムが Windows の起動時に起動されるようレジストリ項目を編集しようとすると、同じアクションが適用されます。

注意
お使いのコンピュータの次回の起動後に実行される新しいプログラムがインストールされると、BitDefender は警告します。多くの場合、こうしたプログラムは問題がなく、信頼できるものです。

記憶されたすべてのルールは、レジストリ画面で開いて調整可能です。 この画面を開くには、個人情報コントロールの詳細設定ウインドウを開き、レジストリタブをクリックしてください。

注意
個人情報コントロールの詳細設定ウインドウを開くには、設定コンソールの個人情報>状態をクリックし、詳細設定をクリックしてください。



レジストリコントロール

これまでに作成したルールが表に記載されます。

ルールを削除するには、それを選択し、 削除ボタンをクリックしてください。ルールを削除せずに一時的に無効とするには、対応するチェックボックスのチェックを外してください。

ルールのアクションを変更するには、アクションフィールドをダブルクリックし、メニューから希望するオプションを選択してください。

OKをクリックして、ウインドウを閉じてください。

9.4. 詳細設定 - Cookie コントロール

Cookieは、インターネットでは非常に一般的なものです。お使いのコンピュータに保管される小さなファイルです。こうした Cookie は、お客様に関する特定の情報を記録しておくためにウェブサイトが作成しています。

Cookie は多くの場合、お客様が楽をできるように作成されます。例えば、お客様の名前や参照情報を毎回入力しなくてもいいように、ウェブサイトがそれを記憶するのを助けます。

しかし、Cookie がお客様のウェブ閲覧行動を監視して、プライバシーを暴露するために使われることもあります。

ここでCookie コントロールの出番です。有効になっていると、新しいウェブサイトが Cookie を設定しようとする度に、Cookie コントロールがお客様の許可を求めます。

Cookie 警告

Cookie　を送信しようとしているアプリケーション名を確認できます。

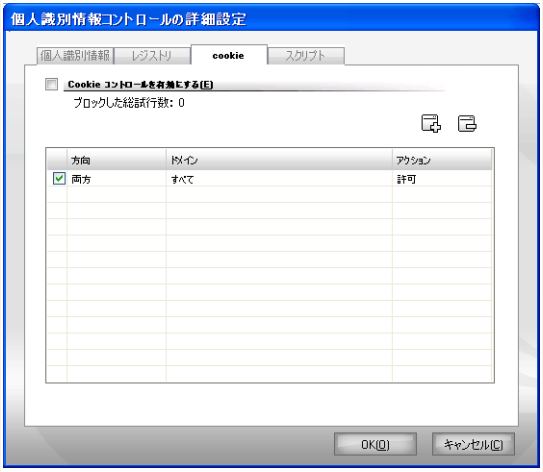
この回答を記憶オプションをチェックし、はい、あるいは、いいえをクリックすれば、ルールが作成され、適用されて、ルール表に記載されます。同じサイトに接続しても、次回から注意を促されることはありません。

これにより、どのウェブサイトを信頼し、どのサイトを信頼しないか選択することができます。

注意
今日のインターネットでは大量の Cookie が使われているので、当初はCookie コントロールが煩わしく感じるかも知れません。最初は、お使いのコンピュータに Cookie を保存しようとするサイトについて多くの質問をします。よく訪問するサイトをルール一覧に追加してしまえば、以前のように楽にサイトの閲覧が楽しめるようになります。

記憶されたすべてのルールは、Cookie画面でさらに調整できます。 この画面を開くには、個人情報コントロールの詳細設定ウインドウを開き、Cookieタブをクリックしてください。

注意
個人情報コントロールの詳細設定ウインドウを開くには、設定コンソールの個人情報>状態をクリックし、詳細設定をクリックしてください。



Cookie コントロール

これまでに作成したルールが表に記載されます。

重要項目
ルールは、上から順番にその優先度に従って並べられます。つまり最初のルールが最も高い優先度を持っています。ルールの優先度を変更するには、ドラッグ&ドロップして順番を入れ替えてください。

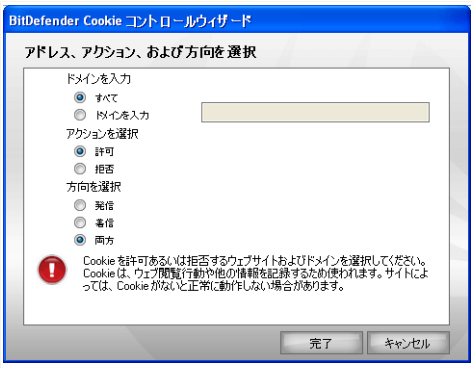
ルールを削除するには、それを選択し、 削除ボタンをクリックしてください。ルールの内容を変更するには、その入力欄をダブルクリックし、必要な変更を加えてください。ルールを削除せず、一時的に無効とするには、対応するチェックボックスのチェックを外してください。

ルールは、警告ウインドウから自動で入力できます。あるいは 追加ボタンをクリックし、ルールの要素を選択すれば手動でも入力できます。すると設定ウィザードが表示されます。

9.4.1. 設定ウィザード

設定ウィザードの手順は１つだけです。

手順1/1 - アドレス、アクション、および方向を選択



アドレス、アクション、および方向を選択

内容を設定できます：

■ドメインアドレス - ルールが適用されるドメインを入力してください。
■アクション - ルールのアクションを選択してください。

アクション	説明
許可	このドメインの Cookie が実行されます。
拒否	このドメインの Cookie は実行されません。

■方向 - 通信方向を選択してください。

形式	説明
送信	ルールは、接続されたサイトに送り返される Cookie にだけ適用されます。
受信	ルールは、接続されたサイトから受け取る Cookie にだけ適用されます。
両方	ルールは、双方向に適用されます。

終了をクリックしてください。

注意
Cookie は受け入れても返信はしない場合、アクションを拒否に、方向を送信に設定してください。

変更を保存してウインドウを閉じるには、OKをクリックしてください。

9.5. 詳細設定 - スクリプトコントロール

スクリプトおよびインタラクティブなウェブページを作成するために使われるActiveXコントロールやJava アプレットのようなコードは、有害な結果を得るためにプログラムすることができます。例えば ActiveX エレメントは、お客様のデータ全体にアクセスでき、お使いのコンピュータからデータを読み出したり、情報を削除したり、パスワードを盗んだり、お客様がオンラインの時にメッセージを横取りしたりできます。アクティブコンテンツは、よく知っていて完全に信用できるサイトからだけ受け入れてください。

BitDefender では、これらのエレメントを実行するか、起動をブロックするか選択できます。

スクリプトコントロールでは、どのウェブサイトを信頼し、どのサイト信頼しないかお客様が決定します。BitDefender は、ウェブサイトがスクリプトや他のアクティブコンテンツを起動しようとする際にお客様の許可を求めます。

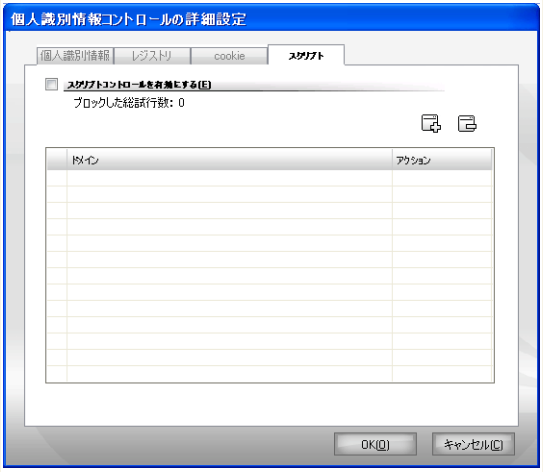
スクリプト警告

リソース名を確認できます。

回答を記憶オプションをチェックして、はいあるいはいいえをクリックすると、ルールが作成、適用され、ルール表示に記載されます。同じサイトがアクティブコンテンツを送ってきても、今後は通知されません。

記憶された各ルールは、スクリプト画面でさらに調整できます。 この画面を開くには、個人情報コントロールの詳細設定ウインドウを開いて、スクリプトタブをクリックしてください。

注意
個人情報コントロールの詳細設定ウインドウを開くには、設定コンソールの個人情報>状態をクリックし、詳細設定をクリックしてください。



スクリプトコントロール

これまでに作成したルールが表に記載されます。

重要項目
ルールは、上から順番にその優先度に従って並べられます。つまり最初のルールが最も高い優先度を持っています。ルールの優先度を変更するには、ドラッグ&ドロップして順番を入れ替えてください。

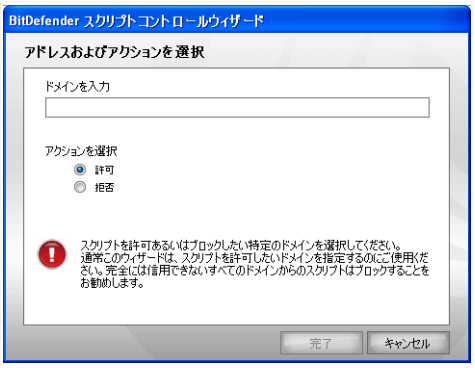
ルールを削除するには、それを選択し、 削除ボタンをクリックしてください。ルールの内容を変更するには、その入力欄をダブルクリックし、必要な変更を加えてください。ルールを削除せず、一時的に無効とするには、対応するチェックボックスのチェックを外してください。

ルールは、警告ウインドウから自動で入力できます。あるいは 追加ボタンをクリックし、ルールの要素を選択すれば手動でも入力できます。すると設定ウィザードが表示されます。

9.5.1. 設定ウィザード

設定ウィザードの手順は１つだけです。

手順1/1 - アドレスおよびアクションを選択



アドレスおよびアクションを選択

内容を設定できます：

■ドメインアドレス - ルールが適用されるドメインを入力してください。
■アクション - ルールのアクションを選択してください。

アクション	説明
許可	そのドメインのスクリプトは、実行されます。
拒否	そのドメインのスクリプトは実行されません。

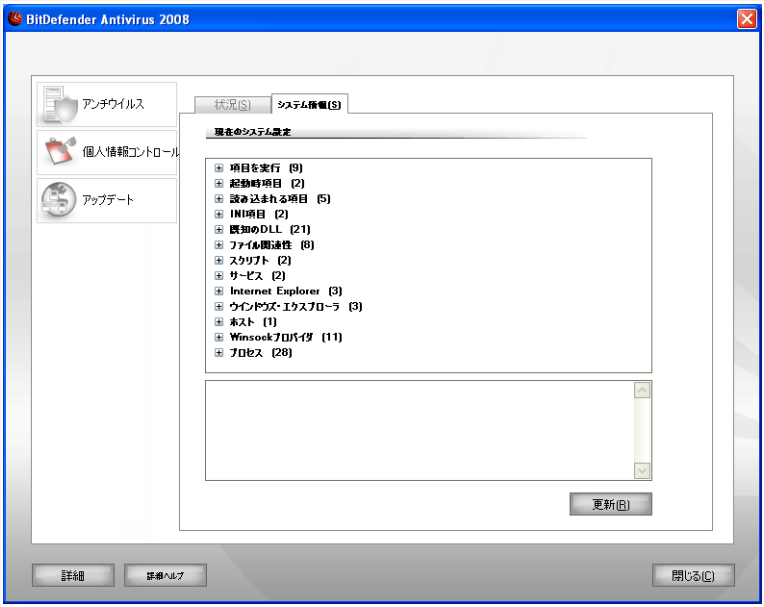
終了をクリックしてください。

変更を保存してウインドウを閉じるには、OKをクリックしてください。

9.6. システム情報

BitDefender では、すべてのシステム設定および起動時に実行するように設定されたアプリケーションを１カ所で確認できます。これにより、システムおよびそこにインストールされたアプリケーションの動作を監視すると同時に、システムの感染の可能性を見つけ出すことができます。

システム情報を取得するには、設定コンソールで個人情報>Sシステム情報をクリックしてください。 次のウインドウが開きます：



システム情報

一覧には、システム起動時に読み込まれるすべての項目に加え、他のアプリケーションが読み込む項目が含まれています。

３つのボタンがあります：

■削除 – 選択した項目を削除します。 選択肢に問題がなければ、はいをクリックしてください。

注意
現在のセッション中に毎回確認されるのが嫌なら、このセッションでは二度と確認しないをチェックしてください。

■表示 – 選択した項目が保管された場所を開きます（例えばレジストリ）。

■更新 - システム情報画面を開き直します。

注意
選択された項目によっては、削除あるいは表示ボタンのいずれか、あるいは両方とも表示されない可能性があります。

9.7. アンチフィッシングツールバー

BitDefender は、お客様がインターネットを閲覧中、フィッシング行為から守ります。 BitDefender は、アクセスするウェブサイトをスキャンし、フィッシングの脅威があれば警告します。 BitDefender にスキャンさせないウェブサイトのホワイトリストを作成することもできます。

Internet Explorer に統合された BitDefender のアンチフィッシングツールバーを使えば、アンチフィッシング保護とホワイトリストを簡単に効率よく管理できます。

BitDefender アイコンで示されるアンチフィッシングツールバーは、Internet Explorer の上部にあります。 ツールバーメニューを開くには、そのアイコンをクリックしてください。

注意
ツールバーが見つからない場合、表示メニューを開き、ツールバーを選択して、BitDefender Toolbarにチェックしてください。

アンチフィッシングツールバー

ツールバーメニューでは、次のコマンドが使えます：

■有効／無効 - BitDefender アンチフィッシングツールバーの有効／無効を切り替えます。

注意
アンチフィッシングツールバーを無効にすると、今後はフィッシング行為から保護されません。

■設定 - アンチフィッシングツールバーの設定を指定するウインドウが開きます。

次のオプションが指定できます：
- スキャンを有効 - アンチフィッシングのスキャンを有効にします。
- ホワイトリストに追加する前に確認 - ウェブサイトをホワイトリストに追加する前にお客様に確認します。

■ホワイトリストに追加 - 現在のウェブサイトをホワイトリストに追加します。

注意
サイトをホワイトリストに追加すると、BitDefender はそのサイトをフィッシング行為を対象にしてスキャンしません。サイトが完全に信用できる場合にのみ、ホワイトリストに追加することをお勧めします。

■ホワイトリストを表示 – ホワイトリストを開きます。

BitDefender のアンチフィッシングエンジンがチェックしないすべてのウェブサイトが一覧表示されます。

そのページにフィッシング脅威があれば警告するように、ホワイトリストから特定のサイトを削除するには、その隣の削除ボタンをクリックしてください。

完全に信用できるサイトは、今後はアンチフィッシングエンジンでスキャンしないよう、ホワイトリストに追加するとよいでしょう。 サイトをホワイトリストに追加するには、対応する入力欄にそのアドレスを入力し、追加をクリックしてください。

■ヘルプ – ヘルプファイルを開きます。

■説明 – BitDefender および何か問題が起きた際の連絡先について情報を確認できるウインドウが開きます。

10. アップデート

毎日新しいマルウェアが生まれ、検出されています。そのため BitDefender を最新のマルウェアのシグネチャで更新することが重要です。

ADSL などのブロードバンドでインターネットに常時接続されていれば、BitDefender が自動でその処理を行います。デフォルトでは、お使いのコンピュータの起動時、およびその後は 1 時間毎にアップデートをチェックします。

アップデートが見つかると、自動アップデート設定画面のオプションの設定内容によって、アップデートの実行について確認するか、自動でアップデートが行われます。

アップデート処理はその場で実行されます。つまりアップデートされるファイルは、順次上書きされていきます。この方法により、アップデート処理は製品の動作に影響せず、同時に脆弱性も除外されます。

アップデートは、次の方法で実行されます：

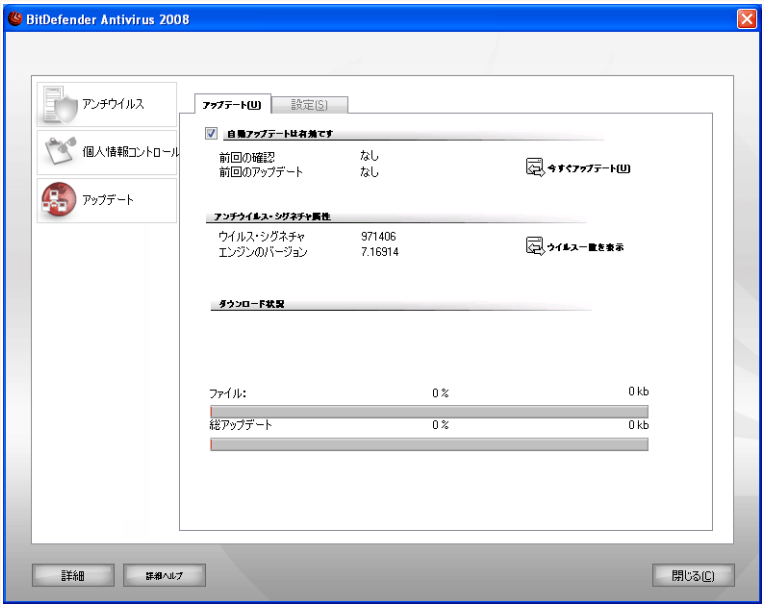
- アンチウイルスエンジン用アップデート - 新しい脅威が現れた際に、今後もそのウイルスから保護するためにはウイルスシグネチャを含むファイルをアップデートしなければなりません。このアップデート形式は、ウイルス定義のアップデートとも呼ばれます。
- アンチスパイウェアエンジン用アップデート - データベースに新しいスパイウェアのシグネチャが追加されます。このアップデート形式は、アンチスパイウェア用アップデートとも呼ばれます。
- 製品アップグレード - 特定の製品の新しいバージョンが公開されると、新しい機能とスキャン技術で製品の機能を向上させることができます。このアップデート形式は、製品アップデートとも呼ばれます。

このユーザガイドのアップデートの項では、次の内容を取り上げます：

- 自動アップデート
- アップデートの設定

10.1. 自動アップデート

アップデート関連の情報を表示し、自動アップデート実行するには、設定コンソールでアップデート>アップデートをクリックしてください。 次のウインドウが開きます：



自動アップデート

アップデートを前回確認した日時およびアップデートが前回実行された日時に加え、前回実行されたアップデートが成功したのか、エラーが起きたのかといった情報が表示されます。お使いのエンジンのバージョンおよびシグネチャの数も表示されます。

ウイルス一覧を表示をクリックすることで、お使いの BitDefender のマルウェアシグネチャを取得できます。使用可能なすべてのシグネチャを記載したHTMLファイルが作成され、ウェブブラウザで開かれます。そのデータベースで特定のマルウェ

アシグネチャを検索したり、BitDefenderのウイルス一覧をクリックしてオンラインの BitDefender シグネチャデータベースを開くこともできます。

アップデート中にこの画面を開くと、ダウンロード状況が表示されます。

重要項目
最新の脅威から保護されるには、自動アップデートを有効にしておいてください。

10.1.1. アップデートを請求

自動アップデートは、今すぐアップデートをクリックすれば、いつでも実行できます。このアップデート形式は、ユーザの請求によるアップデートと呼ばれます。

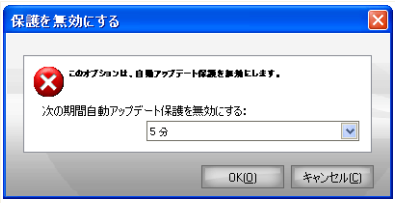
アップデートモジュールは、BitDefender のアップデートサーバに接続し、アップデートがあるかどうか確認します。アップデートが見つかると、手動アップデートの設定画面で指定したオプションに応じて、アップデートの実行を確認するか、自動でアップデートが実行されます。

重要項目
アップデートが完了すると、コンピュータを再起動する必要がある場合があります。できるだけ早く再起動することをお勧めします。

注意
ダイアルアップ接続でインターネットを利用しているなら、BitDefender のアップデートを定期的に行うのがよいでしょう。

10.1.2. 自動アップデートを無効にする

自動アップデートを無効にすると、警告ウインドウが開きます。



自動アップデートを無効にする

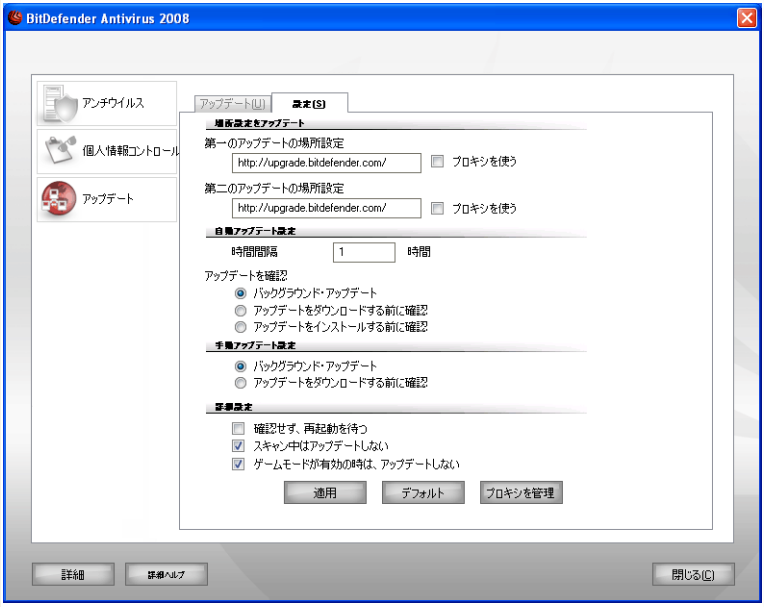
自動アップデートを無効にする期間をメニューから選ぶことで、この選択肢を確定してください。５、15、あるいは30分、１時間、永久、または次のシステム再起動まで、のいずれかの期間自動アップデートを無効にできます。

警告
これは重要なセキュリティの問題を含んでいます。自動アップデートを無効にする期間は、できるだけ短くしてください。BitDefender が定期的にアップデートされないと、お客様を最新の脅威から保護できません。

10.2. アップデート設定

アップデートは、ローカルネットワークから、インターネット経由、直接、あるいはプロキシサーバ経由で実行できます。 デフォルトでは、BitDefenderは１時間毎にアップデートを確認し、お客様に通知することなく、利用可能なアップデートをインストールします。

アップデート設定を行い、プロキシを管理するには、設定コンソールでアップデート>設定をクリックしてください。 次のウインドウが開きます：



アップデート設定

アップデート設定は、４つのカテゴリに分離されています（アップデートの場所の設定、自動アップデート設定、手動アップデートSettings、および詳細設定）。各カテゴリは、個別に解説します。

10.2.1. アップデートの場所を設定

アップデートの場所を設定するには、アップデートの場所の設定カテゴリのオプションを使ってください。

注意
BitDefender のマルウェアシグネチャをローカルで保管しているローカルネットワークに接続しているか、インターネットにプロキシサーバ経由で接続している場合にのみ、これらの設定を行ってください。

さらに安定した高速のアップデートのために、アップデートの場所を２カ所設定できます：第１のアップデートの場所および第２のアップデートの場所です。デフォルトでは、これらの場所は同じです：http://upgrade.bitdefender.com

アップデートの場所のいずれかを変更するには、変更したい場所に対応するURL入力欄に、ローカルミラーのURLを入力してください。

注意
ローカルミラーが使えなくなった場合を想定し、第１のアップデートの場所にはローカルミラーを設定しても、第２のアップデートの場所は変更しないことをお勧めします。

インターネットへの接続にプロキシを使っている企業の場合は、プロキシを使うをチェックし、プロキシを管理をクリックしてプロキシ設定を行ってください。

注意
詳細については、「プロキシを管理」（p. 122）を参照してください。

10.2.2. 自動アップデート設定

BitDefender が自動で実行するアップデート処理を設定するには、自動アップデート設定カテゴリにあるオプションを使ってください。

時間間隔入力欄でアップデートの間隔時間を指定できます。デフォルトでは、アップデートの間隔は１時間に設定されています。

どのように自動アップデート処理が実行されるか指定するには、次のいずれかのオプションを選択してください：

- バックグラウンドアップデート - BitDefender は、アップデートを自動でダウンロードしてインストールします。
- アップデートをダウンロードする前に確認 - アップデートが使用可能になると、それをダウンロードする前にお客様に確認します。

注意
セキュリティセンターを終了しても、アップデートをダウンロードする前には確認されます。

- アップデートをインストールする前に確認 - アップデートがダウンロードされると、それをインストールする前にお客様に確認します。

注意
セキュリティセンターを終了しても、アップデートをインストールする前には確認されます。

10.2.3. 手動アップデート設定

どうやって手動アップデート（ユーザ請求によるアップデート）を実行するか指定するには、手動アップデート設定カテゴリの次のいずれかのオプションを選択してください：

- バックグラウンドアップデート - 手動アップデートが、ユーザを煩わせることなく、バックグラウンドで実行されます。
- アップデートをダウンロードする前に確認 - アップデートが使用可能になると、それをダウンロードする前にお客様に確認します。

注意
セキュリティセンターを終了しても、アップデートをダウンロードする前には確認されます。

10.2.4. 詳細設定

BitDefender のアップデート処理がお客様の作業を邪魔しないようにするには、詳細設定カテゴリのオプションを設定してください：

- 確認せず、再起動を待つ - アップデートが再起動を必要とする場合、システムが再起動するまで製品は古いファイルを使って動作し続けます。ユーザは再起動を促されないので、BitDefender のアップデート処理がユーザの作業の邪魔をすることがありません。
- スキャン中はアップデートしない - スキャン処理の実行中は、BitDefender はアップデートを行いません。これにより、BitDefender のアップデート処理がスキャンタスクの邪魔をすることがありません。

注意
スキャン処理中にBitDefenderがアップデートされると、スキャン処理は中止されます。

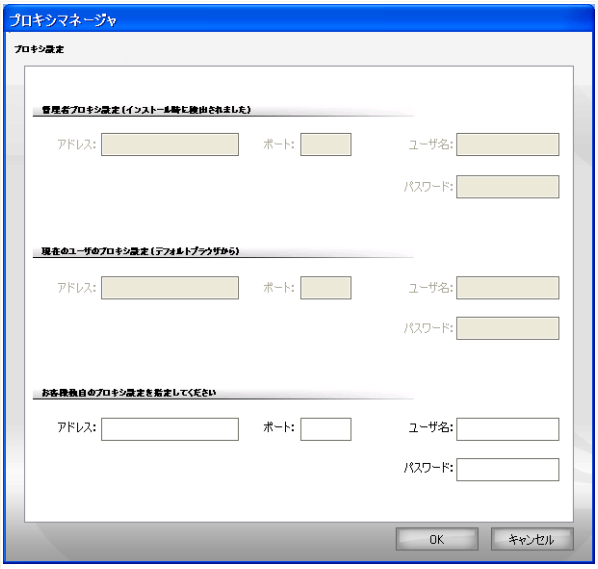
■ゲームモードがオンのときはアップデートしない – ゲームモードがオンだと、BitDefender はアップデートを行いません。 これにより、製品がゲーム中のシステム処理能力に与える影響を最小限にできます。

10.2.5. プロキシを管理

お客様の会社でインターネット接続にプロキシサーバをお使いなら、BitDefender がアップデートできるようにプロキシ設定を指定する必要があります。指定しない場合、製品をインストールした管理者のプロキシ設定か、現在のユーザのデフォルトブラウザのプロキシ設定があればそれを使います。

注意
プロキシ設定は、コンピュータ上で管理者権限を持つユーザか、製品設定のためのパスワードを知っているユーザだけが設定できます。

プロキシ設定を管理するには、プロキシを管理をクリックしてください。プロキシマネージャが開きます。



プロキシマネージャ

プロキシ設定には、３つのセットがあります：

■管理者プロキシ設定（インストール時に検出されます） - インストールの際に管理者アカウントで検出されたプロキシ設定で、お客様がそのアカウントでログインした場合にだけ設定できます。プロキシサーバがユーザ名およびパスワードを必要とする場合は、対応する入力欄に入力してください。
■現在のユーザのプロキシ設定（デフォルトブラウザから） - デフォルトブラウザから流用される、現在のユーザのプロキシ設定です。プロキシサーバがユーザ名およびパスワードを必要とする場合は、対応する入力欄に入力してください。

注意
対応するウェブブラウザは、Internet Explorer、Mozilla Firefox、および Opera です。デフォルトでその他のブラウザを使っている場合、BitDefender が現在のユーザのプロキシ設定を取得することはできません。

■お客様独自のプロキシ設定 - お客様が管理者としてログインしている場合に設定できるプロキシ設定です。

次の設定を指定してください：
- アドレス - プロキシサーバのIPアドレスを入力してください。
- ポート - プロキシサーバへ接続する際に BitDefender が使うポートを入力してください。
- ユーザ名 - プロキシによって認識されるユーザ名を入力してください。
- パスワード - 上で指定したユーザの有効なパスワードを入力してください。

インターネットに接続しようとすると、BitDefender が接続に成功するまで、１度に１つずつ各プロキシ設定が試されます。

インターネットに接続するために、まずお客様独自のプロキシ設定で指定した設定が使われます。失敗すると、次にインストール時に検出されたプロキシ設定が使われます。これらすべてに失敗すると、最後に、デフォルトブラウザから取り出した現在のユーザのプロキシ設定がインターネット接続のために使われます。

変更を保存してウインドウを閉じるには、OKをクリックしてください。

適用をクリックして変更を保存するか、デフォルトをクリックしてデフォルト設定を読み込んでください。

BitDefender Rescue CD

11. 概要

BitDefender Antivirus 2008には、お使いのオペレーティングシステムが起動する前に、すべての既存ハードディスクをスキャンし、ウイルス駆除できる起動用CD（BitDefender Rescue CD）が付いています。

お使いのオペレーティングシステムがウイルス感染のせいで正常に動作していない時は、すぐに BitDefender Rescue CD を使ってください。アンチウイルス製品をインストールしていないとき、そのような状態になる可能性があります。

BitDefender Rescue CD を開始する度に、ユーザを煩わせることなく、ウイルスシグネチャのアップデートが自動で行われます。

BitDefender Rescue CD は、最新の BitDefender for Linux セキュリティソリューションを GNU/Linux Knoppix Live CD に統合した、BitDefender がリマスターした Knoppix ディストリビューションです。既存のハードディスク（Windows NTFS パーティションを含む）をスキャンしてウイルス駆除できるデスクトップアンチウイルス機能を提供します。BitDefender Rescue CD は、お客様が Windows を起動できないときに、お使いの重要なデータを復旧させるためにも使えます。

注意

BitDefender Rescue CD はここからダウンロードできます：http://download.bitdefender.com/rescue_cd/

11.1. システム要項

BitDefender Rescue CD から起動する前に、お使いのシステムが次の必要条件を満たすかご確認ください。

プロセッサ形式
: x86互換、最低166 MHz、ただしこの場合は処理速度は遅くなります。i686世代のプロセッサ、800MHz であれば、それよりは快適な選択となるでしょう。

メモリ
: 最小512 MBのRAMメモリ（１GB推奨）

CD-ROM
: BitDefender Rescue CD は CD-ROM から起動しますので、CD-ROM および CD-ROM からの起動に対応した BIOS が必要となります。

インターネット接続
BitDefender Rescue CD はインターネット接続しなくても実行できますが、プロキシサーバ経由も含め、アップデート処理にはアクティブなHTTPリンクが必要です。そのため最新の保護のためには、インターネット接続が必須です。

グラフィック解像度
標準のSVGA互換グラフィックカードが必要です。

11.2. 同梱されるソフトウェア

BitDefender Rescue CD には、次のソフトウェアパッケージが含まれています。

Xedit
これはテキストファイルエディタです。

Vim
これは構文強調、GUI などの機能を持つ強力なテキストファイルエディタです。詳細については、Vimのホームページを参照してください。

Xcalc
これは計算機です。

RoxFiler
RoxFiler は、高速で強力な、グラフィカルなファイルマネージャです。
詳細については、RoxFiler のホームページをご参照ください。

MidnightCommander
GNU Midnight Commander (mc) は、テキストモードのファイルマネージャです。
詳細については、MC のホームページをご参照ください。

Pstree
Pstree は、実行中のプロセスを表示します。

Top
Top は、Linux タスクを表示します。

Xkill
Xkill は、クライアントをその X リソースで「キル」します。

Partition Image
Partition Image では、パーティションを EXT2、Reiserfs、NTFS、HPFS、FAT16、FAT32ファイルシステム形式のイメージファイルに保存できます。このプログラムは、バックアップに便利です。

詳細については、Partimageのホームページをご参照ください。

GtkRecover
GtkRecover は、GTK版のコンソールプログラムリカバーです。ファイルの復旧に使えます。

詳細については、GtkRecoverのホームページをご参照ください。

ChkRootKit
ChkRootKit は、Rootkit を対象にお使いのコンピュータをスキャンできます。

詳細については、ChkRootKit のホームページをご参照ください。

Nessus Network Scanner
Nessus は、Linux、Solaris、FreeBSD、Mac OS X 用のリモートセキュリティスキャナです。

詳細については、Nessus のホームページをご参照ください。

Iptraf
Iptrafは、IP Network Monitoring Softwareです。

詳細については、Iptraf のホームページをご参照ください。

Iftop
Iftop は、インタフェース上で帯域幅使用状況を表示します。

詳細については、Iftop のホームページをご参照ください。

MTR
MTR は、ネットワーク分析ツールです。

詳細については、MTR のホームページをご参照ください。

PPPStatus
PPPStatus は、受発信されるTCP/IP通信の統計情報を表示します。

詳細については、PPPStatus のホームページをご参照ください。

Wavemon
Wavemon は、ワイヤレスネットワークデバイスの監視アプリケーションです。

詳細については、Wavemon のホームページをご参照ください。

USBView
USBView は、USBバスに接続されているデバイスに関する情報を表示します。

詳細については、USBView のホームページをご参照ください。

Pppconfig
Pppconfig は、ダイアルアップPPP接続を自動設定する手引きをします。

DSL/PPPoe
DSL/PPPoe は、PPPoE (ADSL) 接続を設定します。

I810rotate
I810rotate は、i810ハードウェア上のビデオ出力をi810switch(1)を使って切り替えます。

詳細については、I810rotate のホームページをご参照ください。

Mutt
Mutt は、強力なテキスト方式のMIMEメールクライアントです。

詳細については、Mutt のホームページを参照してください。

Mozilla Firefox
Mozilla Firefox は、広く普及しているウェブブラウザです。

詳細については、Mozilla Firefox のホームページをご参照ください。

Elinks
Elinks は、テキストモードのウェブブラウザです。

詳細については、Elinks のホームページをご参照ください。

12. BitDefender Rescue CD の使い方

この章では、BitDefender Rescue CD の開始および停止方法、マルウェアを対象にお使いのコンピュータをスキャンする方法、感染した Windows PC からデータをリムーバブルデバイスへ保存する方法について説明します。ただし CD に入っているソフトウェアを使うと、このユーザガイドが説明しようとする内容を超えた多くの操作も行えます。

12.1. BitDefender Rescue CD を起動

CD を起動するには、お使いのコンピュータが CD から起動するように BIOS を設定し、CD をドライブに挿入してコンピュータを再起動してください。お使いのコンピュータが、CD からの起動に対応できるか確認しておいてください。

次の画面が表示されるまで待ち、画面上の指示に従って BitDefender Rescue CD を起動してください。

起動画面

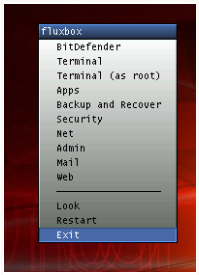
起動時に、ウイルスシグネチャのアップデートが自動で行われます。この処理にしばらくかかります。

起動処理が完了すると、次の画面が表示されます。これで BitDefender Rescue CD が使い始められます。

デスクトップ

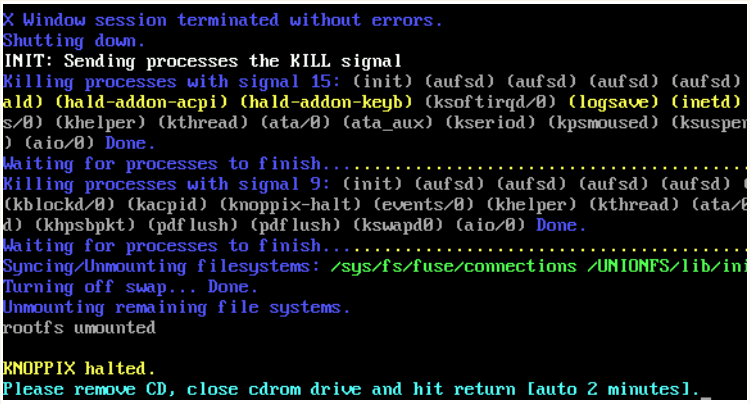
12.2. BitDefender Rescue CD の停止

BitDefender Rescue CD のコンテキストメニュー（右クリックで開きます）からExitを選ぶか、Terminal でhaltコマンドを実行することで、お使いのコンピュータを安全に終了できます。



"EXIT"を選択

BitDefender Rescue CD がすべてのプログラムを正常に終了したら、次のような画面を表示します。お使いのハードディスクから起動するには、CD を取り出してください。これでお使いのコンピュータをシャットダウン、または再起動して構いません。



終了する場合は、このメッセージを待ってください。

12.3. どうやってアンチウイルススキャンを実行するのですか？

起動処理が完了するとウィザードが表示され、お使いのコンピュータ全体をスキャンできます。開始ボタンをクリックするだけです。

注意
お使いの表示解像度が足りないと、テキストモードでスキャンするように促されます。

次の３つの手順に従って、スキャン処理を完了させてください。

1. スキャンの状況および統計（スキャン速度、経過時間、スキャン済み／感染／疑わしい／隠された オブジェクトの数、など）を確認できます。

   注意
   スキャンの内容によっては、スキャン処理に時間がかかる場合があります。

2. お使いのシステムに影響する問題の数を確認できます。

   問題は、グループごとに表示されます。 ″+″ボックスをクリックするとグループが開き、″−″ボックスをクリックするとグループを閉じます。

   問題のそれぞれのグループごとに一括して実行されるアクションを選ぶか、問題ごとに個別のアクションを指定できます。
3. 結果の概要を確認できます。

特定のディレクトリのみをスキャンしたい場合は、次の手順を実行してください：

フォルダを閲覧し、ファイルあるいはフォルダを右クリックしてSend toを選んでください。続いてBitDefender Scannerを選んでください。

あるいはTerminalで、Rootとして次のコマンドを発行してください。選択したファイルあるいはフォルダをデフォルトのスキャン対象としてBitDefender Antivirus Scannerが開始します。

```
# bdscan /path/to/scan/
```

12.4. どうやってプロキシ経由で BitDefender をアップデートするのですか？

お使いのコンピュータとインターネットの間にプロキシサーバがある場合、ウイルスシグネチャをアップデートするための設定を行う必要があります。

プロキシ経由で BitDefender をアップデートするには、次の手順を行ってください：

1. デスクトップを右クリックします。BitDefender Rescue CD のコンテキストメニューが表示されます。
2. Terminal (as root)を選びます。
3. 次のコマンドを入力します：cd /ramdisk/BitDefender-scanner/etc
4. このファイルを GNU Midnight Commander (mc) で編集するために、次のコマンドを入力します：mcedit bdscan.conf
5. 次の行をコメントアウトします：#HttpProxy = (#サインを削除してください) そしてドメイン、ユーザ名、パスワード、プロキシサーバのサーバポートを指定します。例えば、それぞれの行は順番に以下のようになります：

   HttpProxy = myuser:mypassword@proxy.company.com:8080
6. F2を押して現在のファイルを保存します。保存を確認したら、F10を押して閉じます。
7. 次のコマンドを入力します：bdscan update

12.5. データをどうやって保存するのですか？

未知の原因により、お使いの Windows PC を起動できないとします。同時に、お使いのコンピュータ上の重要なデータがどうしても必要だとします。このような状況では、BitDefender Rescue CD が便利です。

コンピュータから USB メモリスティックのようなリムーバブルデバイスにお使いのデータを保存するには、次の手順を実行してください：

1. BitDefender Rescue CD を CD ドライブに挿入し、メモリスティックを USB に挿入し、コンピュータを再起動してください。

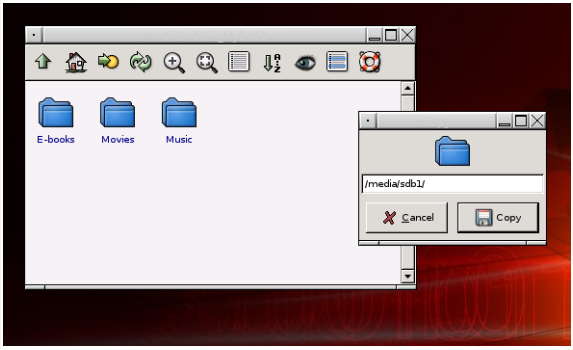
2. BitDefender Rescue CD が起動するのを待ってください。次のウインドウが表示されます。

デスクトップ画面

3. 保存したいデータが保管されたパーティションをダブルクリックしてください（例えば、[sda3]）。

> **注意**
> BitDefender Rescue CD を使用中は、Linux 形式のパーティション名を使います。そのため、おそらく[sda1]は(C:) Windows 形式のパーティションに対応し、[sda3]は(F:)に、[sdb1]はメモリスティックに対応します。

4. フォルダを閲覧し、希望するディレクトリを開きます。例えば、Movies、Music、E-booksというサブディレクトリを持つMyDataです。
5. 希望するディレクトリを右クリックし、Copyを選択してください。次のウインドウが開きます。



データを保存

6. 対応するテキストボックスに/media/sdb1/を入力し、Copyをクリックしてください。

問い合わせ先

13. サポート

BitDefender は、最高の速度と正確さを持つサポートを顧客に提供するように努めています。次のアドレスで連絡可能なサポートセンターは、最新の脅威に対応しています。お客様の問い合わせに対する回答が、迅速に得られます。

BitDefender では、最先端の製品をリーズナブルな価格で提供することで、お客様の時間とお金の節約に寄与することが最優先です。さらに、ビジネスの成功は、良好なコミュニケーションと最高の顧客サポートによって成り立つと信じています。

お客様は、いつでもsupport@bitdefender.comにサポートを依頼できます。迅速に回答できるよう、電子メールにはお使いの BitDefender、お使いのシステムについてできるだけ詳細な情報を書き、経験されている問題について可能な限り正確に説明してください。

13.1. BitDefender Knowledge Base

BitDefender Knowledge Base は、BitDefender 製品に関するオンラインの情報保管庫です。技術サポートの結果報告や、BitDefender サポートおよび開発チームによるバグ修正履歴に加え、ウイルス保護や BitDefender ソリューションの管理方法についての一般的な記事、その他の多くの記事が分かりやすい形式で保管されています。

BitDefender Knowledge Base は一般に開放され、自由に検索できます。その詳細な情報は、BitDefender のお客様に必要な技術的知識と見識を提供する手段でもあります。BitDefender のお客様から受け取る正当な情報の請求やバグレポートは、製品のヘルプを補完するバグ修正レポート、解決のヒント、有益な記事という形で、いつか BitDefender Knowledge Base に追加されます。

BitDefender Knowledge Base は、いつでもhttp://kb.bitdefender.comで参照できます。

13.2. ヘルプを依頼

13.2.1. Web Self Service を開いてください

質問がありますか？我々のセキュリティの専門家は、お客様のために一日24時間、週７日、無料で電話、電子メール、あるいはチャットによるヘルプを提供しています。

次のリンクを参照してください：

English

http://www.bitdefender.com/site/KnowledgeBase/browseProducts/2194/

German

http://www.bitdefender.com/de/KnowledgeBase/browseProducts/2194/

French

http://www.bitdefender.com/fr/KnowledgeBase/browseProducts/2194/

Romanian

http://www.bitdefender.com/ro/KnowledgeBase/browseProducts/2194/

Spanish

http://www.bitdefender.com/es/KnowledgeBase/browseProducts/2194/

13.2.2. サポートチケットを開く

サポートチケットを開き、電子メールでサポートを受けるには、次のいずれかのリンクを使ってください：

English: http://www.bitdefender.com/site/Main/contact/1/
German: http://www.bitdefender.de/site/Main/contact/1/

French: http://www.bitdefender.fr/site/Main/contact/1/
Romanian: http://www.bitdefender.ro/site/Main/contact/1/
Spanish: http://www.bitdefender.es/site/Main/contact/1/

13.3. 連絡先

効率の良いコミュニケーションこそが、ビジネス成功の秘訣です。BITDEFENDER は過去10年間、顧客やパートナーの期待を超えるよりよいコミュニケーションのために常に努力し続けたことで、高い評価を得ています。質問があれば、お気軽にご相談ください。

13.3.1. ウェブアドレス

営業：sales@bitdefender.com
技術サポート：support@bitdefender.com
図書制作：documentation@bitdefender.com
パートナープログラム：partners@bitdefender.com
マーケティング：marketing@bitdefender.com
広報：pr@bitdefender.com
求人：jobs@bitdefender.com
ウイルスの提出：virus_submission@bitdefender.com
迷惑メールの提出：spam_submission@bitdefender.com
悪用の報告：abuse@bitdefender.com
製品のウェブサイト：http://www.bitdefender.com
製品のFTPアーカイブ：ftp://ftp.bitdefender.com/pub
各地の代理店：http://www.bitdefender.com/partner_list
BitDefender Knowledge Base：http://kb.bitdefender.com

13.3.2. 支店

BitDefender の支店は、営業に関するものでも一般的なものでも、その地域での活動に関する問い合わせにいつでも回答いたします。それぞれの所在地と連絡先は次の通りです。

U.S.A

BitDefender, LLC

6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Web: http://www.bitdefender.com
Technical support:

■E-mail: support@bitdefender.com
■Phone:
- 1-888-868-1873 (Registered Users Only; accessible in United States only)
- 1-954-776-6262 (Registered Users Only)

Customer Service:

■E-mail: customerservice@bitdefender.com
■Phone:
- 1-888-868-1873 (Registered Users Only; accessible in United States only)
- 1-954-776-6262 (Registered Users Only)

Germany

BitDefender GmbH
Headquarter Western Europe
Karlsdorferstrasse 56
88069 Tettnang
Germany
Tel: +49 7542 9444 60
ファックス: +49 7542 9444 99
Email: info@bitdefender.com
営業： sales@bitdefender.com
Web: http://www.bitdefender.com
Technical Support: support@bitdefender.com

UK and Ireland

One Victoria Square
Birmingham
B1 1BD
Tel: +44 207 153 9959

ファックス: +44 845 130 5069
Email: info@bitdefender.com
営業： sales@bitdefender.com
Web: http://www.bitdefender.co.uk
技術サポート：support@bitdefender.com

Spain

Constelación Negocial, S.L
C/ Balmes 195, 2a planta, 08006
Barcelona
Soporte técnico: soporte@bitdefender-es.com
Ventas: comercial@bitdefender-es.com
電話： +34 932189615
ファックス: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

Romania

BITDEFENDER
5th Fabrica de Glucoza St.
Bucharest
技術サポート：support@bitdefender.com
営業： sales@bitdefender.com
電話： +40 21 4085600
ファックス: +40 21 2330763
製品のウェブサイト：http://www.bitdefender.com

用語集

ActiveX

ActiveX は、他のプログラムおよびオペレーティングシステムが呼び出すことができるプログラムを開発するためのモデルです。ActiveX 技術は、単に情報を表示するだけでなく、見た目と動作がコンピュータプログラムのようにインタラクティブなウェブページを作成するために、Microsoft Internet Explorer で使用されています。ActiveX では、ユーザは質問や回答、プッシュボタンの使用、といった方法でウェブページと対話することができます。ActiveX コントロールは、多くの場合 Visual Basic で書かれています。

Active X ではセキュリティコントロールが皆無であることに注意してください：コンピュータセキュリティの専門家は、インターネット上では Active X を使わないように勧めています。

アドウェア

アドウェアは、ユーザがアドウェアを受け入れることに同意することで無料で提供されるホストアプリケーションと組み合わせされていることがあります。アドウェアアプリケーションは、アプリケーションの目的を記載したライセンス契約に同意した後でインストールされるのが普通なので、犯罪ではありません。

しかし、ポップアップ広告は煩わしいものであり、場合によってはシステム処理速度を落とします。また、そうしたアプリケーションが収集する情報は、ライセンス契約の条件を完全に理解していないユーザのプライバシの問題を起こす可能性があります。

アーカイブ

バックアップされたファイルを保管するディスク、テープ、あるいはディレクトリです。

１つ以上のファイルを圧縮された状態で保管しているファイルです。

バックドア

設計者あるいは管理者によって、システムに故意に残された抜け穴です。このような抜け穴が、常に悪意に基づくものとは限りません；例えばオペレーティングシステムによっては、フィールドサービス技術者やメーカのメンテ担当プログラマが使うために、最初からそのような特権アカウントが用意されていることもあります。

起動セクター
ディスクの構造（セクターサイズ、クラスターサイズなど）を記録した、各ディスクの開始場所にあたるセクターです。起動ディスクの場合、ブートセクターにはオペレーティングシステムが読み込むプログラムが格納されています。

ブートウイルス
固定ディスク、あるいはフロッピーディスクの起動セクターに感染するウイルスです。起動セクターウイルスに感染したディスケットから起動しようとすると、ウイルスがメモリ内で活動可能となります。お使いのシステムを起動する度に、その時点からウイルスがメモリ内で活動することになります。

ブラウザ
ウェブページを探して表示するソフトウェアアプリケーションであるウェブブラウザの短縮語です。最も著名な２つのブラウザは、Netscape Navigator および Microsoft Internet Explorer です。どちらも文字だけでなく画像も表示できる、グラフィカルブラウザです。さらに最近のブラウザは、各形式に対応したプラグインを使うことで、サウンドやビデオなどのマルチメディア情報も扱えます。

コマンドライン
コマンドラインインタフェースでは、ユーザはコマンド言語を使って画面上に直接コマンドを入力します。

Cookie（クッキー）
インターネットの世界では、Cookie は、お客様のオンライン上での興味や嗜好を知るために広告主が分析、利用する、個々のコンピュータに関する情報を保管した小さなファイルを意味します。その目的は、お客様が興味を持っているものを直接宣伝することですが、Cookie 技術はまだ発展途上でもあります。お客様が興味を持つ広告だけが届くので、ある意味では効率がよく理想的な技術ですが、そのためにお客様が訪問してクリックしたものを"監視"し"記録"もしています。つまり多くの人にとって諸刃の剣と言えます。そのためプライバシーに関する不安もあり、多くの人は"商品登録番号"（レジでスキャンされる商品の背面にあるバーコード番号）のように扱われることに嫌悪感を持っています。このような考え方は極端かもしれませんが、場合によっては正しいものの見方でもあります。

ディスクドライブ
ディスクにデータを読み書きする機械です。

ハードディスクドライブは、ハードディスクを読み書きします。

フロッピードライブは、フロッピーディスクを読み書きします。

ディスクドライブは、内蔵（コンピュータ内に格納）と外接（コンピュータに接続する別のボックスに格納）に分けられます。

ダウンロード
メインのソースから周辺機器へ、データ（通常はファイル全体）をコピーします。この用語は、ファイルをオンラインサービスから自分自身のコンピュータへコピーする処理を指すためによく使われます。ダウンロードは、ネットワーク上のファイルサーバからそのネットワーク上のコンピュータへファイルをコピーする操作を指すこともあります。

電子メール
Eメール（イーメール）とも呼ばれます。ローカルあるいはグローバルのネットワーク経由で、コンピュータ上のメッセージを送信するサービスです。

イベント
プログラムによって検出されたアクションあるいは事象です。イベントは、マウスボタンをクリックしたり、キーを押したりといったユーザ操作またはメモリ不足のようなシステム上の事象です。

擬陽性
スキャナが、実際には感染していないファイルを感染ファイルと特定することです。

ファイル名拡張子
ファイル名の一部で、ピリオドの後ろに続き、ファイル内のデータの種類を表します。

Unix、VMS、MS-DOS といった多くのオペレーティングシステムは、ファイル名拡張子を使っています。通常は、１文字から３文字です（時代遅れのOSでは３文字以上は使えないため）。例えば、"c"はC言語のソースコード、"ps"はPostScript、"txt"はテキストを意味します。

ヒューリスティック
新しいウイルスをルールに基づいて検出する方式です。このスキャン方式は、特定のウイルスシグネチャに依存しません。ヒューリスティックスキャンの利点は、既存のウイルスの亜種を見逃さないことです。しかし、まれに普通のプログラム内の怪しいコードを報告し、"擬陽性"と呼ばれる結果を生み出すこともあります。

IP
Internet Protocol - IPアドレス付与、ルーティング、IPパケットのフラグメンテーションとリアッセンブリを行う、一連のTCP/IPプロトコル内のルータブル・プロトコルです。

Java アプレット
ウェブページ上だけで実行されるように設計された Java プログラムです。ウェブページでアプレットを使うには、アプレットが利用できるアプレットの名前とサイズ（ピクセル単位の長さと幅）を指定します。ウェブページにアクセスすると、ブラウザはサーバからアプレットをダウンロードし、ユーザのマシン（クライアント）上で実行します。アプレットは、厳密なセキュリティプロトコルで管理されている点で、アプリケーションと異なります。

例えば、アプレットはクライアント上で実行しますが、クライアントのマシンにデータを読み書きすることはできません。さらにアプレットは、提供元と同じドメインからしかデータの読み書きはできません。

マクロウイルス
書類に埋め込まれたマクロとして作成されたコンピュータウイルスです。Microsoft Word や Excel のような多くのアプリケーションが、強力なマクロ言語を採用しています。

こうしたアプリケーションでは、ユーザが書類内にマクロを埋め込んで、書類が開く度にマクロを実行させることができます。

メールクライアント
電子メールクライアントは、電子メールを送受信するためのアプリケーションです。

メモリ
コンピュータ内の記憶領域です。メモリという用語は、チップの状態のデータ記憶媒体を指し、テープやディスク上の記憶領域はストレージなどと呼ばれます。すべてのコンピュータは、メインメモリあるいはRAMと呼ばれるある程度の容量の物理的メモリを搭載しています。

非ヒューリスティック
このスキャン方式は、特定のウイルスシグネチャに依存しています。非ヒューリスティックなスキャンの利点は、ウイルスに見えるファイルを間違えないため、擬陽性警告を生成しないことです。

パックされたプログラム
圧縮形式のファイルです。多くのオペレーティングシステムおよびアプリケーションは、ファイルサイズを小さくするためにファイルをパックする機能を持っています。例えば、10個の連続するスペース記号を持つテキストファイルがあるとすると、通常、このファイルは10バイトの容量を消費します。

しかしファイルをパックするプログラムは、このスペース記号を、対象とするスペースの数に特別な連続スペースを意味する文字を付けて置き換えます。この場合、10個のスペースが消費するのは２バイトだけとなります。これはパック技術の１例で、世の中には多くの技術が存在します。

パス
コンピュータ上のファイルの正確な場所を示します。通常、階層ファイルシステムを上から辿った形式で表されます。

２台のコンピュータ間の通信チャンネルのような、２点間をつなぐルートです。

フィッシング
著名で正当な企業のふりをして、ユーザに個人情報を明け渡させようとする詐欺メールを送る行為です。こうした電子メールでは、本来の企業が既に情報を持っているパスワードやクレジットカード番号、社会保障番号、および銀行口座番号などの個人情報を更新するように促すウェブサイトへユーザを誘導します。しかし、そのウェブサイトは偽で、ユーザの情報を盗む目的のためだけに設置されたものです。

多形性ウイルス
感染するファイル毎にその形式を変化させるウイルスです。一貫したバイナリパターンを持たないため、このようなウイルスを特定するのは困難です。

ポート
デバイスを接続するためのコンピュータ上のインタフェースです。パーソナルコンピュータには、様々な種類のポートがあります。内部には、ディスクドライブ、ディスプレイスクリーン、そしてキーボードを接続するいくつかのポートがあります。外部には、モデム、プリンタ、マウス、そして他の周辺機器を接続するポートも持っています。

TCP/IPおよびUDPネットワークでは、論理接続の終端を指します。ポート番号は、そのポートの種類を表します。例えば、ポート80はHTTP通信用です。

レポートファイル
起きたアクションを一覧したファイルです。BitDefender は、スキャンしたパス、スキャンしたフォルダとアーカイブとファイルの数、見つかった感染ファイルと疑わしいファイルの数、などを一覧するレポートファイルを常時生成しています。

Rootkit
Rootkit は、システムへの管理者レベルのアクセスを実現する一連のソフトウェアツールです。この用語が初めて使われたのはUNIXオペレーティングシステムです。侵入者がその存在を隠し、システム管理者に見つからないように、侵入者に管理者権限を与えるリコンパイルされたツールを意味します。

Rootkit の主な役割は、プロセス、ファイル、ログインおよびログを隠すことです。また、適当なソフトウェアと組み合わせることで、ターミナル、ネットワーク接続、あるいは周辺機器からのデータを横取りすることもできます。

Rootkitは、それ自体が悪ということではありません。例えば、システムやアプリケーションによっては Rootkit を使って重要なファイルを隠します。しかし多くの場合、マルウェアを隠すか、システムへの侵入者の存在を秘密にするために使われます。マルウェアと組み合わされると、Rootkit はシステムの整合性とセキュリティに多大な脅威となります。通信を監視したり、システムへのバックドアを作成したり、ファイルやログを編集したりして発見を避けます。

スクリプト
マクロあるいはバッチファイルの別名です。スクリプトは、コマンドを列記したもので、ユーザの操作なしで実行されます。

迷惑メール
電子的なゴミメールあるいはニューズグループへのゴミ投稿です。一般に、すべての未承諾の電子メールを指します。

スパイウェア
多くの場合、広告宣伝の目的で、ユーザが知らない内に、ユーザのインターネット接続を介してユーザ情報を密かに集めるソフトウェアです。通常のスパイウェアアプリケーションは、インターネットからダウンロードできるフリーウェアやシェアウェアの一部に組み込まれて隠されています。ただし多くのフリーウェアやシェアウェアには、スパイウェアは含まれていません。インストールされると、スパイウェアはインターネット上でのユーザの行動を監視し、その情報を第三者にバックグラウンドで送信します。スパイウェアは、電子メールアド

レスに加え、パスワードやクレジットカード番号などの情報を収集することもできます。

スパイウェアは、ユーザが何かをインストールする時、知らずにその製品をインストールしてしまうという点で、トロイの木馬に似ています。最近使われているピアツーピアでファイル交換する製品をダウンロードすることで、スパイウェアの犠牲者になるケースがよくあります。

倫理およびプライバシの問題以外にも、スパイウェアがコンピュータのメモリリソースを使ってユーザから盗みを働き、ユーザのインターネット接続を使ってスパイウェアの作者へ情報を送り返すために帯域幅を消費するという問題があります。スパイウェアはメモリおよびシステムリソースを使うため、バックグラウンドで動作しているそのアプリケーションがシステムをクラッシュさせたり、システム全般を不安定にします。

起動項目
: このフォルダに保管されたファイルは、コンピュータの起動時に開かれます。例えば、起動画面、コンピュータが初めて起動した際に再生されるサウンドファイル、カレンダの通知、あるいはアプリケーションプログラムが起動項目として使えます。通常、このフォルダには、ファイルそのものでなく、ファイルのエイリアスを保存しておきます。

システムトレイ
: Windows 95 で登場したシステムトレイは、Windows タスクバー（通常下部の時計の隣）にあり、ファックス、プリンタ、モデム、音量、などのシステム機能を簡単に呼び出すための小さなアイコンが表示されます。アイコンをダブルクリックするか右クリックして、その詳細を表示したり機能を利用したりできます。

TCP/IP
: Transmission Control Protocol/Internet Protocol - 様々なハードウェアやオペレーティングシステムを使う互いに接続されたコンピュータ間での通信を行うために、インターネットで広く使われている一連のネットワークプロトコルです。TCP/IPには、コンピュータがどのように通信するかを決めた標準仕様、およびネットワークを接続して通信をルーティングするための方式が含まれています。

トロイの木馬
: 悪意のないアプリケーションのふりをした破壊的なプログラムです。ウイルスと違い、トロイの木馬は自身を複製しませんが、同様に被害を及ぼします。最

も油断のできないトロイの木馬は、お使いのコンピュータのウイルスを駆除すると称しておきながら、実際にはお使いのコンピュータにウイルスを移植する種類のものです。

この用語は、ギリシャが一見贈り物のような巨大な木馬を敵であるトロイに差し出す、ホメロスのイリアッドというストーリーから来ています。しかしトロイが木馬を城壁内に引き入れると、その空洞の腹からギリシャの兵士が忍び出て、ゲートを開いて仲間を侵入させ、トロイは占領されてしまうのです。

アップデート

古いバージョンのソフトウェアあるいはハードウェア製品を置き換えるために設計された、同じ製品の新しいバージョンです。また、アップデートのインストール処理では、お使いのコンピュータに古いバージョンがインストールされているか確認するのが普通です。この場合、インストールされていないと、アップデートもインストールできません。

BitDefender は、お客様が手動でアップデートを確認する以外に、製品を自動でアップデートできる、独自のアップデートモジュールを持っています。

ウイルス

お使いのコンピュータに知らない間に読み込まれ、お客様が希望していない動作を勝手に行う、プログラムあるいはコードの一部です。多くのウイルスは、自分自身を複製して増殖します。すべてのコンピュータウイルスは、人の手によるものです。自身を複製し続けるだけの単純ウイルスは、比較的簡単に作成できます。そんな単純なウイルスでも、使用可能なメモリをすぐに使い尽くし、システムを停止させてしまうので危険です。もっと危険な種類のウイルスでは、ネットワーク全体に自身を蔓延させ、セキュリティシステムを回避します。

ウイルス定義

アンチウイルスプログラムがウイルスを検出して除去するために使う、ウイルスのバイナリパターンです。

ワーム

ネットワークを通過する度に自身を複製し、ネットワークを超えて自己増殖するプログラムです。他のプログラムに自身を添付することはできません。