bitdefender

ANTIVIRUS 2009

ユーザガイド

bitdefender

BitDefender Antivirus 2009
ユーザガイド

発行 2009.04.02

法的通知

BitDefender Antivirus 2009

bitdefender

目次

エンドユーザ ソフトウェアライセンス契約

これら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、いかなる形であれソフトウェアをインストールまたは使用すると、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。

製品登録：このライセンス契約に同意した場合、ソフトウェアの登録に同意したこととなります。"マイアカウント"を使用することによって、ソフトウェアのアップデートやライセンスの更新をすることができます。このライセンス契約は正当なソフトウェアライセンスのもとで使用されているコンピュータおよびエンドユーザに適用され、アップデートやサポートなどのサービスが受けられることを保証いたします。登録には、有効なライセンスキーと更新のご案内や法的なご案内を受け取るための有効なメールアドレスが必要です。

これらの条件は、関連文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、文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製品およびサービスに適用されます。

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る、コンピュータソフトウェアおよびサービス、場合により関連するメディア、印刷物、および"オンライン"または電子的な文書も含む上記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）とBITDEFENDERと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、または使用すると、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、ならびに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、単独のコンピュータにインストールでき、ネットワークサービスを提供しないBitDefenderソフトウェアに適用されます。初期ユーザはそれぞれ、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。許可される初期ユーザの数は、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直ちにその機能を停止します。

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または代理店によって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、音声、音楽、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のあらゆる複製は、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。そのためお客様は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複製することはできません。BitDefenderが保存される媒体や形式に関わらず、作成されたすべての複製に対して、元の状態のまま著作権表示を作成し、添付しなければなりません。BitDefenderライセンス

は、サブライセンス、賃貸、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、派生品の作成、改造、翻訳、および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およびその代理店は、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およびその代理店が独自の判断で、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およびその代理店は、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およびその代理店は、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およびその代理店は、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およびその代理店は、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、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およびその代理店は、BITDEFENDERおよびその代理店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およびその代理店の責任は、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。

州や国によっては、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。

BITDEFENDERおよびその代理店の責任はBitDefenderの購入費用を超えることはありません。この免責事項と制限は、BitDefenderの使用、評価、テストにかか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耐障害性製品ではなく、安全な動作あるいは運用を必要とする危険環境で使用するための設計または想定はされていません。このソフトウェアは、航空機の航行操作、核施設、あるいは通信システム、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対象には使用できません。

メール、ウェブなどを通じた告知への同意：．　BITDEFENDERおよびその代理店は法的な告知やソフトウェアのライセンス更新、有用と思われる情報を送信いたします。（以下、"コミュニケーション"といいます）BITDEFENDERおよびその代理店からのコミュニケーションは製品内での告知や製品登録時にご登録頂いたメールアドレスへのメール、またはウェブサイトへの掲載にて行います。このライセンス契約に同意した場合、お客様はこれら全てのコミュニケーションについて同意したものとみなされます。

全体的な事柄：この契約は、ルーマニアの法律、日本国内の関連する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。日本国内においてライセンスされたものについては、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、東京地方裁判所とします。

製品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。

この契約条件の一部が無効な場合でも、その無効性が、この契約の残り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。この製品あるいは関連して使われるその他の商標は、すべて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、このライセンスは通知なしに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およびその代理店は、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。

この諸条件の他言語への翻訳内容が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。日本国内においては、日本国内総代理店である株式会社サンブリッジソリューションズ（東京都渋谷区恵比寿１−１９−１９ 恵比寿ビジネスタワー１３階 電話番号：03-4360-4010 またはＦＡＸ：03-4360-4011、電子メールアドレス：sales@bitdefender.jp）へお願いいたします。

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 2009を選択されたすべてのお客様を対象にしています。この文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。

この文書では、BitDefender Antivirus 2009、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 2009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。

お客様にとって、喜ばしく有益な内容であることを願っています。

1. この文書で使用されている決まり事

1.1. 字体の決まり事

内容を読みやすくするために複数の字体を使っています。その内容と目的は以下の表のようになっています。

表記	説明
sample syntax	構文の例は、等幅文字で記載されています。
http://www.bitdefender.com	URL リンクは、http または ftp サーバの外部の場所を示しています。
support@bitdefender.com	連絡先として、メールアドレスが本文に挿入されています。
「はじめに」 (p. xv)	これは、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、等幅フォントを使用して記載されています。

表記	説明
option	すべての製品オプションは、強調文字で記載されています。
sample code listing	コードリストは、等幅文字で記載されています。

1.2. お知らせ・警告

警告は、テキスト内の注意書きです。現在の段落に関係する追加情報をお客様にわかりやすく、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、関連する話題についての特別な機能やリンクなど有益な情報を提供している場合があります。

重要項目
注意が必要な内容で読み飛ばしてはいけません。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要な情報です。内容に従うことを強くお勧めいたします。高い危険を伴う内容が含まれていますので、よく読んで理解しておいてください。

2. この文書の構造

このドキュメントはいくつかの大きな章に分かれています。 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をパソコ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 2009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。

基本設定. BitDefenderの基本的な管理とメンテナンスの説明です。

詳細設定. BitDefenderが提供するセキュリティ機能の詳細な説明です。 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。

方法. BitDefenderで最もよく使われるタスクをすぐに実行するための手順を用意します。

問い合わせ先. 予期しない事態が起きた時に相談するための連絡先です。

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。

用語集. 用語集では、この文書の中で使用されている専門用語や一般的でない用語を説明します。

3. コメントのお願い

本書の内容を改善していくため、ご意見・ご感想をお寄せください。ご紹介するすべての情報に関して、可能な限り調査・検証を行っておりますが、この文書に関する問題点や改良できる点がございましたら、ぜひお知らせください。

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

重要項目

メールを効率的に処理できるよう、本書の内容に関するメールは、具体的で簡潔にまとめて送っていただけますようお願い申し上げます。

インストール

1. システム要件

BitDefender Antivirus 2009は、以下のオペレーティングシステムでのみ動作します：

■Windows XPおよびService Pack 2 (32/64 bit)以上
■Windows Vista (32/64 bit)またはWindows Vista Service Pack 1(32/64 bit)
■Windows Home Server

インストールをする前に、お使いのコンピュータが最低限のハードウェアおよびソフトウェアの要件を満たしていることを確認してください。

注意
あなたがお使いのコンピュータがどのWindowsバージョンやハードウェアで動作しているのかを確認するには、デスクトップにある マイコンピュータ を右クリックし、メニューから プロパティを選択します。

1.1. ハードウェア要件：

Windows XP

■800MHz以上のプロセッサ
■512MBのRAMメモリ（1GB以上を推奨）
■170MBのハードディスク空き容量（200MB以上を推奨）

Windows Vista

■800MHz以上のプロセッサ
■1GBのRAMメモリ
■170MBのハードディスク空き容量（200MB以上を推奨）

Windows Home Server

■800MHz以上のプロセッサ
■1GBのRAMメモリ
■170MBのハードディスク空き容量（200MB以上を推奨）

1.2. ソフトウェア要件：

■Internet Explorer 6.0以降
■.NET Framework 1.1(インストーラーに含まれています)

アンチフィッシング保護は以下の製品に対して有効です：

■Internet Explorer 6.0以降
■Mozilla Firefox 2.0
■Yahoo! Messenger 8.1（英語版）
■Windows Live (MSN) Messenger 8.5

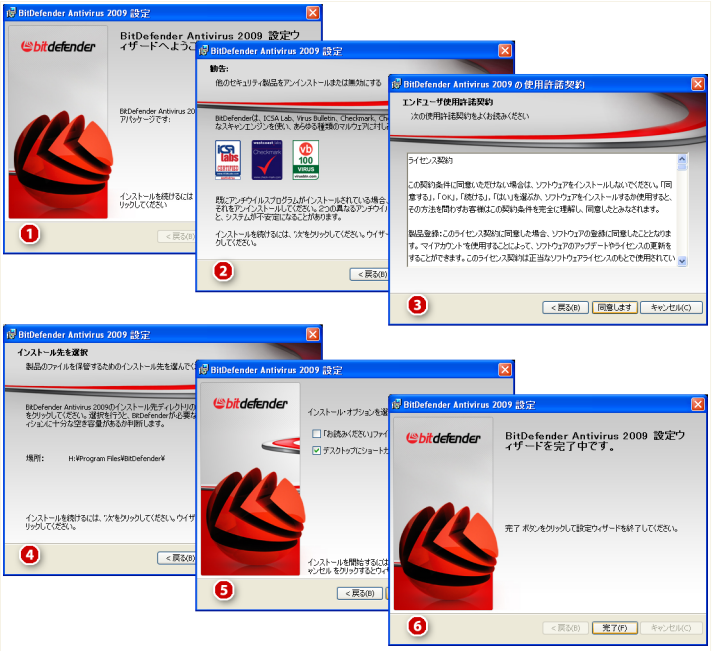
インスタントメッセージ暗号化は以下の製品に対して有効です：

■Yahoo! Messenger 8.1（英語版）
■Windows Live (MSN) Messenger 8.5

2. BitDefenderのインストール

Setupファイル探してダブルクリックしてください。起動されたウィザードに従って設定作業を進められます。

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。「はい」をクリックして新しいバージョンをダウンロードするか、「いいえ」をクリックしてインストールを続けてください。



インストール手順

次の手順に従ってBitDefender Antivirus 2009をインストールしてください：

1. 次へをクリックして次へ進むか、キャンセルをクリックしてインストールを中止してください。
2. 次へをクリックします。

   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 2009が警告します。 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. ライセンス契約をお読みになり、同意をクリックします。

   重要項目

   条件に同意して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中断され、Setupを終了します。

4. デフォルトでは、BitDefender Antivirus 2009は C:¥Program Files¥BitDefender¥BitDefender 2009 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。

   次へをクリックします。

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:

   ■「お読み下さい」ファイルを開く - インストールの最後で、「お読み下さい」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 2009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ます。 もし、.NET Framework 1.1がインストールされていない場合には、BitDefenderインストーラーは最初にこれをインストールいたします。

インストールが完了するまでお待ちください。

6. 終了をクリックします。 設定ウィザードがインストール処理を完了するために、システムの再起動を促される場合があります。 その場合はできるだけ早く再起動するようお勧めします。

重要項目

インストール終了後、コンピュータを再起動します。製品登録ウィザード、そして設定ウィザードが表示されます。 製品登録ウィザードとBitDefender Antivirus 2009の設定ウィザードが完了するとBitDefenderアカウントを作成します。

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 2009というサブフォルダがあります。

2.1. 製品登録ウィザード

インストール後、はじめてコンピュータを再起動するときに製品登録ウィザードは表示されます。 ウィザードを使ってBitDefender製品の登録やBitDefenderアカウントの設定を簡単に行うことができます。

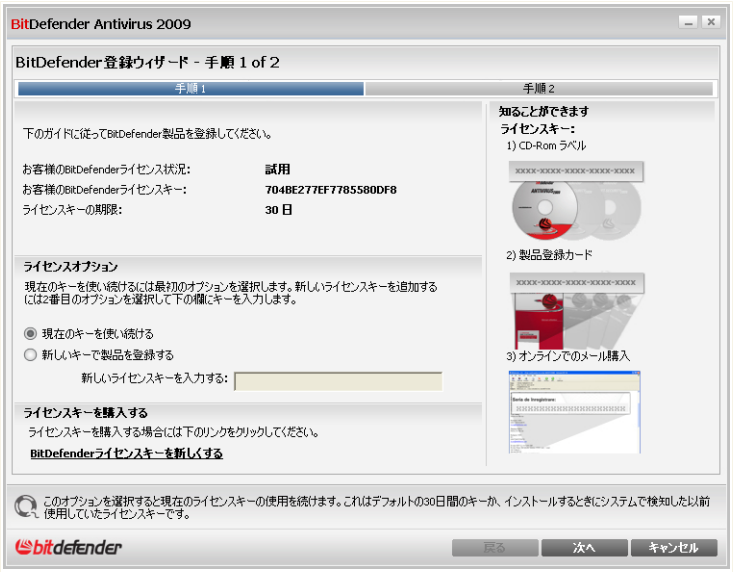
BitDefenderアカウントは、BitDefenderの更新に必要となりますので必ず作成してください。 BitDefenderアカウントは、無料のテクニカルサポートや製品をお得に購入できるご案内を受けることができます。 登録した電子メールアドレスとパスワードを使用しhttp://myaccount.bitdefender.comからマイページにログインすることができます。

注意

このウィザードを進めたくない場合、キャンセルをクリックしてください。 製品登録ウィザードは製品内に表示される登録をクリックすることでいつでも実行することができます。

登録ウィザードをキャンセルすると、構成ウィザードもキャンセルされることに注意してください。 設定ウィザードをもう開くことができません。BitDefenderを開いて存在している問題を修正する必要があります。追加の設定が必要です。

2.1.1. 手順 1/2 - BitDefender Antivirus 2009を登録する



製品登録

BitDefender Antivirus 2009には30日間の試用期間が設けられています。 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。

BitDefender Antivirus 2009を登録する

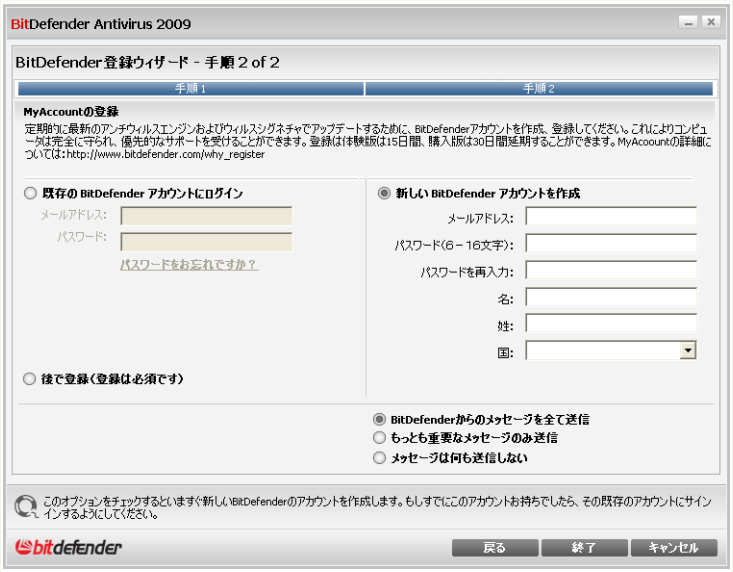
1. この製品を登録を選択します。
2. ライセンスキーを入力します。

注意
ライセンスキーはこちらに書かれています：
■CDラベル
■製品登録カード
■オンラインストアからのメール

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

次へをクリックしてください。

2.1.2. 手順 2/2 - BitDefenderアカウントを作成



アカウント作成

もし、いまBitDefenderアカウントを作成しない場合には、登録をスキップを選択し、終了をクリックします。 それ以外の場合は、このまま進めます：

- 「まだBitDefenderアカウントをお持ちでない場合」 (p. 10)
- 「既にBitDefenderアカウントを持っている場合」 (p. 10)

重要項目

BitDefenderをインストールして15日以内にBitDefenderアカウントを作成してください。（ライセンスキーを登録した場合、BitDefenderアカウントの作成期限は30日まで延長されます） 登録がない場合にはBitDefenderは更新されなくなります。

まだBitDefenderアカウントをお持ちでない場合

新しい BitDefenderアカウントを作成を選択して必要な情報を入力してください。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。 パスワードは６文字から１６文字の間である必要があります。

■パスワードを再入力 - 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 - 名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
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からマイページ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アクティブ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。

BitDefenderは製品の特別価格での販売のご案内やプロモーションをアカウントとして登録していただいたメールアドレスに送ることがあります。 以下のオプションから選択できます：

■BitDefenderからの全ての案内を受け取る
■大切なメッセージだけ受け取る
■全てのメッセージを受け取らない

終了をクリックします。

既にBitDefenderアカウントを持っている場合

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。 この場合はアカウントのパスワードを入力してください。

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。

パスワードを忘れた場合は、パスワードを忘れたら？をクリックし指示に従ってください。

BitDefenderは製品の特別価格での販売のご案内やプロモーションをアカウントとして登録していただいたメールアドレスに送ることがあります。 以下のオプションから選択できます：

■BitDefenderからの全ての案内を受け取る
■大切なメッセージだけ受け取る
■全てのメッセージを受け取らない

終了をクリックします。

2.2. 設定ウィザード

製品登録ウィザードを完了させると、設定ウィザードが表示されます。 ウィザードでは製品モジュールの設定や重要なセキュリティ設定を容易に行えるようにします。

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 Antivirus 2009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。

注意

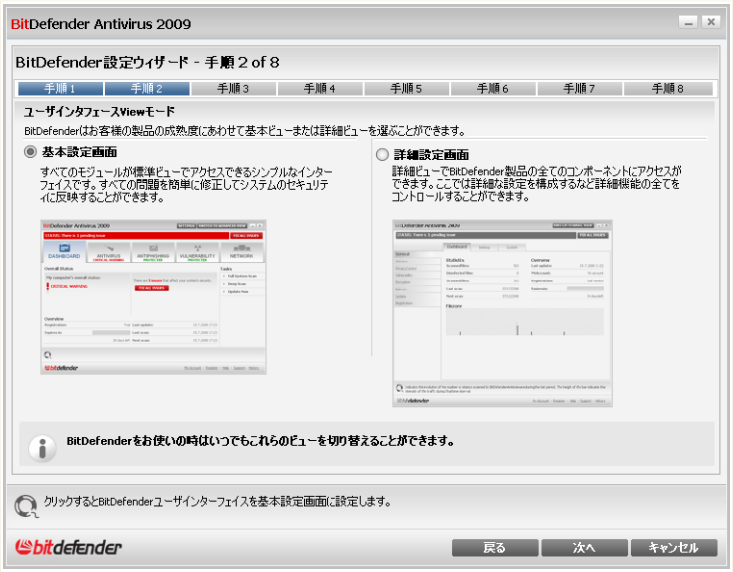
このウィザードを進めたくない場合、キャンセルをクリックしてください。 ユーザインタフェースを開いたとき、設定が必要なコンポーネントがあると通知されます。

2.2.1. 手順 1/8 - はじめに

はじめに

次へをクリックしてください。

2.2.2. 手順 2/8 - 設定画面の選択



設定画面

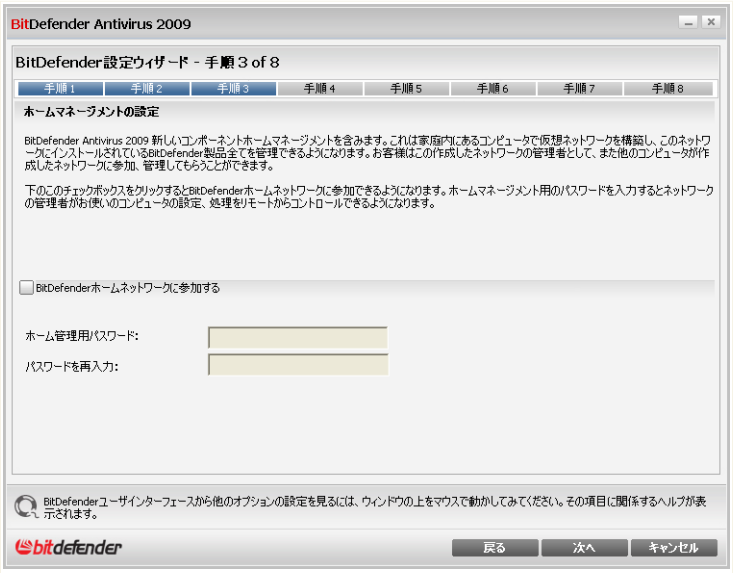
BitDefenderの使い方や使用経験によって、２つの設定画面を使い分けることができます。

■基本設定画面. 基本的な設定を簡単に設定したいというようなユーザや初心者に向けたシンプルなインタフェースです。 BitDefenderからの警告を確認して問題を修理しなければなりません。

■詳細設定画面. 全ての設定を行いたいというユーザや技術に詳しい方に向けた詳細設定ができるインタフェースです。 全てのコンポーネントの詳細設定を行うことができます。

次へをクリックしてください。

2.2.3. 手順 3/8 - BitDefenderネットワークを設定する



BitDefenderネットワーク設定

BitDefenderは家庭内にあるコンピュータで仮想ネットワークを構成することができ、BitDefender製品のインストールや管理を行うことができます。

このコンピュータをBitDefenderネットワークに参加させるには、以下の手順に従ってください：

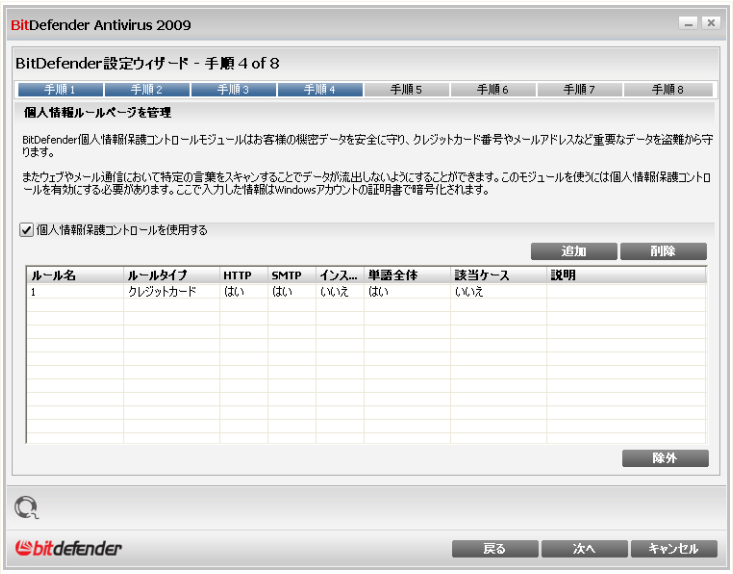
1. BitDefenderネットワークに参加するを選択します
2. 入力欄に同じ管理者パスワードをを入力します。

重要項目

このパスワードで他のコンピュータのBitDefender製品の管理を行うことができるようになります。

次へをクリックしてください。

2.2.4. 手順 4/8 - 個人情報コントロール



個人情報コントロールの設定

個人情報コントロールは個人情報がネットワークに漏洩することを防ぎます。 個人情報コントロールは、作られたルールに従って、ウェブ、メール、インスタントメッセージから特定の文字列（例えばクレジットカード番号）をスキャンします。もし該当する情報があった場合には、それらが流出するのを防ぎます。

個人情報コントロールを使うには、以下の手順で設定します：

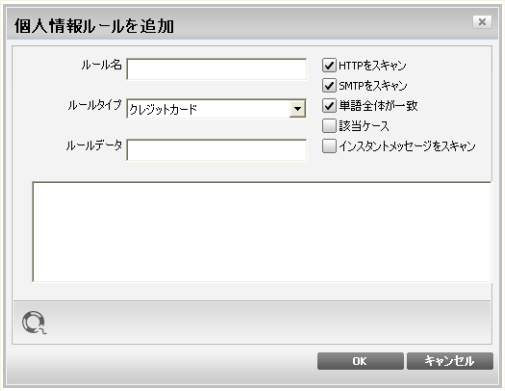
1. 個人情報コントロールを使うを選択します。
2. あなたの重要なデータを守るルールを作成します　詳細については、「個人情報コントロールのルールを作成します」（p. 16）をご参照ください。

3. 必要に応じて例外を定義することもできます。 詳細については、「個人情報コントロールの例外を指定」 (p. 17)をご参照ください。

次へをクリックしてください。

個人情報コントロールのルールを作成します

個人情報コントロールのルールを作成する場合は追加をクリックしてください。 新しい設定ウィンドウが表示されます。



個人情報コントロール

以下の内容を設定する必要があります：

- ルール名 – 編集欄に新しい名前を入力してください。
- 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）、SSN（ソーシャルセキュリティ番号）などのルールの形式を選択してください。
- ルールデータフィールドに、送信したくない文字列の種類を入力します。 例えばクレジットカード番号を保護する場合には、ここに全ての形式または形式の一部を入力します。

注意
入力した内容が３文字未満の場合、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文字は入力することをお勧めします。

ルールのデータが単語全体と一致した場合のみ、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のみ、ルールが適用されるように指定できます。

ルールに沿ってブロックされることが多い場合には、より詳細なルールを記入欄に記述します。

特定の形式のトラフィックをスキャンするには、これらのオプションを設定します：

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

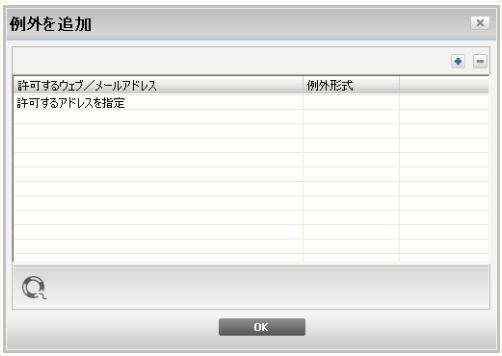
■インスタントメッセージをスキャン - インスタントメッセージをスキャンし、ルールのデータと一致するメッセージをブロックします。

完了をクリックしてルールを追加します。

個人情報コントロールの例外を指定

特定の個人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。 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ためのルールを作成した場合を考えてみましょう。この場合は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たびに、対象となるページがブロックされます。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場合には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ィンドウを開くには、例外をクリックします。



個人情報コントロールの例外

例外を追加するには以下の手順に従ってください：

1. ルールを追加ボタンをクリックしてルールの属性を選択してください。
2. 許可するアドレスを指定をダブルクリックして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ます。
3. 形式を選択をダブルクリックして先に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ます。
   ■ウェブアドレスを指定した場合はHTTPを選択してください。
   ■メールアドレスを指定した場合はSMTPを選択してください。

例外を削除するには削除ボタンをクリックしてください。

OKをクリックしてウィンドウを閉じます。

2.2.5. 手順 5/8 -ウィルスレポートの設定

ウイルスレポートの設定

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。

以下のオプションを設定することができます：

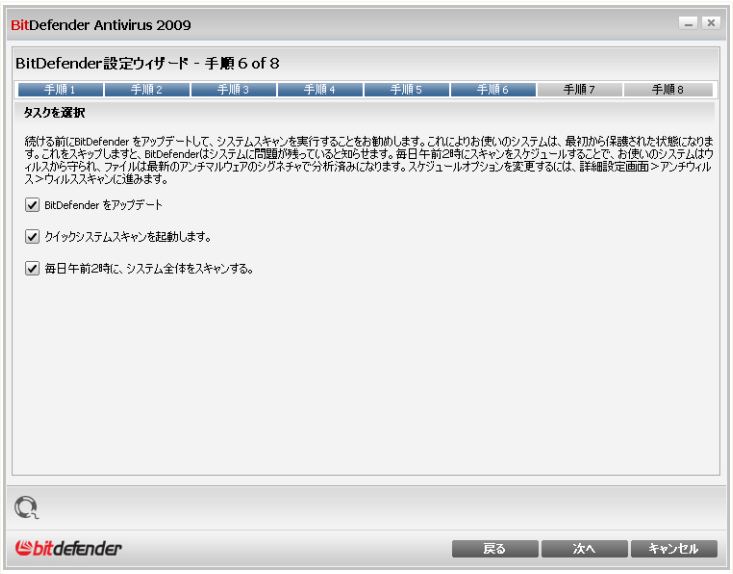
■ウイルスレポートを送信 - コンピュータで見つかったウイルスに関するレポートをBitDefender研究所へ送ります。

■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。

注意
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。

次へをクリックしてください。

2.2.6. 手順 6/8 - 実行するタスクを選択



タスク選択

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 Antivirus 2009を設定してください。 以下のオプションを指定できます：

■BitDefenderをアップデート - 次のステップで、BitDefenderエンジンのアップデータが行われます。これはコンピューターを最新の脅威から守るためです。

■クイックシステムスキャンを実行 - 次のステップで、BitDefenderはWindowsおよびProgram Filesフォルダ内のファイルが感染していないことを確認するためクイックシステムスキャンを実行します。

■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。

注意

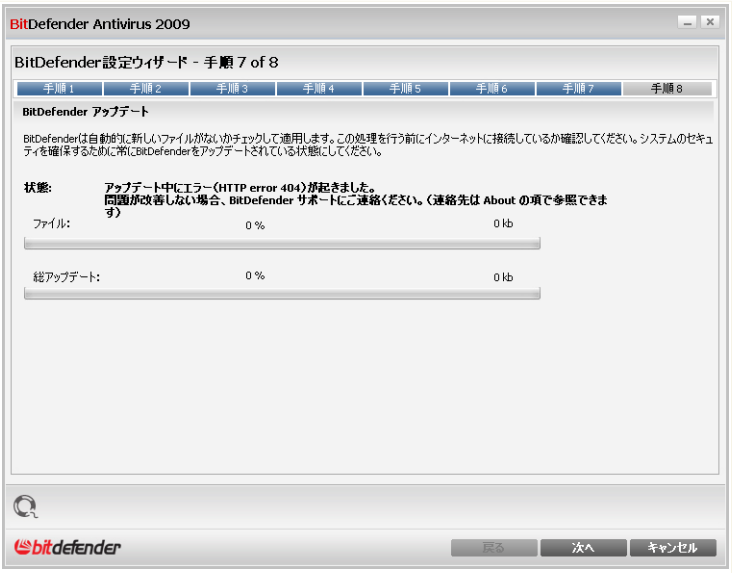
スキャンを実行するスケジュールを変更したい場合には、ウィザード終了後次の手順に従ってください。

1. BitDefenderを開く。
2. 画面が標準設定画面の場合には詳細設定画面 ボタンをクリックしてください。画面の右上にあります。
3. 左メニューにあるアンチウィルスをクリックします。
4. ウィルススキャン タブをクリックします。
5. フルシステムスキャン タスクを右クリックして スケジュールを選択します。新しいウィンドウが開きます。
6. 頻度と開始時間を必要に応じて変更する。
7. OKをクリックして変更を保存します。

お使いのシステムのセキュリティを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しているか、あるいはオプションを１つも選択していない場合には次の手順は省略されます。

次へをクリックしてください。

2.2.7. 手順 7/8 - タスクが完了するまでお待ちください



タスクの状況

BitDefenderがマルウェアのシグネチャとスキャンエンジンをアップデートするまでお待ちください。アップデートが完了しだい、クイックシステムスキャンが起動します（選択されている場合）。 スキャンはバックグラウンドで実行されます。 スキャンが進行していることを表すアイコンが システムトレイにあることが確認できます。 このアイコンをクリックするとスキャンウィンドウが開き、スキャン状況をみることができます。

注意

スキャンにはしばらく時間がかかります。終了時にスキャンウィンドウを開いてスキャン結果をチェックしてシステムがクリーンがどうか確認してください。 もしウィ

ルスがスキャン中に検出された場合、すぐにBitDefenderをオープンしてフルシステムスキャンを実行してください。

次へをクリックしてください。 スキャン完了までまつ必要はありません。

2.2.8. 手順 8/8 - 終了

終了

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。

終了をクリックします。

3. アップグレード

古いバージョンのBitDefender製品からBitDefender Antivirus 2009へのアップグレードは、以下の方法で行います：

1. 古いバージョンのBitDefender製品をコンピュータから削除します。 詳細についてはヘルプや製品のユーザマニュアルをご参照ください。
2. コンピュータを再起動してください。
3. BitDefender Antivirus 2009のインストールについては、「BitDefenderのインストール」 (p. 4)ユーザガイドをご覧ください。

4. BitDefenderの修復または削除

BitDefender Antivirus 2009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 2009 → 修復・削除

次へをクリックして確認を行います。新しいウィンドウが表示されそこで以下の項目を選択できます：

■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ィンドウが開きます。 修復をクリックすると修復処理が開始されます。

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 Antivirus 2009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。 終了をクリックします。

■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
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の削除を選択すると新しいウィンドウが開きます。

重要項目
Windows Vistaのみ. 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。

削除をクリックするとお使いのコンピュータからのBitDefender Antivirus 2009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。 終了をクリックします。

注意

削除処理が完了したらプログラムから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発生した場合

BitDefenderの削除中にエラーが発生すると、削除処理が中止されて新しいウィンドウが開きます。 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レジストリキーを削除します。

基本設定

5. 使い方

インストールされたBitdefenderはコンピュータを守ります。 設定ウィザードを終えていない場合は、まずBitDefenderを開いて問題を修正してください。 特定のBitDefenderコンポーネントを構成するか、予防的な処理を行ってコンピュータとデータを守ってください。 特定の問題に関してBitDefenderが警告を出さないようにすることができます。

製品を登録（BitDefenderアカウントの作成を含む）していない場合には、試用期間終了までに行う必要があります。 BitDefenderをインストールして15日以内にBitDefenderアカウントを作成してください。（ライセンスキーを登録した場合、BitDefenderアカウントの作成期限は30日まで延長されます） 登録がない場合にはBitDefenderは更新されなくなります。 登録手続きに関しては以下を参照してください。 「登録とマイアカウント」 (p. 93).

5.1. BitDefenderを開く

BitDefender Antivirus 2009のメインインターフェースを開くには、Windowsスタートメニューから、スタート → プログラム → BitDefender 2009 → BitDefender Antivirus 2009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。

5.2. ユーザインタフェース選択

BitDefender Antivirus 2009はコンピュータに詳しい人だけでなく初心者でも簡単に使うことができます。グラフィカルなユーザインターフェースは全ての方々に使いやすいようにデザインされています。

BitDefenderでは基本設定画面または詳細設定画面を選ぶことができます。

注意
基本設定画面または詳細設定画面をクリックすることで簡単にどちらかを選ぶことができます。

5.2.1. 基本設定画面

基本設定画面では全てのモジュールの基本設定がシンプルなインターフェースから行うことができます。また警告やクリティカルな問題の修正もできます。

基本設定画面

■インターフェースの上段には状況を示す２つのボタンがあり、状況がわかりやすく表示されます。

アイテム	説明
設定	ウィンドウを開き、重要なセキュリティモジュールを有効にしたり無効にすることが簡単にできます。
詳細設定画面に切替	詳細設定画面を開く。　ここで各BitDefenderモジュールについて詳細に設定できます。　BitDefenderはこのオプションを次回この画面を開いたときにも覚えています。
ステータス	コンピュータの脆弱性を修正する情報が含まれています。

■真ん中のウィンドウには５つのタブがあります。 このタブは次のセクションの詳細を表示しています 「基本設定画面タブ」（p. 56）。

タブ	説明
ダッシュボード	重要な製品に関する統計情報および製品登録状況、重要なオンデマンドタスクの状況が表示されます。
アンチウイルス	BitDefenderの更新およびウィルスの感染などアンチウィルスモジュールの状況が表示されます。
アンチフィッシング	オンライン時にフィッシング攻撃（個人情報盗難）から守るモジュールのステータスをあらわしています。
脆弱性	脆弱性モジュールはお使いのソフトウェアを最新版に保つために役立ちます。 ここでコンピュータのセキュリティに影響する脆弱性の問題を簡単に修復できます。
ネットワーク	BitDefenderネットワークを表示する。 ここではホームネットワークに参加しているBitDefender製品のさまざまな設定や管理を行うことができます。 このようにして、ホームネットワーク内のセキュリティを、1台のコンピュータから管理することができます。

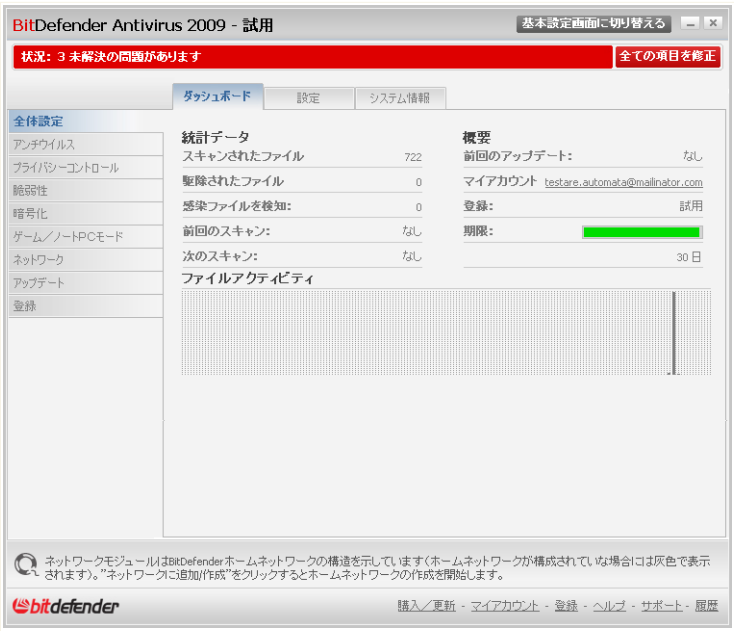
■さらにBitDefender基本設定画面には複数の便利なショートカットがあります。

リンク	説明
購入／更新	ウェブページを開いてお使いのBitDefender Antivirus 2009のライセンスキーを購入できます。
マイアカウント	ウェブページを開いてBitDefenderアカウントにログインします。 BitDefenderアカウントの作成は登録に必須です。BitDefenderアカウントについては次を参照してください。「BitDefenderアカウントの作成方法」（p. 225）.
登録する	新しいライセンスキーの登録やいまのライセンスキーの有効期限などを確認することができます。
ヘルプ	BitDefenderの使い方を表示するヘルプファイルを開きます。

リンク	説明
サポート	BitDefenderのサポートウェブページを開きます。
履歴	BitDefenderを使って行ったタスクの履歴を確認することができます。

5.2.2. 詳細設定画面

詳細設定画面ではBitDefenderの各コンポーネントにアクセスすることができます。ここで詳細にBitDefenderを構成することができます。



詳細設定画面

■ウィンドウ上部にあるボタンとステータスバーではいまの状況を簡単に理解することができます。

アイテム	説明
基本設定画面	基本設定画面を開きます。ここはBitDefenderの基本的な画面で主要モジュールとダッシュボードが含まれます。BitDefenderはこのオプションを次回開く際にも覚えています。
ステータス	コンピュータの脆弱性を修正する情報が含まれています。

■設定コンソールの左側で選択できるモジュールを確認できます：

注意
詳細設定画面のモジュールはユーザガイドの 「詳細設定」（p. 101）に詳しく説明されています。

モジュール	説明
一般設定	一般設定へのアクセスやダッシュボード、システム情報を見ることができます。
アンチウィルス	ウィルスからの保護や例外の設定、隔離モジュールの設定などスキャンの詳細を設定することができます。
個人情報コントロール	コンピュータがオンラインの時に個人情報が漏洩することを防ぐことができます。
脆弱性	重要なソフトウェアを常に最新版に保つことができます。
暗号化	Yahoo MessangerとWindows Live(MSN)メッセンジャーでの会話を暗号化することができます。
ゲーム/ノートＰＣモード	ノートＰＣがバッテリで動作しているときにスケジュールされているタスクを延期したりやゲームを楽しんでいるときに全てのアラートやポップアップを表示しないようにします。
ネットワーク	自宅内でネットワークに接続されているコンピュータを管理することができます。

モジュール	説明
アップデート	製品のアップデートやアップデートに関する詳細の設定を行うことができます。
製品登録	BitDefender Antivirus 2009を登録やライセンスキーを変更、または BitDefenderアカウントを作成することができます。

■さらに詳細設定画面ではいくつか便利なリンクがあります。

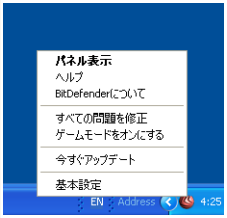
リンク	説明
購入／更新	ウェブページを開いてお使いのBitDefender Antivirus 2009のライセンスキーを購入できます。
マイアカウント	ウェブページを開いてBitDefenderアカウントにログインします。 BitDefenderアカウントの作成は登録に必須です。BitDefenderアカウントについては次を参照してください。「BitDefenderアカウントの作成方法」 (p. 225).
登録する	新しいライセンスキーの登録やいまのライセンスキーの有効期限などを確認することができます。
ヘルプ	BitDefenderの使い方を表示するヘルプファイルを開きます。
サポート	BitDefenderのサポートウェブページを開きます。
履歴	BitDefenderを使って行ったタスクの履歴を確認することができます。

5.3. システムトレイのBitDefenderアイコン

製品全体をより素早く管理するために、システムトレイの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のメイン画面を開きます。



BitDefenderアイコン

■

■ヘルプ - ヘルプファイルを開きます。ヘルプにはBitDefender Antivirus 2009の設定方法、使い方が詳細に書かれています。

■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ィンドウが開きます。

■すべての問題を修正 - 現時点でのセキュリティ上の脆弱性を除去する手助けをします。 このオプションが利用できない場合は、何も修正すべき問題がありません。 詳細については次を参照してください。「問題を修正」 (p. 52)

■ゲームモードをオン / オフ - ゲームモードの動作、停止を行います。

■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。

■基本設定 - 重要なセキュリティモジュールの有効化/無効化を簡単に設定することができます。 新しいウィンドウが表示されクリックすることで動作／停止をすることができます。 詳細については次を参照してください。 「クイック有効／無効設定」 (p. 89).

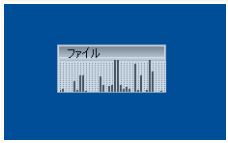
ゲームモードがオンのときにはGという文字がBitDefenderアイコンの上に表示されます。

お使いのシステムに影響する重大な問題がある場合には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。

5.4. スキャンアクティビティバー

スキャンアクティビティバーはシステムのスキャン処理をグラフにより視覚化したものです。 小さな画面だけが詳細設定画面では利用できます。 基本設定画面に切り替えると、スキャンアクティビティバーは消えます。

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



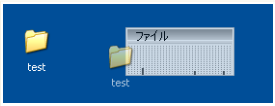
スキャンアクティビティバー

注意
スキャンアクティビティバーはリアルタイムプロテクション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。

5.4.1. ファイルとフォルダをスキャン

スキャンアクティビティバーを使ってファイルとフォルダをスキャンできます。 スキャンしたいファイルまたはフォルダを、以下のようにスキャン処理バーへドラッグ&ドロップします。

ファイルをドラッグ



ファイルをドロップ

アンチウィルススキャンウィザード ではスキャン処理についてガイドします。

スキャン・オプション. スキャンオプションは事前に最高の検出結果を得るよう設定されています。 感染ファイルを検知すると、BitDefenderは駆除（マルウェアのコードの除去）しようとします。駆除が失敗した場合には、アンチウィルススキャ

ンウィザードは感染ファイルに対して他の処理を選択するよう聞いてきます。　スキャンオプションは基本的なもので変更することはできません。

5.4.2. スキャンアクティビティバーの無効と復元

グラフィカルなインタフェースを表示したくない場合は右クリックして隠すを選択してください。 スキャンアクティビティバーを復元するには次の手順を行います：

1. BitDefenderを開く。
2. 画面が標準設定画面の場合には詳細設定画面　ボタンをクリックしてください。画面の右上にあります。

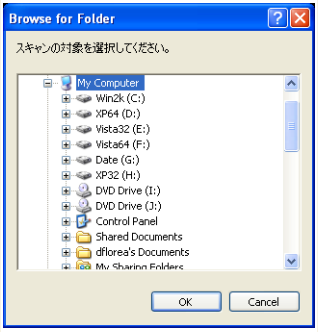
   重要項目
   スキャンアクティビティバーは詳細設定画面のときのみに利用できます。

3. 左側にあるメニューから一般設定をクリック
4. 設定タブをクリックします。
5. スキャンアクティビティバーを有効にする（処理状況を画面にグラフ表示）チェックボックスのチェックを選択します。

5.5. BitDefender手動スキャン

BitDefender手動スキャンでは、ハードディスクパーティション上の特定のフォルダを、新たにタスクを作成することなく実施できます。 このモードはWindowsがセーフモードで動作している場合の使用を想定しています。 もしシステムが耐久性のあるウィルスに感染している場合には、このウィルスをWindwosをセーフモードで起動して、各ハードディスクのパーティションからBitDefender手動スキャンによって除去を試みてください。

BitDefender手動スキャンにアクセスするには、Windows のスタートメニューから、スタート → プログラム → BitDefender 2009 → BitDefender手動スキャンを選んでください。 以下のウィンドウが開きます：



BitDefender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択してOKをクリックするだけです。 アンチウィルススキャンウィザード ではスキャン処理についてガイドします。

スキャン・オプション. スキャンオプションは事前に最高の検出結果を得るよう設定されています。感染ファイルを検知すると、BitDefenderは駆除（マルウェアのコードの除去）しようとします。駆除が失敗した場合には、アンチウィルススキャンウィザードは感染ファイルに対して他の処理を選択するよう聞いてきます。 スキャンオプションは基本的なもので変更することはできません。

セーフモードとは？.
セーフモードは特殊なWindowsの起動方法です。主に通常のWindowsの動作に影響する問題の解決のために使われます。その問題にはドライバーの衝突から、ウィルスによってWindwosが通常に起動できないなどさまざまのものがあります。 セーフモードでは、Windowsは必要最小限のOSコンポーネントとドライバしかロードしません。セーフモードではわずかなアプリケーションしか動作しません。このためセーフモードのWindowsではほとんどのウィルスが活動できず、よって除去もしやすくなります。
Windwosをセーフモードで動作させるには、再起動してF8 キーを押し続け Windows Advanced Options Menu を表示させます。セーフモードで起動できるオプションから選択することができます。セーフモード（ネットワーク） を選ぶことでインターネットへのアクセスが可能です。

注意

セーフモードについてより詳細はWindowsのヘルプとサポートセンターにアクセスします（スタートメニューからヘルプとサポート）をクリックします。 インターネットを検索することで役に立つ情報をみつけることができます。

5.6. 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に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：

■プロセッサの消費とメモリ消費を最小に

■自動アップデートとスキャンを延期

■全ての警告とポップアップを抑制

■重要なファイルのみスキャン

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。

5.6.1. 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。

■Ctrl+Shift+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。

5.6.2. 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を開く。
2. 画面が標準設定画面の場合には詳細設定画面　ボタンをクリックしてください。画面の右上にあります。
3. 左側のメニューからゲーム／ノートＰＣモードをクリックします。
4. ゲームモードタブをクリックします。
5. 詳細設定ボタンをクリックします。
6. 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)

■入力欄に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

ホットキーを使うのチェックを外すことでホットキーを無効にすることができます。

7. OKをクリックして変更を保存します。

5.7. アンチウィルススキャンウィザード

オンデマンドスキャンを実行すると（フォルダを右クリックして BitDefender 2009 でスキャンを選択）、BitDefender アンチウィルススキャンウィザードが表示されます。 以下の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。

注意

スキャンウィザードが表示されない場合には、スキャンがバックグラウンドで実行されるように設定されています。 スキャンが進行していることを表すアイコンが システムトレイにあります。 このアイコンをクリックするとスキャンウィンドウが開き、スキャン状況をみることができます。

5.7.1. 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。

BitDefenderがスキャンを完了するまでお待ちください。

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。

パスワード保護されたアーカイブ．　BitDefenderがパスワード保護されたアーカイブをスキャン中に発見すると、デフォルトでは パスワード入力プロンプトを表示してパスワードの提供を求めてきます。　パスワードでプロテクトされたアーカイブは、あなたがパスワードを提供しない限りスキャンすることはできません。 以下のオプションを指定できます：

■このオブジェクトのパスワードを入力します。. BitDefenderにこのアーカイブをスキャンさせる場合には、このオプションを選択してパスワードを入力します。パスワードを知らない場合には、他のオプションを選択してください。

■このオブジェクトのパスワードを入力しません（このオブジェクトをスキップ）. このオプションを選択するとこのアーカイブのスキャンをスキップします。

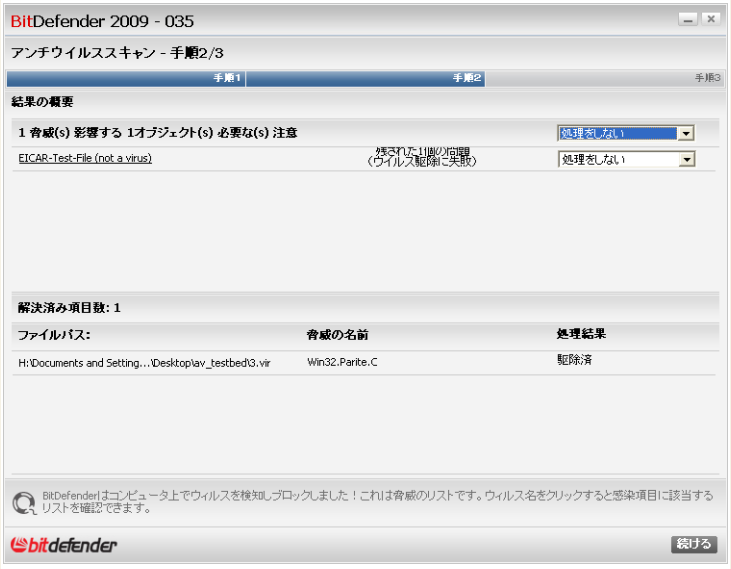
■すべてのオブジェクトのパスワードを入力しません（パスワード保護されたオブジェクト全てをスキップします）. パスワード保護されたパスワードに悩まされたくない場合にはこのオプションを選択します。 BitDefenderはそれらをスキャンできません。しかしログファイルに記録が残されます。

OK をクリックしてスキャンを続けます。

スキャンを停止または一時停止. 停止&はいをクリックしていつでもスキャンを停止することができます。その場合はウィザードの最後の手順に移動します。 スキャン処理を一時的に停止するには一時停止をクリックします。スキャンを再開するには再開をクリックします。

5.7.2. 手順 2/3 - アクションを選択

スキャンが完了するとスキャンの結果を示す新しいウィンドウが表示されます。



処理

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に基づくグループごとに表示されます。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。

全ての問題に対して一括した処理を行うか、もしくは個々の問題のグループごとに個別の処理を行うかを選択できます。

１つまたは複数のオプションがメニューで表示されます：

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。スキャン完了後、スキャンログを開いてこれらのファイルの情報をみることができます。

アクション	説明
ウイルスを除去	感染しているファイルからマルウェアのコードを取り除きます。
削除	検出したファイルを削除します。
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。　隔離されたファイルは実行されることも開かれることもありません。そのため感染が広がるリスクはそれ以上ありません。
ファイル名変更	隠しファイルを可視化しました。それらは.bd.ren という拡張子がファイル名に付加されています。 そのような場合には、コンピュータ内のそのようなファイルを検索することで見つけることができます。 これらの隠しファイルはWindwosからお客様が隠したものではありません。このファイルは特殊なプログラムによって隠されており、ルートキットとして知られています。 ルートキットはそのそもは悪意を持つものではありません。しかしウィルスやスパイウェアを通常のアンチウィルスプログラムでは検知されないようにするために使われることが多いです。

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ます。

5.7.3. 手順 3/3 - 結果を表示

BitDefenderによる問題の修正が終了すると、スキャンの結果が新しいウィンドウに表示されます。

概要

結果の概要を確認できます。 スキャン処理について包括的な情報をご覧になりたい場合には ログファイルを表示 をクリックしてスキャン履歴を確認してください。

重要項目
削除処理を完了するために必要に応じてシステムを再起動してください。

閉じるをクリックしてウィ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

多くの場合には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。 しかし、解決できない問題もあります。

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。

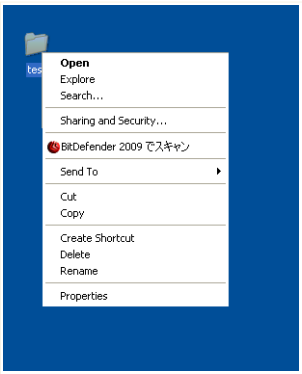
BitDefenderは疑わしいファイルを検出しました

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、BitDefender研究所へ報告するよう促されます。 OKをクリックすると詳しく分析するためにファイルがBitDefender研究所に送信されます。

5.8. Windowsコンテキストメニューへの統合

Windowsのコンテキストメニューはコンピュータ上のファイルやフォルダ、デスクトップにあるオブジェクトを右クリックすると表示されるものです。



Windowsコンテキストメニュー

BitDefenderはWindowsのコンテキストメニューと統合して、簡単にファイルのウィルススキャンをできるようになっています。 コンテキストメニューの中からBitDefenderのオプションは BitDefender のアイコンによって簡単にみつけられるはずです。

5.8.1. BitDefender 2009 でスキャン

このコンテキストメニューからファイル、フォルダそしてハードドライブ全体をスキャンすることができます。　　スキャンしたいオブジェクトを右クリックしてBitDefender 2009でスキャン をメニューから選びます。 アンチウィルススキャンウィザード ではスキャン処理についてガイドします。

スキャン・オプション. スキャンオプションは事前に最高の検出結果を得るよう設定されています。 感染ファイルを検知すると、BitDefenderは駆除（マルウェアのコードの除去）しようとします。駆除が失敗した場合には、アンチウィルススキャンウィザードは感染ファイルに対して他の処理を選択するよう聞いてきます。

スキャンオプションを変更する場合には次の手順で行います：

1. BitDefenderを開く。
2. 画面が標準設定画面の場合には詳細設定画面　ボタンをクリックしてください。画面の右上にあります。
3. 左メニューにあるアンチウィルスをクリックします。
4. ウィルススキャン タブをクリックします。
5. コンテキストスキャン タスクを右クリックして 開くを選択します。 ウィンドウが表示されます。
6. カスタムをクリックして必要におうじてスキャンオプションを選択します。 オプションの意味を知るには、その上にマウスのカーソルを重ね、画面下に表示される説明をご覧ください。
7. OKをクリックして変更を保存します。
8. OK をクリックして新しいスキャンオプションを確認して適用します。

注意
このスキャン方法においてこのオプションの変更は、どうしてもという理由がない限り行わないないでください。

5.9. ブラウザとの連携

BitDefenderはインターネットの閲覧中に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。

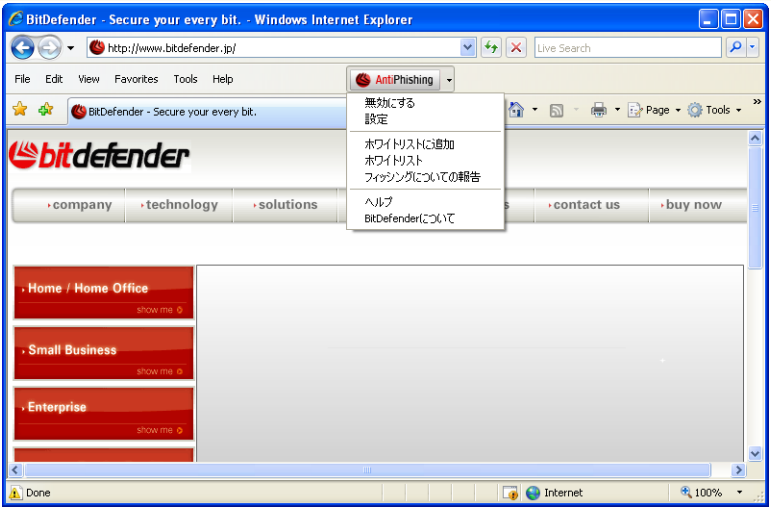
BitDefenderは分かりやすくて使いやすいツールバーから次のブラウザに組み込まれます：

■Internet Explorer
■Mozilla Firefox

ブラウザに統合された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ブラウザの上部にあります。 アイコンをクリックしてツールバーメニューを開きます。

注意
ツールバーが見つからない場合は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、以下のコマンドを使用することができます：

■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。

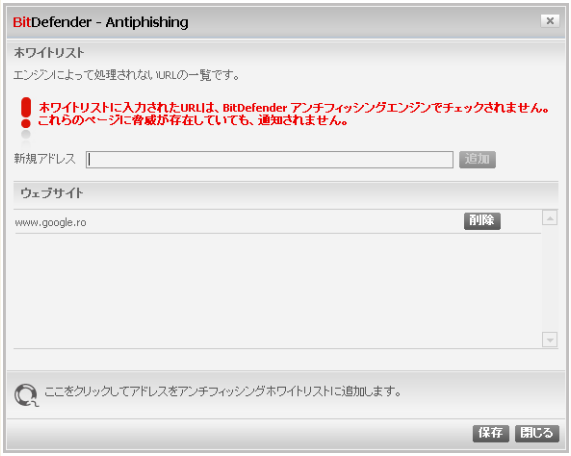
注意
アンチフィッシングツールバーを無効にすると、以降はフィッシング行為から保護されません。

■設定 - アンチフィッシングツールバーの設定項目を指定するウィンドウが開きます。 以下のオプションを指定できます：
- リアルタイム　アンチフィッシングウェブプロテクション　-　ウェブサイトがフィッシングサイトである(個人情報取得のために開設）かをリアルタイムで検出して警告を発します。　このオプションはBitDefenderアンチフィッシングプロテクションを現在のウェブブラウザにおいてのみコントロールします。
- 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ユーザに確認します。

■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。



アンチフィッシングのホワイトリスト

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一覧を確認することができます。　ホワイトリストから特定のサイトを削除して、そのページにフィッシングの脅威があれば警告するようにするには、横にある削除ボタンをクリックします。

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て追加をクリックします。

■フィッシングとして報告 - BitDefender研究所に該当のウェブサイトがフィッシングサイトの疑いがあると報告します。 フィッシングサイトを報告することは、他の人を、個人情報盗難から守るのに役立ちます。

■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ィンドウが開きます。

5.10. インスタントメッセンジャープログラムへの統合

BitDefenderでは重要なドキュメントやYahoo! MessengerやMSNメッセンジャーでの会話を暗号化することができます。

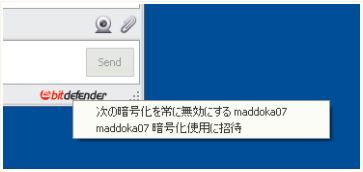
初期設定ではBitDefenderは全てのインスタントメッセンジャーでの会話を暗号化します：

■インスタントメッセンジャーの相手がBitDefenderのIM暗号化をサポートしているバージョンを使用している必要があります。

■Yahoo! Messenger（英語版）かMSN Messengerを使用する必要があります。

重要項目
BitDefenderはもし相手がウェブベースのチャットアプリケーションを使用している場合、例えば、MeeboやYahoo Messengerや他のMSNをサポートするチャットアプリケーションでは会話を暗号化しません。

インスタントメッセンジャーの暗号化はチャットウィンドウにあるBitDefenderツールバーから簡単に設定することができます。 ツールバーはチャットウィンドウの右下に表示されます。BitDefenderのロゴがみつけてください。



BitDefenderツールバー

注意
ツールバーは会話が暗号化されているかどうか小さな鍵マークを表示することで示しています。 BitDefenderロゴの隣にあります。

BitDefenderツールバーを右クリックすると、以下のようなオプションが設定できます：

■恒久的に次の コンタクト では暗号化を無効にする.

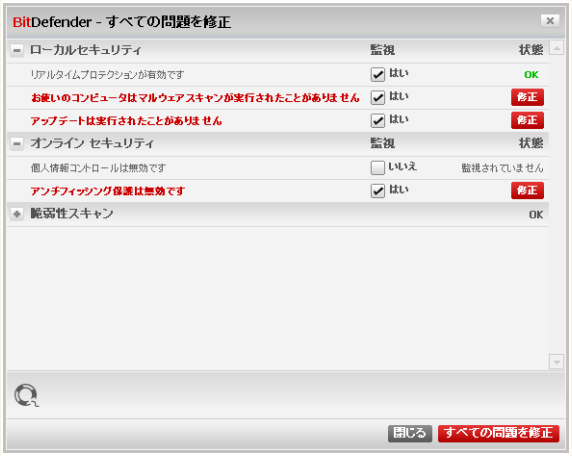
■コンタクト先 を暗号化に招待する. 会話を暗号化するためにはコンタクト先もBitDefenderがインストールされており対応したIMプログラムを使用している必要があります。

この中からどれかのオプションを選択してください。

6. 問題を修正

BitDefender Antivirus 2009のウィンドウ上部に解決すべき項目数をわかりやすく表示しています。全てを解決するボタンをクリックするとセキュリティステータスウィンドウが表示され、セキュリティに関する問題点をすべて解決することができます。

注意
もしシステムにセキュリティ上の問題がなければステータスバーは緑です。



ステータスバー

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 Antivirus 2009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。

6.1. ローカルセキュリティ

お使いのコンピュータのセキュリティに影響を与えるような問題は、どんな場合でも認識しておくことが重要です。各セキュリティモジュールを監視することによって、BitDefender Total Security 2009は、あなたが設定を構成してコンピュータセキュリティに影響を与えようとしているときだけではなく、あなたが重要なタスクを忘れてしまっているときでも、それをお知らせします。

ローカルセキュリティに関する問題はとてもわかりやすく表示されます。何かセキュリティ上の問題があると思われる項目については赤い修正ボタンが表示されます。問題がない場合には緑のOKボタンが表示されます。

問題	説明
リアルタイムプロテクションが有効です	このコンピュータで動くアプリケーションやそれらがアクセスするすべてのファイルをスキャンします。
マルウェアスキャンをこれまでに実行していません	マルウェアを除去するためにオンデマンドスキャンを至急行うことを強くお勧めいたします。
自動アップデートは無効です	最新のマルウェアに対応するためにBitDefenderの自動アップデートは有効にしたままにしておいてください。
アップデートは x 日間実行されていません	BitDefenderをただちにアップデートしてください。BitDefenderを常に最新にしておくことで、コンピュータをインターネット上の最新のマルウェアから守ることができます。
アップデート	製品とシグネチャの更新が実行されています。
製品はアクティベートされていません	製品をアクティベートするためには、BitDefenderアカウントの作成が必要です。

ステータスボタンが緑の時はセキュリティリスクは最低になっています。ボタンをグリーンにするためには、以下の手順を行います：

1. 修正 - セキュリティの脆弱性を除去する手助けをします。
2. 問題がその場で修正されない場合にはウィザードに沿って修正してください。

監視対象から例外としたい問題があれば、 監視 列にあるチェックボックスをクリアします。

6.2. オンライン セキュリティ

オンライン セキュリティの問題はとてもわかりやすく表示されます。何かセキュリティ上の問題があると思われる項目については、赤い修正ボタンが表示されます。問題がない場合には緑のOKボタンが表示されます。

問題	説明
個人情報コントロールは有効	重要データが安全に保たれるように、全てのWEBとメール通信上に特定の文字列がないかをスキャンします。個人情報保護コントロールを有効にして、重要なデータ（メール、住所、ユーザID、パスワード、クレジットカード番号など）を安全に、盗まれることがないようにされることをお勧めします。
アンチフィッシングプロテクションは有効です	BitDefenderはインターネットの閲覧中にフィッシング行為から守ります。

ステータスボタンが緑の時はセキュリティリスクは最低になっています。ボタンをグリーンにするためには、以下の手順を行います：

1. 修正 - セキュリティの脆弱性を除去する手助けをします。
2. 問題がその場で修正されない場合にはウィザードに沿って修正してください。

監視対象から例外としたい問題があれば、 監視 列にあるチェックボックスをクリアします。

6.3. 脆弱性スキャン

脆弱性に関する問題はとてもわかりやすく表示されます。何かセキュリティ上の問題があると思われる項目については、赤い修正ボタンが表示されます。 問題がない場合には緑のOKボタンが表示されます。

問題	説明
脆弱性チェックが有効です	Microsoft Windows UpdatesやMicrosoft Windows Office Updatesを監視し、さらにはMicrosoft Windowsアカウントのパスワードに脆弱性がないか確認します。
クリティカルなMicrosoft updates	クリティカルでインストール可能なMicrosoft updates
その他のMicrosoft updates	クリティカルでないがインストール可能なMicrosoft updates
Windows自動アップデートが有効です	新しいWindows security updatesが利用できるようになり次第、インストールを行います。
Yahoo! Messenger（古い）	最新のYahoo! Messengerをできるだけはやくインストールしてください。
Winamp（古い）	最新のWinamp をできるだけはやくインストールしてください。
Firefox（古い）	最新のFirefox をできるだけはやくインストールしてください。
管理者(強いパスワード)	指定されたユーザアカウントのパスワード強度が表示されます。 パスワードは 堅固（推測困難）にも 脆弱(容易に悪意をもった人々の特化したソフトウェアにより類推可能)にもなりえます。

ステータスボタンが緑の時はセキュリティリスクは最低になっています。ボタンをグリーンにするためには、以下の手順を行います：

1. 修正 - セキュリティの脆弱性を除去する手助けをします。
2. 問題がその場で修正されない場合にはウィザードに沿って修正してください。

監視対象から例外としたい問題があれば、 監視 列にあるチェックボックスをクリアします。

7. 基本設定画面タブ

基本設定画面はシンプルなインターフェイスでセキュリティ問題を監視、修正が簡単に行えます。またコンピュータの防御処理も行うことができます。 基本設定画面は複数のタブで構成されています：

タブ	説明
ダッシュボード	重要な製品に関する統計情報および製品登録状況、重要なオンデマンドタスクの状況が表示されます。
アンチウイルス	BitDefenderの更新およびウィルスの感染などアンチウィルスモジュールの状況が表示されます。
アンチフィッシング	オンライン時にフィッシング攻撃（個人情報盗難）から守るモジュールのステータスをあらわしています。
脆弱性	脆弱性モジュールはお使いのソフトウェアを最新版に保つために役立ちます。 ここでコンピュータのセキュリティに影響する脆弱性の問題を簡単に修復できます。
ネットワーク	BitDefenderネットワークを表示する。 ここではホームネットワークに参加しているBitDefender製品のさまざまな設定や管理を行うことができます。 このようにして、ホームネットワーク内のセキュリティを、1台のコンピュータから管理することができます。

7.1. ダッシュボード

ダッシュボードタブをクリックすると重要な製品に関する統計情報や重要なオンデマンドタスクの登録状況を見ることができます。

ダッシュボード

この文書はいくつかの大きな章に分かれています。

■状態 – 問題がコンピュータにある場合に警告して、その修復を手助けします。

■概要 – アップデート状況、登録、ライセンス情報を表示します。

■タスク – もっとも重要なセキュリティタスクへのリンク：フルシステムスキャン、完全スキャン、今すぐアップデート。

7.1.1. 概要

ここではアップデート状況、登録、ライセンス情報などをまとめて確認することができます。

アイテム	説明
登録	ライセンスキーのタイプと状況が表示されます。システムのセキュリティを維持し続けるためには、ライセンスの有効期

アイテム	説明
	限が切れている場合は、BitDefender Antivirus 2009を新しくするか更新する必要があります。
有効期限	ライセンス期限が切れるまでの日数 ライセンスキーが残りわずかで切れる場合には、製品を新しいキーで登録してください。 ライセンスキーの購入またはライセンスの更新には、購入/更新 リンクをクリックします。画面下にこのリンクはあります。
マイアカウント	BitDefenderから提供されるサービスやサポート、有用な情報、ライセンスキーをなくしたときなどに利用するBitDefenderアカウントのメールアドレスが表示されます。 製品をアクティベートするためにアカウントを作成する必要があります。BitDefenderアカウントについては次を参照してください。「BitDefenderアカウントの作成方法」 (p. 225).
直前のアップデート	BitDefenderがいつ最後にアップデートされたがを示しています。 完全にシステムを守るために定期的なアップデートを実行してください。
前回のスキャン	前回いつコンピュータがスキャンされたかを示しています。もし前回のスキャンが１週間以上前に実施されたものなら、できるだけはやい機会にスキャンを行ってください。

7.1.2. タスク一覧

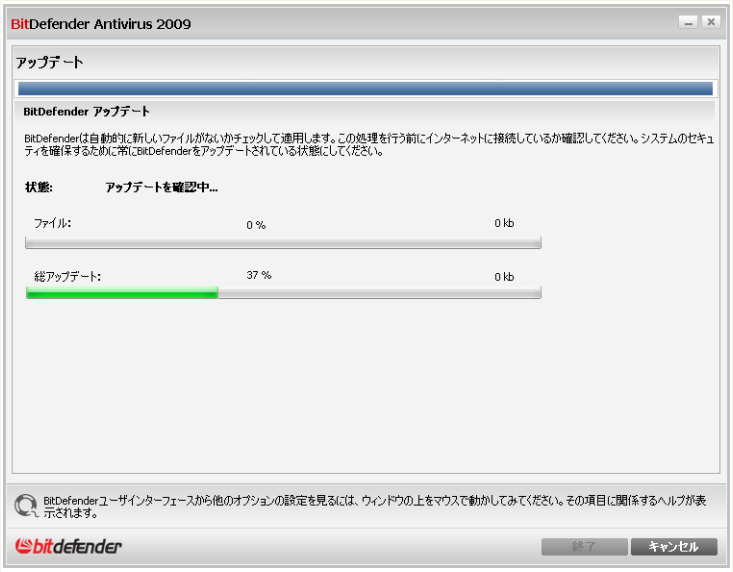
ここにはもっとも重要なセキュリティタスクのリンクがあります：

- アップデート - すぐにアップデートを開始します。
- フルシステムスキャン - 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。
- ディープシステムスキャン - 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。

BitDefenderのアップデート

毎日のように新しいマルウェアが発生・検出されており、それに対処するにはBitDefenderを最新のマルウェアのシグネチャで更新することがとても重要です。

デフォルトでは、コンピュータの起動時とその後は１時間ごとにBitDefenderがアップデートをチェックします。 しかし、ユーザがBitDefenderをアップデートしたい場合は、今すぐアップデートをクリックするだけです。 アップデート処理が開始され、すぐに以下のウィンドウが表示されます：



BitDefenderのアップデート

このウィ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。 しかし、ウィンドウを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場合は、ユーザ要求によってBitDefenderのアップデートを定期的に行うことをお勧めします。

必要に応じてコンピュータを再起動します。. 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。

あとでシステムを再起動するにはOKをクリックします。 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。

BitDefenderによるスキャン

マルウェアを対象にコンピュータをスキャンするには、該当のボタンをクリックして特定のスキャンタスクを実行します。 以下の表に、使用可能なスキャンタスクと簡単な説明を示します：

タスク	説明
フルシステムスキャン	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 などシステムのセキュリティを脅かす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	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 などシステムのセキュリティを脅かすあらゆる種類のマルウェアをスキャンします。

注意
完全システムスキャンとフル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、スキャン処理に時間がかかります。従って、これらのタスクは優先度を低くして実行するか、できればシステムが使われていない時に実行することをお勧めします。

スキャンを開始すると、アンチウィルススキャンウィザードが表示されます。 以下の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。 詳細については次を参照してください。 「アンチウィルススキャンウィザード」 (p. 39)

7.2. アンチウイルス

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。 アンチウィルスモジュールに入るにはアンチウィルスタブをクリックしてください。

アンチウイルス

アンチウィルスモジュールは２つのセクションで構成されています。

- 監視済みコンポーネント - 監視済みのコンポーネントの全てのリストを確認できます。 どのコンポーネントを監視するか選択できます。すべてを監視するようにおすすめします。
- タスク - もっとも重要なセキュリティタスクへのリンクがあります：フルシステムスキャン、完全スキャン、アップデート

7.2.1. 監視されているコンポーネント

監視されているコンポーネントは１つのカテゴリでまとめられています：ローカルセキュリティ. ここで各セキュリティモジュール、コンピュータに格納されているオブジェクト（ファイル、レジストリ、メモリなど）を保護するモジュールの状態を監視できます。

"+" が付いたボックスをクリックするとカテゴリが開き、"-" をクリックすると閉じます。

ローカルセキュリティ

お使いのコンピュータのセキュリティに影響を与えるような問題は、どんな場合でも認識しておくことが重要です。各セキュリティモジュールを監視することによって、BitDefender Total Security 2009は、あなたが設定を構成してコンピュータセキュリティに影響を与えようとしているときだけではなく、あなたが重要なタスクを忘れてしまっているときでも、それをお知らせします。

ローカルセキュリティに関する問題はとてもわかりやすく表示されます。何かセキュリティ上の問題があると思われる項目については赤い修正ボタンが表示されます。問題がない場合には緑のOKボタンが表示されます。

問題	説明
リアルタイムプロテクションが有効です	このコンピュータで動くアプリケーションやそれらがアクセスするすべてのファイルをスキャンします。
マルウェアスキャンをこれまでに実行していません	マルウェアを除去するためにオンデマンドスキャンを至急行うことを強くお勧めいたします。
自動アップデートは無効です	最新のマルウェアに対応するためにBitDefenderの自動アップデートは有効にしたままにしておいてください。
アップデートは x 日間実行されていません	BitDefenderをただちにアップデートしてください。BitDefenderを常に最新にしておくことで、コンピュータをインターネット上の最新のマルウェアから守ることができます。
アップデート	製品とシグネチャの更新が実行されています。
製品はアクティベートされていません	製品をアクティベートするためには、BitDefenderアカウントの作成が必要です。

ステータスボタンが緑の時はセキュリティリスクは最低になっています。ボタンをグリーンにするためには、以下の手順を行います：

1. 修正 - セキュリティの脆弱性を除去する手助けをします。
2. 問題がその場で修正されない場合にはウィザードに沿って修正してください。

監視対象から例外としたい問題があれば、 監視 列にあるチェックボックスをクリアします。

7.2.2. タスク一覧

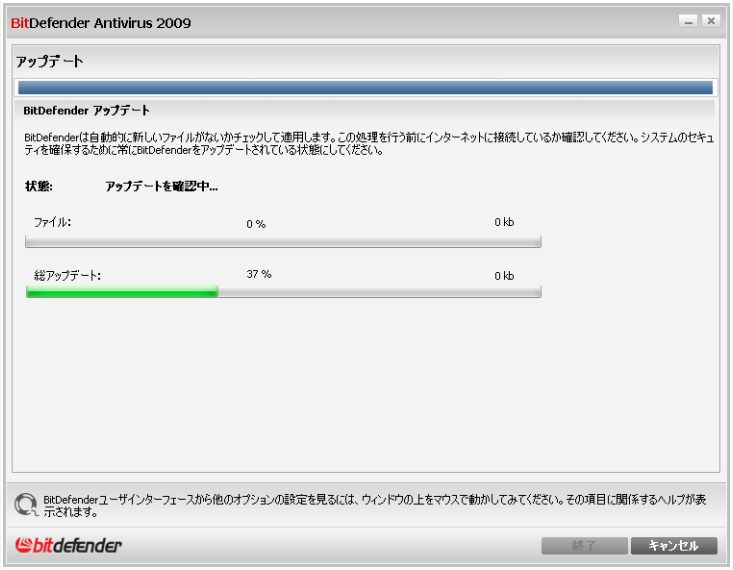
ここにはもっとも重要なセキュリティタスクのリンクがあります：

- アップデート - すぐにアップデートを開始します。
- マイドキュメントスキャン - 文書と設定のクイックスキャンを開始します。
- フルシステムスキャン - 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。
- ディープシステムスキャン - 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。

BitDefenderのアップデート

毎日のように新しいマルウェアが発生・検出されており、それに対処するにはBitDefenderを最新のマルウェアのシグネチャで更新することがとても重要です。

デフォルトでは、コンピュータの起動時とその後は１時間ごとにBitDefenderがアップデートをチェックします。 しかし、ユーザがBitDefenderをアップデートしたい場合は、今すぐアップデートをクリックするだけです。 アップデート処理が開始され、すぐに以下のウィンドウが表示されます：



BitDefenderのアップデート

このウィ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。 しかし、ウィンドウを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場合は、ユーザ要求によってBitDefenderのアップデートを定期的に行うことをお勧めします。

必要に応じてコンピュータを再起動します。. 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。

あとでシステムを再起動するにはOKをクリックします。 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。

BitDefenderによるスキャン

マルウェアを対象にコンピュータをスキャンするには、該当のボタンをクリックして特定のスキャンタスクを実行します。 以下の表に、使用可能なスキャンタスクと簡単な説明を示します：

タスク	説明
マイドキュメントスキャン	重要なカレントユーザのフォルダをスキャンするにはこのタスクを使用します：マイドキュメント，デスクトップ，スタートアップ　これにより文書、ワークスペース、起動時に実行するアプリケーションの安全性が確保されます。
フルシステムスキャン	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 などシステムのセキュリティを脅かす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	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 などシステムのセキュリティを脅かすあらゆる種類のマルウェアをスキャンします。

注意
完全システムスキャンとフル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、スキャン処理に時間がかかります。従って、これらのタスクは優先度を低くして実行するか、できればシステムが使われていない時に実行することをお勧めします。

スキャンを開始すると、アンチウィルススキャンウィザードが表示されます。 以下の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。 詳細については次を参照してください。 「アンチウィルススキャンウィザード」 (p. 39)

7.3. アンチフィッシング

BitDefenderのアンチフィッシングモジュールはInternet ExplorerやFirefox経由でアクセスする全てのページを安全にします。 アンチフィッシングモジュールに入るにはアンチフィッシングタブをクリックしてください。

アンチフィッシング

アンチフィッシングモジュールは２つのセクションから構成されています。

■監視済みコンポーネント - 監視済みのコンポーネントの全てのリストを確認できます。 どのコンポーネントを監視するか選択できます。すべてを監視するようにおすすめします。

■タスク - もっとも重要なセキュリティタスクへのリンクがあります：フルシステムスキャン、完全スキャン、アップデート

7.3.1. 監視されているコンポーネント

監視されているコンポーネントは１つのカテゴリでまとめられています：オンラインセキュリティ．ここで各モジュールの状況、インターネット接続時にオンライントランザクションやコンピュータの防御状況を確認できます。

"+" が付いたボックスをクリックするとカテゴリが開き、"-" をクリックすると閉じます。

オンライン セキュリティ

オンライン セキュリティの問題はとてもわかりやすく表示されます。何かセキュリティ上の問題があると思われる項目については、赤い修正ボタンが表示されます。問題がない場合には緑のOKボタンが表示されます。

問題	説明
個人情報コントロールは有効	重要データが安全に保たれるように、全てのWEBとメール通信上に特定の文字列がないかをスキャンします。個人情報保護コントロールを有効にして、重要なデータ（メール、住所、ユーザID、パスワード、クレジットカード番号など）を安全に、盗まれることがないようにされることをお勧めします。
アンチフィッシングプロテクションは有効です	BitDefenderはインターネットの閲覧中にフィッシング行為から守ります。

ステータスボタンが緑の時はセキュリティリスクは最低になっています。ボタンをグリーンにするためには、以下の手順を行います：

1. 修正 - セキュリティの脆弱性を除去する手助けをします。
2. 問題がその場で修正されない場合にはウィザードに沿って修正してください。

監視対象から例外としたい問題があれば、 監視 列にあるチェックボックスをクリアします。

7.3.2. タスク一覧

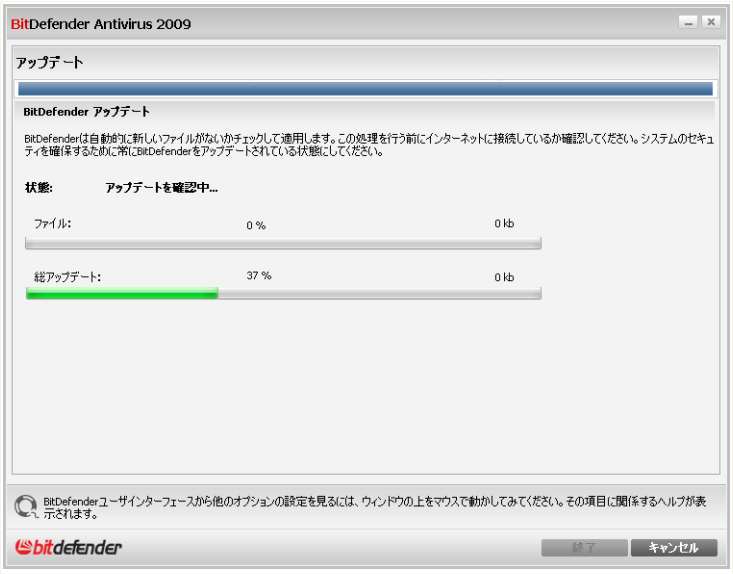
ここにはもっとも重要なセキュリティタスクのリンクがあります：

■アップデート – すぐにアップデートを開始します。
■フルシステムスキャン – 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。
■ディープシステムスキャン – 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。

BitDefenderのアップデート

毎日のように新しいマルウェアが発生・検出されており、それに対処するにはBitDefenderを最新のマルウェアのシグネチャで更新することがとても重要です。

デフォルトでは、コンピュータの起動時とその後は１時間ごとにBitDefenderがアップデートをチェックします。 しかし、ユーザがBitDefenderをアップデートしたい場合は、今すぐアップデートをクリックするだけです。 アップデート処理が開始され、すぐに以下のウィンドウが表示されます：



BitDefenderのアップデート

このウィ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。 しかし、ウィンドウを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場合は、ユーザ要求によってBitDefenderのアップデートを定期的に行うことをお勧めします。

必要に応じてコンピュータを再起動します。. 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。

あとでシステムを再起動するにはOKをクリックします。 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。

BitDefenderによるスキャン

マルウェアを対象にコンピュータをスキャンするには、該当のボタンをクリックして特定のスキャンタスクを実行します。 以下の表に、使用可能なスキャンタスクと簡単な説明を示します：

タスク	説明
フルシステムスキャン	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 などシステムのセキュリティを脅かす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	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 などシステムのセキュリティを脅かすあらゆる種類のマルウェアをスキャンします。

注意
完全システムスキャンとフル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、スキャン処理に時間がかかります。従って、これらのタスクは優先度を低くして実行するか、できればシステムが使われていない時に実行することをお勧めします。

スキャンを開始すると、アンチウィルススキャンウィザードが表示されます。 以下の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。 詳細については次を参照してください。 「アンチウィルススキャンウィザード」 (p. 39)

7.4. 脆弱性

BitDefenderの脆弱性モジュールはお使いのソフトウェアを最新版に保つために役立ちます。 システムの脆弱性を監視修正するには脆弱性 タブをクリックします。

脆弱性

脆弱性モジュールは２つのセクションから構成されています。

- 監視されているコンポーネント - BitDefenderによって監視されている潜在的な脆弱性を持つコンポーネントの全てのリストを確認できます。 どの脆弱性について通知させるか選択できます。ただすべてを監視するようにおすすめします。
- タスク - ここにはもっとも重要なセキュリティタスクのリンクがあります。

7.4.1. 監視されているコンポーネント

１つの監視コンポーネントがあります： 脆弱性スキャン. ここではお使いのソフトウェアが最新かどうかチェックすることができます。Windowsアカウントのパスワードがセキュリティルールにそっているかどうかもチェックします。

"+" が付いたボックスをクリックするとカテゴリが開き、"-" をクリックすると閉じます。

脆弱性スキャン

脆弱性に関する問題はとてもわかりやすく表示されます。何かセキュリティ上の問題があると思われる項目については、赤い修正ボタンが表示されます。 問題がない場合には緑のOKボタンが表示されます。

問題	説明
脆弱性チェックが有効です	Microsoft Windows UpdatesやMicrosoft Windows Office Updatesを監視し、さらにはMicrosoft Windowsアカウントのパスワードに脆弱性がないか確認します。
クリティカルなMicrosoft updates	クリティカルでインストール可能なMicrosoft updates
その他のMicrosoft updates	クリティカルでないがインストール可能なMicrosoft updates
Windows自動アップデートが有効です	新しいWindows security updatesが利用できるようになり次第、インストールを行います。
Yahoo! Messenger （古い）	最新のYahoo! Messengerをできるだけはやくインストールしてください。
Winamp （古い）	最新のWinamp をできるだけはやくインストールしてください。
Firefox （古い）	最新のFirefox をできるだけはやくインストールしてください。
管理者(強いパスワード)	指定されたユーザアカウントのパスワード強度が表示されます。 パスワードは 堅固（推測困難）にも 脆弱

問題	説明
	(容易に悪意をもった人々の特化したソフトウェアにより類推可能)にもなりえます。

ステータスボタンが緑の時はセキュリティリスクは最低になっています。ボタンをグリーンにするためには、以下の手順を行います：

1. 修正 - セキュリティの脆弱性を除去する手助けをします。
2. 問題がその場で修正されない場合にはウィザードに沿って修正してください。

監視対象から例外としたい問題があれば、 監視 列にあるチェックボックスをクリアします。

7.4.2. タスク一覧

１つのテスクだけが利用できます：

■脆弱性スキャン - ウィザードを開始してシステム上の脆弱性をチェックして修正するようガイドします。

脆弱性の検索

脆弱性スキャンはMicrosoft Windows UpdatesやMicrosoft Windows Office Updatesのチェックと Microsoft Windowsアカウントのパスワードに脆弱性がないか確認します。

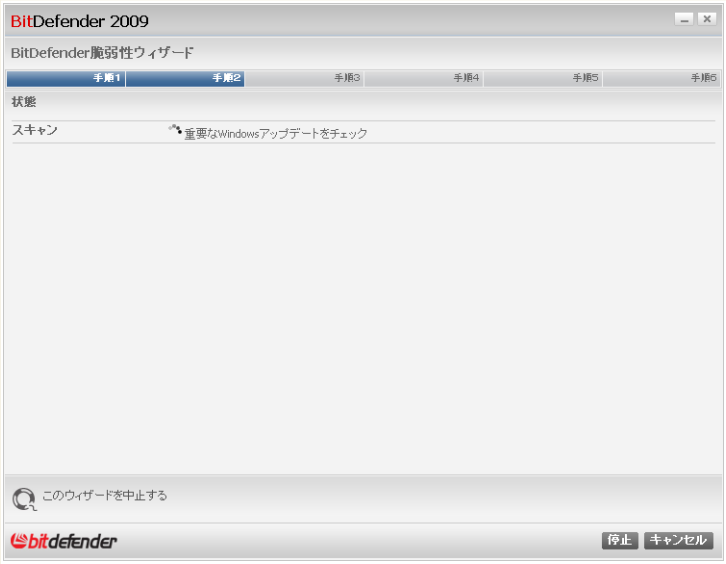
コンピュータの脆弱性をチェックするには脆弱性スキャンをクリックし、ウィザードの通りに進めます。

手順 1/6 - 脆弱性チェックを選択

脆弱性

次にをクリックし選択した脆弱性チェックを行います。

手順 2/6 - 脆弱性チェック



脆弱性チェック

BitDefenderが脆弱性チェックを完了するまでお待ちください。

手順3/6 - Windowsをアップデートする

Windowsアップデート

このコンピュータにインストールされていないアップデート、クリティカルなアップデート、クリティカルではないアップデートがそれぞれ表示されます。　全てのアップデートをインストールするをクリックすると、インストール可能な全てのアップデートをインストールします。

次へをクリックします。

手順 4/6 - アプリケーションのアップデート

アプリケーション

BitDefenderがアップデートが必要なアプリケーションをチェックしリストを作成します。 もしアプリケーションが最新でない場合には、最新版をダウンロードするをクリックします。

次へをクリックします。

手順5/6 - 弱いパスワードを変更

パスワードを入力

このコンピュータのWindowsアカウントに設定されているパスワードに脆弱性がないか確認することができます。 パスワードは 堅固（推測困難）にも 脆弱（容易に悪意をもった人々の特化したソフトウェアにより類推可能)にもなりえます。

修正をクリックして弱いパスワードを変更します。 新しいウィンドウが開きます。

パスワードを変更

この問題を修正する方法を選択してください：

■次のログイン時に強制的にパスワード変更. BitDefenderはユーザが次にWindowsにログインするときにパスワード変更するようにプロンプトを表示します。

■パスワード変更. 入力欄に新しいパスワードを入力します。 パスワード変更するようユーザに通知する

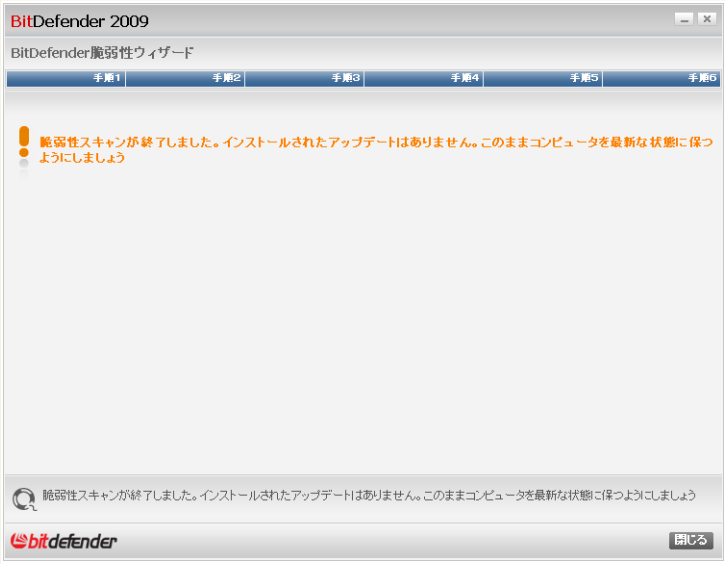
注意

強いパスワードを作るためには、大文字と小文字を混ぜる、数字と記号 （例えば #, $, @）を使います。 堅固なパスワードについてはインターネットを検索すると様々な役立つ情報があります。

OKをクリックするとパスワードが変更されます。

次へをクリックします。

手順 6/6 - 結果を表示する

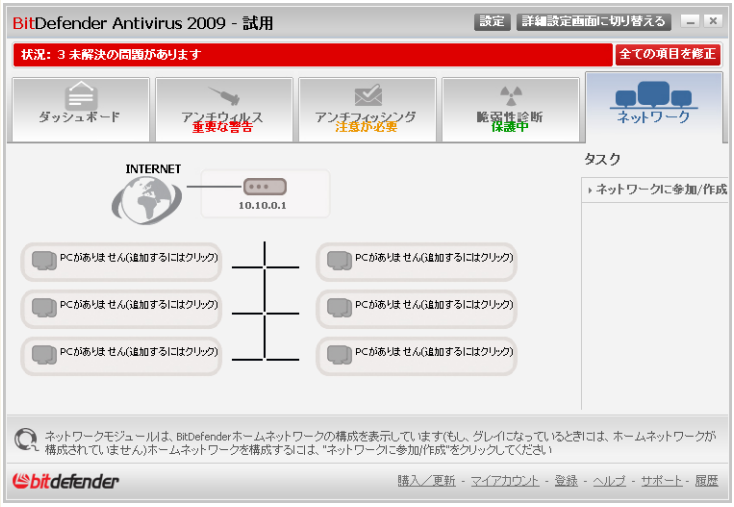


結果

閉じるをクリックします。

7.5. ネットワーク

ネットワークモジュールを使うとBitDefender製品がインストールされているご家庭内のコンピュータを一元管理することができます。 ネットワークモジュールに入るには、 the ネットワーク タブをクリックします。



ネットワーク

BitDefender製品がインストールされている家庭内のコンピュータを管理するには、次の手順を行ってください：

1. コンピュータからBitDefenderネットワークに参加する ネットワークに加わるためにはホームネットワーク管理のための管理者パスワードを必要とします。
2. 管理したいコンピュータをそれぞれネットワークに参加させます(パスワードを設定してください)
3. コンピュータに戻って管理したいコンピュータを追加してください

7.5.1. タスク一覧

最初の状態では１つのボタンが使用できるだけです。

■ネットワークに参加する/つくる - ネットワークパスワードを設定してネットワークに参加します。

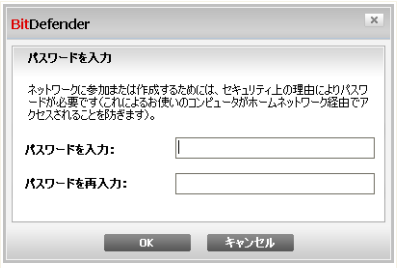
ネットワークに参加すると、さらにいくつかのボタンが表示されます。

■ネットワークを離脱する - ネットワークから離脱します。
■コンピュータを追加 - ネットワークにコンピュータを追加します。
■全てをスキャン - 同時にネットワークに参加している全てのコンピュータをスキャンします。
■全てをアップデートする - 同時にネットワークに参加している全てのコンピュータをアップデートします。
■全てを登録する - 同時にネットワークに参加している全てのコンピュータを登録します。

BitDefenderネットワークに参加する

BitDefender home networkに参加するには、以下の手順に従ってください：

1. ネットワークに参加する/つくるをクリックする ホームネットワークを管理するパスワードを決めます。



パスワード設定

2. それぞれの入力欄に同じパスワードを入力します。
3. OKをクリックします。

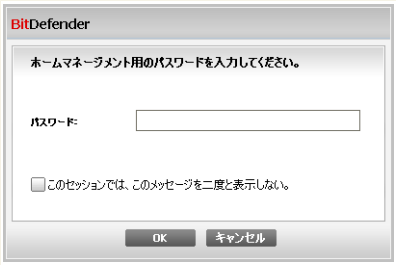
ネットワークマップ上にコンピュータ名が表示されます。

BitDefenderネットワークにコンピュータを追加する

BitDefenderホームネットワークにコンピュータを追加するには、はじめにBitDefenderホームネットワークを管理するためのパスワードを個々のコンピュータへ設定しなければなりません。

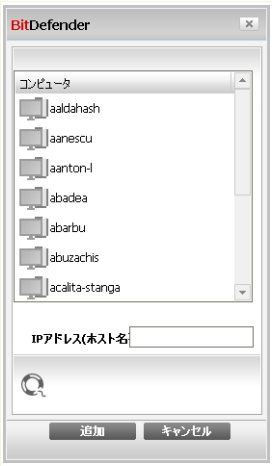
BitDefenderホームネットワークにコンピュータを追加するには、次の手順を行ってください：

1. ネットワークを管理するをクリックしてください。 ホームネットワークを管理するためのパスワードを決めます。



パスワードを入力

2. ホームネットワークを管理するパスワードを入力してOKをクリックします。 新しいウィンドウが開きます。

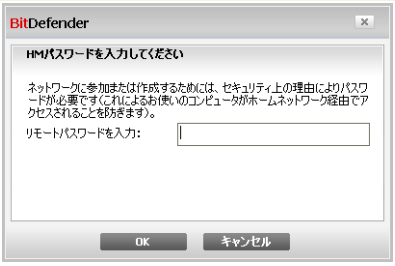


コンピュータを追加

ネットワークに参加しているコンピュータの一覧を確認できます。　アイコンの意味は次の通りです：

- オンラインでBitDefenderがインストールされていないコンピュータ
- オンラインでBitDefenderがインストールされているコンピュータ
- オフラインでBitDefenderがインストールされているコンピュータ

3. 以下のいずれかを実行します：
   - ネットワークに追加するコンピュータ名を選択します
   - IPアドレスかコンピュータ名を入力します。
4. 追加をクリックします。　それぞれのコンピュータを管理するパスワードを決めます。



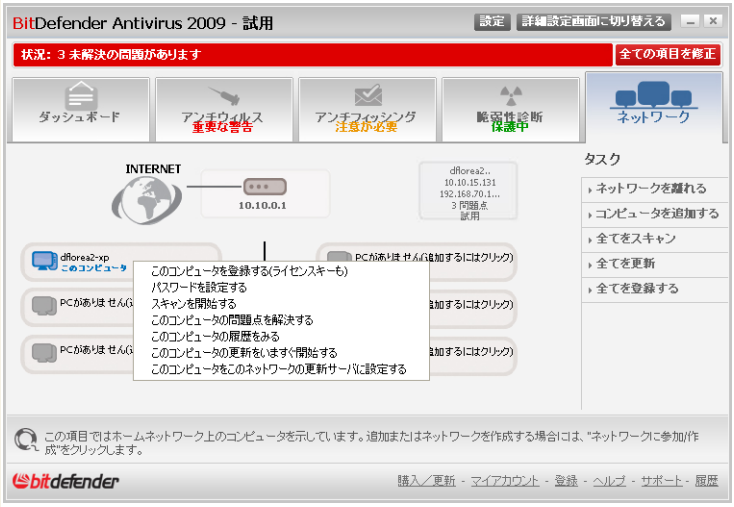
認証

5. ホームネットワーク管理者パスワードはそれぞれのコンピュータに設定します。
6. OKをクリックします。　正しいパスワードを入力すると選択したコンピュータがネットワークマップに表示されます。

注意
コンピュータを最大５台までネットワークマップに追加することができます。

BitDefenderネットワークを管理する

BitDefenderホームネットワークを作成すると１台のコンピュータから全てのBitDefender製品を管理することができます。



ネットワークマップ

ネットワークマップ上のコンピュータにマウスカーソルを当てるとコンピュータ名・IPアドレス・セキュリティに関する問題点の数・BitDefender製品登録の状態などの情報を見ることができます。

ネットワークマップのコンピュータ名の上で右クリックをするとリモートのコンピュータに対して管理作業を行うことができます。

■このコンピュータを登録

■パスワードの設定

■スキャンを実行

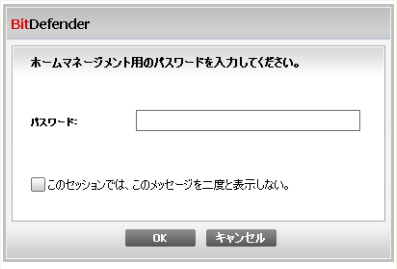
■このコンピュータの問題点を修正

■このコンピュータの履歴を表示

■このコンピュータをすぐにアップデートする

■このコンピュータをこのネットワークのアップデートサーバにする

特定のコンピュータでタスクを実行する前に管理用のパスワードを入力する必要があります。



パスワードを入力

ホームネットワークを管理するパスワードを入力してOKをクリックします。

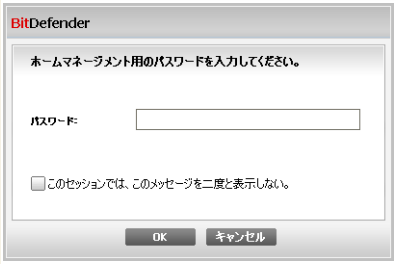
注意

いくつかのタスクを実行させる場合には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。　このオプションを選択した場合には、このセッションの間にもう一度パスワードを入力する必要があります。

全てのコンピュータのスキャン

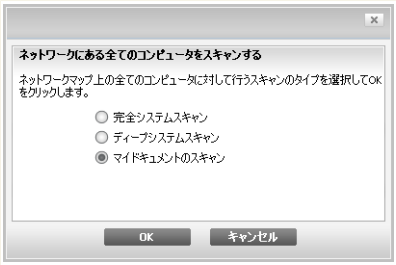
全ての管理しているコンピュータをスキャンするには、以下の手順を行います：

1. 全てをスキャンをクリックしてください。　ホームネットワークを管理するためのパスワードを決めます。



パスワードを入力

2. スキャンタイプを選択します
   - フルシステムスキャン – 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。
   - ディープシステムスキャン – 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。
   - マイドキュメントをスキャン – 文書と設定のクイックスキャンを開始します。



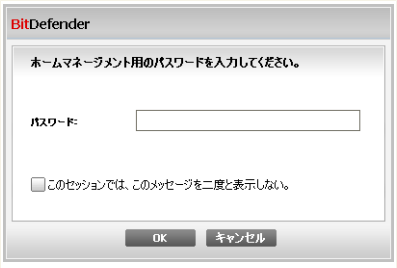
スキャンタイプを選択

3. OKをクリックします。

全てのコンピュータをアップデートする

全てのコンピュータをアップデートするには、以下の手順に従ってください：

1. 全てをアップデートをクリックしてください。　ホームネットワークを管理するためのパスワードを決めます。



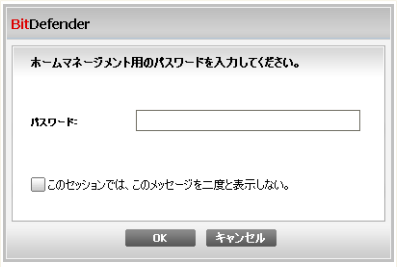
パスワードを入力

2. OKをクリックします。

全てのコンピュータを登録する

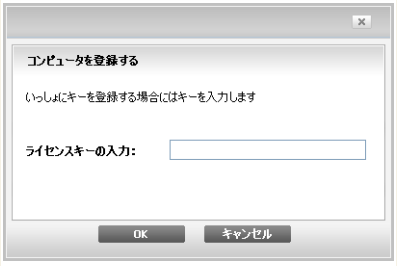
全てのコンピュータを登録するには、以下の手順に従ってください：

1. 全てを登録するをクリックしてください。　ホームネットワークを管理するためのパスワードを決めます。



パスワードを入力

2. 一緒にキーを登録する場合にはキーを入力します



全PCを登録

3. OKをクリックします。

8. クイック有効／無効設定

基本設定モジュールは重要なセキュリティモジュールの有効化/無効化を簡単に設定することができます。　基本設定モジュールの入るには上部にある設定リンクをクリックします。 システムトレイ上のBitDefenderアイコンを右クリックして 基本設定を選択します。

警告

リアルタイムアンチウィルスプロテクションや自動アップデートを無効にすることは注意して行ってください。　これらの機能を無効にすることはコンピュータのセキュリティを危険にするかもしれません。本当に無効にする必要がある場合は、できるだけはやく有効にするようにしてください。

基本設定

セキュリティモジュールはいくつかのカテゴリーがあります。

カテゴリ	説明
ローカルセキュリティ	この項ではリアルタイムプロテクションを有効または無効にすることができます。
オンライン セキュリティ	この項ではリアルタイムプロテクションを有効または無効にすることができます。
一般設定	ここにはゲームモード・ノートＰＣモードの有効化/無効化、パスワード、スキャンアクティビティバーなどがあります。

"+"が付いたボックスをクリックするとカテゴリが開き、"-"をクリックすると閉じます。

8.1. ローカルセキュリティ

ワンクリックでセキュリティモジュールの有効化/無効化ができます。

セキュリティモジュール	説明
リアルタイムアンチウィルス＆アンチスパイウェアプロテクション	リアルタイムファイルプロテクションはアプリケーションがアクセスするファイル全てをスキャンします。
自動アップデート	自動アップデートは基本機能として最新のBitDefender製品とシグネチャをダウンロードしインストールします。
自動脆弱性チェック	自動脆弱性チェックはあなたのPCの上の重要なソフトウェアが確実に最新になるようにします。

8.2. オンライン セキュリティ

ワンクリックでセキュリティモジュールの有効化/無効化ができます。

セキュリティモジュール	説明
リアルタイムアンチウィルス & アンチスパイウェア Webプロテクション	リアルタイムwebプロテクションは、HTTPでダウンロードされる全てのファイルにウィルスやスパイウェアがないかチェックします。
リアルタイム アンチフィッシング ウェブプロテクション	リアルタイム アンチフィッシング ウェブプロテクションは、あるページが個人情報を盗もうとしていることをリアルタイムに検知して警告します。
個人情報コントロール	個人情報コントロールはウェブやメールに特定の文字列が含まれていないかチェックし個人情報の漏洩を防ぎます。
インスタントメッセージ暗号化	BitDefender 2009をインストールしているインスタントメッセンジャー（Yahoo! Messenger（英語版）とWindows Live(MSN)メッセンジャー）のユーザ同士であればメッセージが暗号化されます。

8.3. 全体設定

ワンクリックでセキュリティ設定を有効/無効にすることができます。

アイテム	説明
ゲームモード	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。
ノートＰＣモード	ノートＰＣモードはバッテリ消費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。
パスワード設定	パスワードを知っている人だけが設定変更ができるようになります。
BitDefender News	このオプションを有効にするとBitDefenderからの重要なご案内、新製品のご案内、セキュリティに関する情報を受け取ることができます。
製品通知アラート	このオプションを有効にすると製品通知アラートを受け取ることができます。

アイテム	説明
スキャンアクティビティバー	スキャンアクティビティバーは小さいです。透過的なウィンドウでBitDefenderのスキャン進行状況を示しています。 詳細については 「スキャンアクティビティバー」 (p. 35) を参照してください。
起動時にBitDefenderを読み込む	このオプションを有効にすることでBitDefenderは起動時にロードされます。 このオプションを選択しておくことをお勧めします。
ウィルス報告を送る	このオプションを有効にすると、BitDefender研究所にウィルススキャンレポートを送信します。このレポートには、氏名・IPアドレスなど個人を特定するような重要な情報は含まれておりません。送信元のIPアドレスは、純粋に統計目的だけに利用されます。
爆発的発生検出	このオプションを有効にすると、ウィルスが爆発的に拡散する可能性がある場合にBitDefender研究所にレポートを送信します。このレポートには、氏名・IPアドレスなど個人を特定するような重要な情報は含まれておりません。

9. 登録とマイアカウント

BitDefender Antivirus 2009には30日間の試用期間が設けられています。 試用期間中、製品はすべての機能が動作しますので、要望にあうものであるかテストしてください。 評価から１５日間経過すると、BitDefenderアカウントを作成しないかぎりアップデートが行われません。 BitDefenderアカウントの作成は登録に必須です。

試用期間が終了する前に製品を登録してコンピュータを保護するようにしてください。 登録は２つの手順でおこないます：

1. 製品のアクティベーション（BitDefenderアカウントの登録）. BitDefenderアカウントは、アップデートやテクニカルサポートへの連絡に必要なものです、すでにBitDefenderアカウントをお持ちの場合は、そのアカウントに対して登録してください。 BitDefenderはアクティベートが必要なことと、問題解決に役立つことをお知らせします。

   重要項目

   BitDefenderをインストールして15日以内にBitDefenderアカウントを作成してください。（ライセンスキーを登録した場合、BitDefenderアカウントの作成期限は30日まで延長されます） 登録がない場合にはBitDefenderは更新されなくなります。

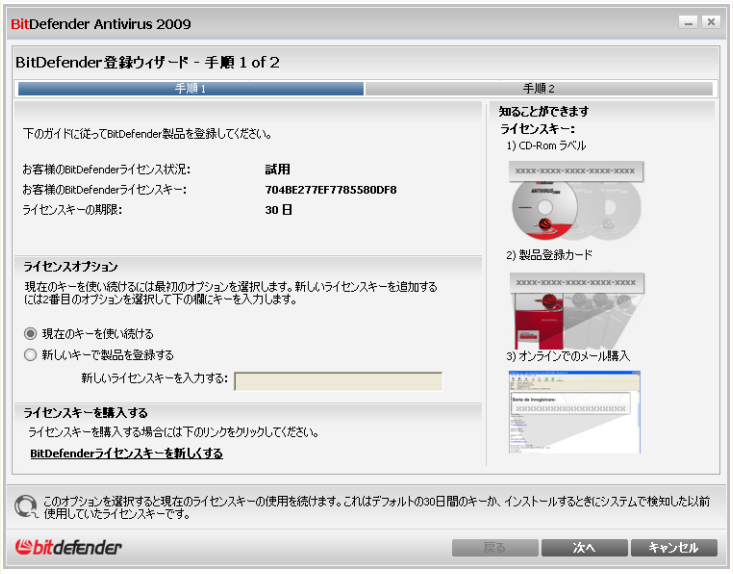
2. ライセンスキーを登録. ライセンスキーはその製品をどのぐらい使い続けることができるかを示しています。 ライセンスキーが期限切れを迎えると、BitDefenderはその機能を停止してコンピュータが保護されなくなります。 試用期間終了時にライセンスキーで製品を登録しなければなりません。 ライセンスキーを購入するか、お使いのライセンスを期限がきれる数日前には新しくする必要があります。

登録は登録ウィザードで行われます。

9.1. 製品登録ウィザード

BitDefender Antivirus 2009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。

9.1.1. 手順 1/2 - BitDefender Antivirus 2009を登録する



製品登録

BitDefender registration statusでは、お使いのライセンスキーが切れるまであと何日あるのか確認することができます。

BitDefender Antivirus 2009を登録する

1. この製品を登録を選択します。
2. ライセンスキーを入力します。

注意
ライセンスキーはこちらに書かれています：
■CDラベル
■製品登録カード

■オンラインストアからのメール

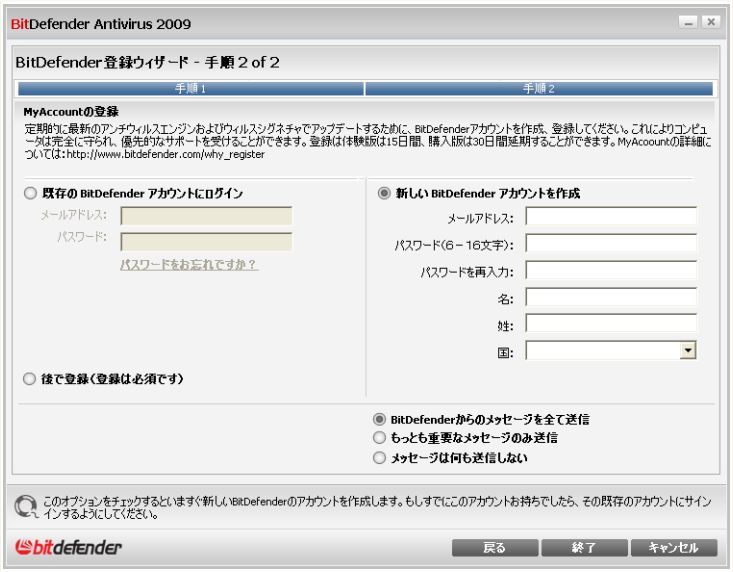
BitDefenderライセンスをお持ちでない場合ははオンラインストアか代理店からライセンスキーをご購入ください。

次へをクリックしてください。

注意

完了 ボタンが代わりに表示されている場合には、コンピュータでBitDefenderアカウントがすでに登録されています。　お客様のアカウントの情報について確認する場合には、詳細設定画面に切り替えて 左メニューにある製品登録 をクリックします。

9.1.2. 手順 2/2 - BitDefenderアカウントを作成



アカウント作成

もし、いまBitDefenderアカウントを作成しない場合には、登録をスキップを選択し、終了をクリックします。 それ以外の場合は、このまま進めます：

- 「まだBitDefenderアカウントをお持ちでない場合」 (p. 97)
- 「既にBitDefenderアカウントを持っている場合」 (p. 97)

重要項目

BitDefenderをインストールして15日以内にBitDefenderアカウントを作成してください。（ライセンスキーを登録した場合、BitDefenderアカウントの作成期限は30日まで延長されます） 登録がない場合にはBitDefenderは更新されなくなります。

まだBitDefenderアカウントをお持ちでない場合

新しい BitDefenderアカウントを作成を選択して必要な情報を入力してください。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。 パスワードは６文字から１６文字の間である必要があります。

■パスワードを再入力 - 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 - 名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
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からマイページ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アクティブ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。

BitDefenderは製品の特別価格での販売のご案内やプロモーションをアカウントとして登録していただいたメールアドレスに送ることがあります。 以下のオプションから選択できます：

■BitDefenderからの全ての案内を受け取る
■大切なメッセージだけ受け取る
■全てのメッセージを受け取らない

終了をクリックします。

既にBitDefenderアカウントを持っている場合

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。 この場合はアカウントのパスワードを入力してください。

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。

パスワードを忘れた場合は、パスワードを忘れたら？をクリックし指示に従ってください。

BitDefenderは製品の特別価格での販売のご案内やプロモーションをアカウントとして登録していただいたメールアドレスに送ることがあります。 以下のオプションから選択できます：

■BitDefenderからの全ての案内を受け取る
■大切なメッセージだけ受け取る
■全てのメッセージを受け取らない

終了をクリックします。

9.2. ライセンスキーの購入

試用期間はまもなく終了となります。ライセンスキーを購入して製品登録を行ってください。 BitDefenderを開いて画面下にある購入/更新 リンクをクリックしてください。 このリンクで開かれるウェブページでお使いのBitDefender製品のライセンスキーを購入することができます。

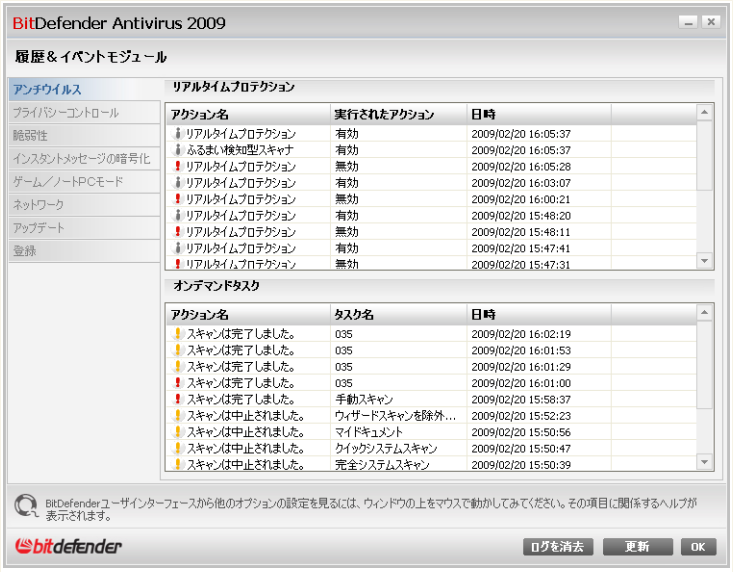
9.3. ライセンスを更新する

BitDefenderをお使いのユーザはBitDefender製品のライセンス更新時に優待を受けられます。また製品の最新版へ特別な割引または無料でアップグレードすることができます。

ライセンスキーが期限切れを迎えようとしています。ライセンスを更新してください。 BitDefenderを開いて画面下にある購入/更新 リンクをクリックしてください。このリンクで開かれるウェブページでライセンスを更新することができます。

10. 履歴

BitDefender メインウインドウの下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
■個人情報コントロール
■脆弱性
■IM暗号化

■ゲーム/ノートＰＣモード
■ネットワーク
■アップデート
■登録

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。

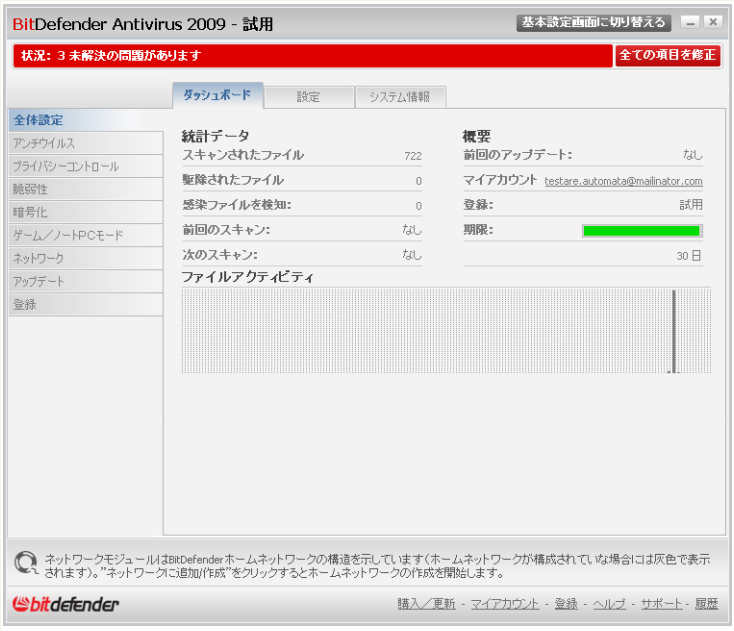
詳細設定

11. 一般

全体設定ではBitDefenderの作動状況およびシステムの稼働状況を表示します。 ここではBitDefenderの全ての動作を変更することができます。

11.1. ダッシュボード

製品の動作状況と登録状況を見るには詳細設定画面からダッシュボードをご覧ください



ダッシュボード

この文書はいくつかの大きな章に分かれています。

■統計情報：BitDefenderの統計情報と重要な情報をみることができます

■概要 - 更新状況やBitDefenderアカウント、ライセンスの状況を確認することができます。

■ファイルゾーン - BitDefenderアンチマルウェアスキャンによって検査されたオブジェクト数を表示しています。一番上には時間あたりのトラフィック数を表示しています。

11.1.1. 統計データ

BitDefenderの動作状況を確認するときには、この統計情報をみることをお勧めします。 次の内容を見ることができます：

アイテム	説明
スキャン済みのファイル	マルウェアのスキャンを行ったファイル数の最新情報を表示しています
駆除されたファイル	ウィルススキャンの結果、駆除されたファイル数の最新情報を表示しています
検出されたウィルス	このシステムで見つかったウィルス数の最新情報を表示しています
前回のスキャン	前回いつコンピュータがスキャンされたかを示しています。 もし前回のスキャンが１週間以上前に実施されたものなら、できるだけはやい機会にスキャンを行ってください。 コンピュータ全体のスキャンは、 アンチウィルス, ウィルススキャン タブを開いて、フルシステムスキャンまたは完全システムスキャンを実行します。
次回のスキャン	次回いつコンピュータがスキャンされるかを示しています。

11.1.2. 概要

ここでアップデート状況、アカウント状況、製品登録、ライセンス情報を確認できます。

アイテム	説明
直前のアップデート	BitDefenderがいつ最後にアップデートされたがを示しています。 完全にシステムを守るために定期的なアップデートを実行してください。
マイアカウント	BitDefenderから提供されるサービスやサポート、有用な情報、ライセンスキーをなくしたときなどに利用するBitDefenderアカウントのメールアドレスが表示されます。製品をアクティベートするためにアカウントを作成する必要があります。 BitDefenderアカウントについては次を参照してください。「BitDefenderアカウントの作成方法」(p. 225).
登録	ライセンスキーのタイプと状況が表示されます。システムのセキュリティを維持し続けるためには、BitDefenderのライセンスの有効期限が来るまでにライセンスを更新するかアップグレードする必要があります。
有効期限	ライセンス期限が切れるまでの日数 ライセンスキーが残りわずかで切れる場合には、製品を新しいキーで登録してください。 ライセンスキーの購入またはライセンスの更新には、購入/更新 リンクをクリックします。画面下にこのリンクはあります。

11.2. 設定

BitDefender Antivirus 2009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。

全体設定

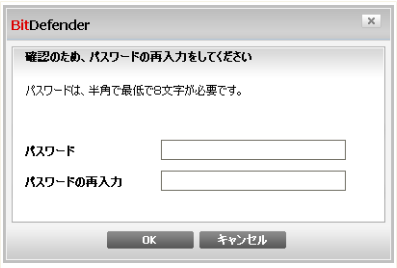
BitDefenderの全体的な動作をここで設定できます。デフォルトでは、BitDefenderはWindowsの起動時に読み込まれ、タスクバーに最小化された状態で実行されます。

11.2.1. 全体設定

■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
コンピュータの管理者権限を持つユーザが他にもいる場合は、BitDefenderの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、以下のウィンドウが開きます：



パスワードを入力

パスワードフィールドにパスワードを入力し、同じパスワードをパスワードを再入力フィールドに再度入力してOKをクリックします。

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

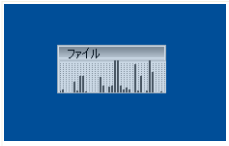
重要項目
パスワードを忘れた場合にBitDefenderの設定を変更するには、製品を修復しなければなりません。

■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ィンドウを表示します。 BitDefenderがポップアップ画面をどの状態のとき（基本設定画面もしくは詳細設定画面）に表示するかを指定します。

■Windowsの起動時にBitDefenderを読み込む – システム起動時に自動的に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。

■スキャンアクティビティーバーを有効にする（処理状況を画面にグラフ表示） – Windowsにログオンするたびに、スキャン処理バーを表示します。スキャンアクティビティー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ます。



スキャンアクティビティバー

注意
このオプションは実行中のWindowsユーザアカウントでのみ設定可能です。 スキャンアクティビティバーは詳細設定画面のときのみに利用できます。

11.2.2. ウイルスレポート設定

■ウイルスレポートを送信 - 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、BitDefender研究所へ送ります。ウイルス発生を監視するために使用されます。

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 - 可能性のあるウイルス発生のレポートをBitDefender研究所に送ります。

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用されます。

11.3. 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、詳細設定画面で一般情報>Sシステム情報をクリックします。

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ます。

３つのボタンがあります：

■取消 – 設定をデフォルトに戻します。 File Associationsは設定のみです。

■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）。

注意
選択された項目によっては、表示ボタンが表示されない場合があります

■更新 – システム情報画面を開き直します。

12. アンチウイルス

BitDefenderは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）からコンピュータを保護します。 BitDefenderが提供する保護は２つのカテゴリに分類できます：

■リアルタイムプロテクション - 新しいマルウェアが侵入するのを防ぎます 例えばBitDefenderは、WORD文書を開いた時に既知の脅威を対象に文書をスキャンします。メールの場合は受信時にスキャンを行します。

注意
リアルタイムプロテクションは、ユーザ操作により読み込まれるファイルを全てスキャンします。

■オンデマンドスキャン- 既にシステムに存在しているマルウェアを検出および除去することができます。 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、ファイルをユーザが指定します - 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。

12.1. シールド

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、リアルタイムプロテクションとも呼ばれています。アンチフィッシングはフィッシングの可能性があるウェブページについてユーザに警告しウェブ利用の安全性を確保します。

リアルタイムプロテクションの設定および監視を行うには、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ます。

シールド

リアルタイムプロテクションを有効にしたり無効にしたりできます リアルタイムプロテクションの有効/無効を切り替えるには、チェックボックスをクリックします

重要項目
コンピュータをウイルス感染から保護するためにリアルタイム保護を常に有効にしておいてください。

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ます。

12.1.1. 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：

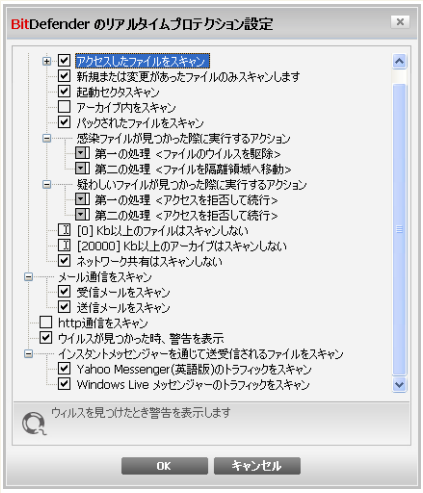
保護レベル	説明
弱	基本的に必要なセキュリティはカバーします。リソース消費レベルはとても低いです。 ウイルスを対象にプログラムおよび受信メールメッセージだけをスキャンします。従来のシグネチャ方式のスキャンに加え、ヒューリスティック分析も使用されます。感染ファイルに対するアクションは以下の通りです： ファイルを感染除去/アクセス拒否
デフォルト	標準的なセキュリティを提供します。リソース消費レベルは低いです。 すべてのファイルと受信&送信メールメッセージをウイルスとスパイウェアを対象にスキャンします。従来のシグネチャ方式のスキャンに加え、ヒューリスティック分析も使用されます。感染ファイルに対す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

12.1.2. 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、アーカイブを例外と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コンピュータの動作を改善することができます。

カスタムレベルをクリックして、リアルタイム保護をカスタマイズできます。以下のウィンドウが表示されます：



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ます。

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。選択すると開けるようになります。

■アクセスされたファイルと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）経由の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ます。

オプション		説明
アクセス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、アクセスされるファイルがすべてスキャンされます。
	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のみをスキャンします。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をスキャン	ユーザが指定した拡張子を持つファイルのみをスキャンします。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の場合には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可能性があります。 これらの種類のファイルをスキャン対象から例外としたい場合は、ダイアラとアプリケーションをスキャンから例外を選択します。
新規または更新されたファイルのみスキャン		前回スキャンされていないファイル、または前回スキャンされてから変更されていないファイルのみをスキャンします。　このオプションを選択することで、システム全体のレスポンスを、セキュリティへの影響を最小限に抑えながら改善させることができるでしょう。
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。

オプション		説明
アーカイブ内部をスキャン		アクセスされたアーカイブがスキャンされます。このオプションがオンの場合には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。
最初のアクション		感染ファイルや疑わしいファイルに対する最初のアクションをドロップダウンメニューから選択します。
	アクセスを拒否して続行	感染ファイルが検出された場合にはこのファイルへのアクセスは拒否されます。
	駆除されたファイル	感染しているファイルからマルウェアのコードを取り除きます。
	ファイルを削除	警告なしで感染ファイルを即時に削除します。
	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。 隔離されたファイルは実行されることも開かれることもありません。そのため感染が広がるリスクはそれ以上ありません。
２番目のアクション		最初のアクションが失敗した場合に感染ファイルに対して実行される２番目のアクションをドロップダウンメニューから選択します。
	アクセスを拒否して続行	感染ファイルが検出された場合には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時に削除します。
	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。 隔離されたファイルは実行されることも開かれることもありません。そのため感染が広がるリスクはそれ以上ありません。
[x]Kb以上のファイルはスキャンしない		スキャンするファイルの最大サイズを入力します。このサイズが0Kbに設定されていると、

オプション	説明
	サイズに関わらずすべてのファイルがスキャンされます。
サイズが[20000]Kb以上のファイルはスキャンしない	スキャンするアーカイブファイルの最大容量(KB)を入力してください　ファイルサイズに0を指定すると、ファイルの大きさに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の場合には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。 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のみ、このオプションを有効にすることをお勧めします。

■メール通信をスキャン - メール通信をスキャンします。

以下のオプションを指定できます：

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。

■ウイルス発見時に警告を表示 - ファイルやメールメッセージでウイルスが見つかった時に警告ウィンドウが開きます。

感染ファイルの場合には警告ウィンドウにはウイルス名、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。感染メールの場合は送信者と宛先の情報も警告ウィンドウに表示されます。

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研究所へ送るように警告ウィンドウからウィザードを起動できます。このレポートに関する情報を受け取れるようにメールアドレスを入力することもできます。

■メッセンジャーから送受信されるファイルをスキャンする。 Yahoo! Mesenger（英語版）またはWindows Liveメッセンジャーで送受信ファイルのスキャンをするにはチェックボックスにチェックします

OKをクリックして変更を保存しウィンドウを閉じます。

12.1.3. ふるまい検知型スキャナの設定

ふるまい検知型スキャナは新しい脅威に対する防御壁で、まだウィルス定義が提供されれていない脅威に対応します。 このスキャナはお使いのコンピュータで動作しているアプリケーションの動作を常時監視して分析し、もし疑わしい動作を検知した場合に警告します。

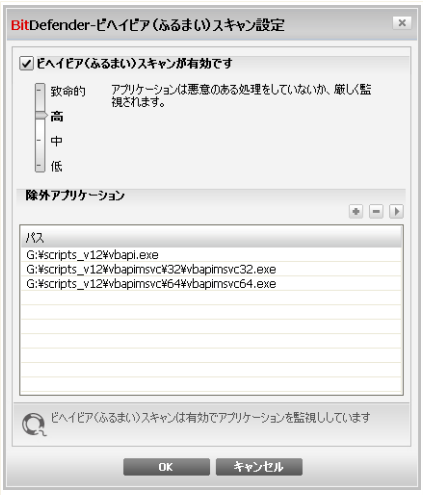
ふるまい検知型スキャナは、悪意があるとおもわれる処理を行ったアプリケーションがあれば警告を発し、あなたに対処方法を尋ねます。

ふるまい検知型スキャナの警告

もし検知されたアプリケーションを知っていて信頼できるものであれば許可をクリックしてください。 このふるまい検知型スキャナはそれ以上、悪意のある動作の疑いがあるアプリケーションのスキャンを行いません。

そのアプリケーションをただちに終了する場合にはOKをクリックしてください。

ふるまい検知型スキャナの設定を行うにはスキャン設定をクリックします。



ふるまい検知型スキャナの設定

デフォルトではふるまい検知スキャナは無効となっています。該当するチェックボックスを選択してそれを有効にしてください。

重要項目
ふるまい検知型スキャナを有効にして未知のウィルスを防いでください。

保護レベルの設定

ふるまい検知型スキャナの防御レベルは、新しくリアルタイム防御レベルを設定すると自動的に変更します。 デフォルトの設定に満足されない場合は手動で防御レベルを設定できます。

注意
もし現在のリアルタイム防御レベルを変更した場合には、ふるまい検知型スキャナの防御レベルも伴って変更されることに注意してください。 リアルタイムプロテクションを　弱にセットしている場合、ふるまい検知型スキャナは自動的に無効となる設定することができません。

スライドバーをドラッグして動かしてセキュリティの要件にもっともフィットする防御レベルに設定します。

保護レベル	説明
致命的	アプリケーションは厳密に悪意のある処理をしていないか監視されます。
高	アプリケーションは悪意のある処理をしていないか厳しく監視されます。
中	アプリケーションは悪意のある処理をしていないか適度に監視されます。
低	アプリケーションは悪意のある処理をしていないか監視されます。

対象外アプリケーションの管理

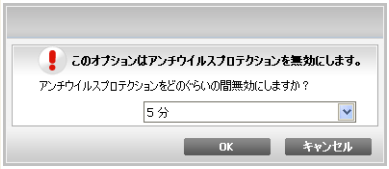
ふるまい検知型スキャナを設定して特定のアプリケーションをチェックしないようにすることができます。 現在ふるまい検知型スキャナによってチェックされていないアプリケーションは、対象外アプリケーション表に表示されています。

対象外アプリケーションを管理する場合には、表の上にあるボタンを使用します：

- 追加 - 新しいアプリケーションをスキャン対象から例外とします。
- 除去 - アプリケーションをリストから削除します。
- 編集 - アプリケーションパスを編集します。

12.1.4. リアルタイムプロテクションを無効にする

リアルタイム保護を無効にしようとすると警告ウィンドウが開きます。



リアルタイムプロテクションを無効にする

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、永続的に、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の場合はマルウェアの脅威から保護されません。

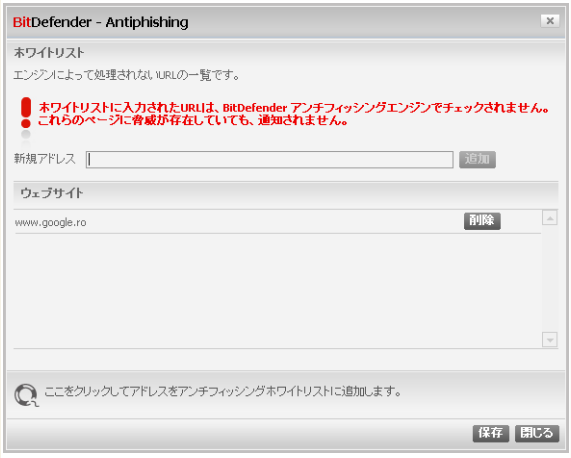
12.1.5. アンチフィッシング防御の設定

BitDefenderはリアルタイムのアンチフィッシングを次のものに対して提供します：

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger（英語版）
- Windows Live (MSN) Messenger

アンチフィッシングは完全に、もしくは特定のアプリケーションのみに無効するか選択できます。

ホワイトリストをクリックしてBitDefenderアンチフィッシングエンジンではスキャンさせないwebリストを設定、管理することができます。



アンチフィッシングのホワイトリスト

BitDefenderが現在フィッシングチェックを行わないwebサイトをみることができます。

新しくwebサイトをホワイトリストに追加するには、そのURLアドレスを新しいアドレスフィールドに入力して追加をクリックしてください。 ホワイトリストにはあなたが完全に信頼しているwebサイトのみを登録してください。 例えば現在利用しているオンラインショップのサイトを追加します。

注意

ホワイトリストへの追加はwebブラウザーに組み込まれたBitDefenderアンチフィッシングツールバーから簡単にできます。 詳細については、「ブラウザとの連携」 (p. 46)を参照してください。

ホワイトリストからwebサイトを除くには対応する除去ボタンをクリックします。

閉じるをクリックして変更を保存しウィンドウを閉じます。

12.2. ウィルススキャン

BitDefenderの主な目的はコンピュータをウイルスから守ることです。これはコンピュータへの新しいウイルスの侵入を防ぎ、メールメッセージや、ダウンロードおよび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をインストールする前にシステムに既にウイルスが存在している可能性もあります。このため、BitDefenderをインストールした後で既に存在するウイルスを対象に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の設定および実行を行う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また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時に実行するように設定することもできます。

12.2.1. 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に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の設定やスキャン結果の確認を行うプロパティウィンドウがあります。詳細については「スキャンタスクを設定」（p. 125）を参照してください。

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。以下のタスクが利用できます：

デフォルトタスク	説明
完全システムスキャン	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 などシステムのセキュリティを脅かすあらゆる種類のマルウェアをスキャンします。
フルシステムスキャン	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 などシステムのセキュリティを脅かす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，および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対象にスキャンしますが、メモリ，レジストリ，Cookieはスキャンしません。

デフォルトタスク	説明
自動ログオン スキャン	ユーザがWindowsにログオンしてきた際に動作している項目をスキャン　デフォルトでは自動ログオンスキャンは無効になっています。 もしこの処理を行うには、それを右クリックしてスケジュールを選択して起動時にその処理を行うようにします。 起動からどのぐらい時間が経過してからその処理を開始するかを指定（分）できます。

注意
完全システムスキャンとフル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、スキャン処理に時間がかかります。従って、これらのタスクは優先度を低くして実行するか、できればシステムが使われていない時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含みます。

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。 カレントユーザの重要なフォルダをスキャンする場合にはこのタスクを使用します： マイドキュメント，デスクトップ，スタートアップ。これにより文書，作業環境，起動されるアプリケーションの安全を確認することができます。

■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ィ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できます。

各タスクの右側に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ィンドウ、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。

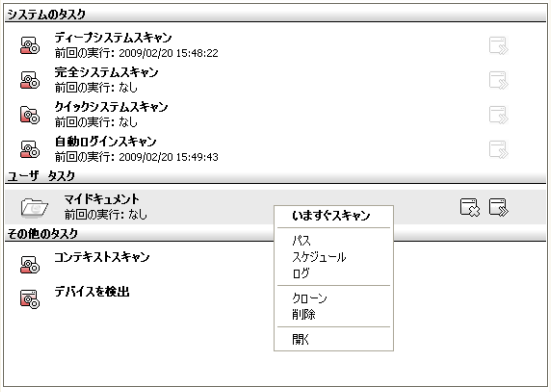
注意
システムタスクには使えません。システムタスクを削除することはできません。

■ 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。

各タスクの左側にタスクの設定とスキャンログの表示を行えるプロパティボタンがあります。

12.2.2. 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ると開きます。



ショートカットメニュー

ショートカットメニューには、以下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。

■パス - プロパティウィンドウ、 パスタブを開き、そこで選択タスクのスキャンターゲットを変更できます。

注意
システムタスクの場合には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。

■スケジュール - プロパティ ウィンドウ、スケジューラータブを開き、そこで選択したタスクをスケジュール指定できます。

■ログ - プロパティウィンドウ、ログタブを開き、そこで選択したタスクが実行後に生成されたレポートをみることができます。

■複製 - 選択したタスクを複製します。 複製したタスクの設定を編集できるので新しいタスクを作成する時に便利です。

■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。

■開く - プロパティ ウィンドウ、概要タブを開きます。そこで選択したタスクを変更することができます。

注意
その他のタスクカテゴリの特殊性により、ここではログおよび開くオプションのみが使用できます。

12.2.3. スキャンタスクを作成

スキャンタスクを作成するには、以下のいずれかの方法を使用できます：

■既存のタスクを複製し、名前を変更してプロパティウィ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て設定を行ってください。

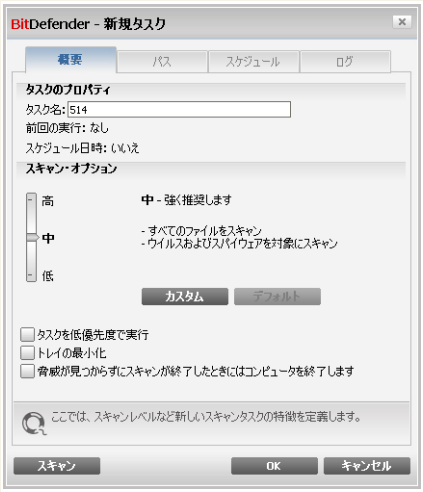
12.2.4. スキャンタスクを設定

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ィンドウがあります。 このウィンドウを開くにはタスクの右側に表示される開くボタンをクリックします（または、タスクを右クリックして、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. 148)を参照してください。

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ます。 以下のウィンドウが開きます：



概要

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）の確認とスキャンの設定をここで行うことができます。

スキャンレベルの選択

スキャンレベルを選択してスキャン設定を簡単に設定することができます。スライダをドラッグして適切なスキャンレベルを設定します。

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使用されます。
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位です。 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使用されます。
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使用されます。

スキャン処理に関する一連の全体的なオプションも用意されています：

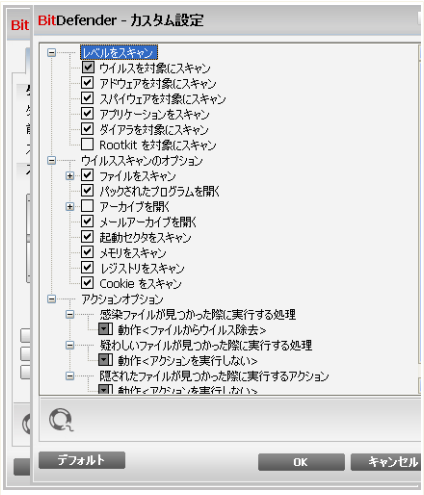
- タスクを低優先度で実行. スキャン処理の優先順位を下げます。他のプログラムはより高速で実行されますがスキャン処理終了までの時間が長くなります。
- 最小化してトレイに格納. スキャンウィンドウをシステムトレイにしまいます。BitDefenderアイコンをダブルクリックすると開きます。
- スキャンが完了し、なにも脅威が発見されない場合にはコンピュータをシャットダウンします。

変更を保存してウィンドウを閉じるにはOKをクリックします。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、アーカイブを例外と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ます。新しいウィンドウが開きます。



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ます。

スキャンオプションは３つのカテゴリに分類されています：

■スキャンレベル. スキャンレベルカテゴリで適切な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。

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の場合にはアドウェアコンポーネント

オプション	説明
	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。
スパイウェアを対象にスキャン	既知の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対象にスキャン	正当なアプリケーションをスキャンしてスパイツールとして使われ、悪意のあるアプリケーションを隠したり、その他の悪意のある目的に使われる可能性があるかを検査します。
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の場合には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）を対象にスキャンします。

■ウイルススキャンのオプション. スキャンするオブジェクトのタイプ（ファイル種別、アーカイブなど）を指定するためウィルススキャンオプションカテゴリにおいて適切なオプションを選択します。

オプション		説明
スキャンファイル	すべてのファイルをスキャン	ファイルの種類に関わらずすべての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のみをスキャンします。以下の拡張子を持つファイルです： 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;

オプション		説明
		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をスキャン	ユーザが指定した拡張子を持つファイルのみをスキャンします。これらの拡張子は";"で区切ってください。
圧縮されたプログラムを開く		圧縮されたファイルをスキャンします。
アーカイブを開く		通常のアーカイブ .zip, .rar, .ace, .iso などの内部をスキャンします。 すべてのアーカイブ形式のスキャンを行う場合には（インストーラーやchmファイル）、全体スキャンを選択します。 アーカイブ（圧縮）ファイルのスキャンはより長いスキャン時間と、多くのシステムリソースが必要です。 アーカイブサイズ制限フィールドをクリックしてスキャンの対象とする最大サイズをキロバイト(KB)で指定します。
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。

■アクションオプション. 感染したファイルの各カテゴリに対してどのような処理を行うか処理オプションカテゴリのオプションで指定します。

注意

新しい処理を設定するには現在の処理をクリックして希望するオプションをメニューから選択します。 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場合には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。

- 検出された感染ファイルに対するアクションを選択します。 以下のオプションを指定できます：

アクション	説明
アクションなし	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表示されます。
ファイルからウイルスを駆除	検知された感染ファイルからマルウェアのコードを取り除きます。
ファイルを削除	警告なしで感染ファイルを即時に削除します。
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。 隔離されたファイルは実行されることも開かれることもありません。そのため感染が広がるリスクはそれ以上ありません。

- 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ます。 以下のオプションを指定できます：

アクション	説明
アクションなし	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時に削除します。
ファイルを隔離領域へ移動	疑わしいファイルを隔離領域へ移動します。 隔離されたファイルは実行されることも開かれることもありません。そのため感染が広がるリスクはそれ以上ありません。

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。ファイルを BitDefender研究所へ送ることをお勧めします。

- 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ます。 以下のオプションを指定できます：

アクション	説明
アクションなし	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。
ファイル名変更	隠しファイルを可視化しました。それらは.bd.renという拡張子がファイル名に付加されています。そのような場合には、コンピュータ内のそのようなファイルを検索することで見つけることができます。
ファイルを隔離領域へ移動	隠されたファイルを隔離領域へ移動します。 隔離されたファイルは実行されることも開かれることもありません。そのため感染が広がるリスクはそれ以上ありません。

注意

これらの隠しファイルはWindwosからお客様が隠したものではありません。このファイルは特殊なプログラムによって隠されており、ルートキットとして知られています。 ルートキットはそのそもは悪意を持つものではありません。しかしウィルスやスパイウェアを通常のアンチウィルスプログラムでは検知されないようにするために使われることが多いです。

- パスワード保護または暗号化ファイルに対する処理オプション. Windwosの暗号化機能を使っているファイルは重要だとおもいます。 これが、Windowsの暗号化機能が使われているファイルで感染しているもの、またはその疑いがあるものに対して、異なった処理をとらなくてはいけない理由です。 他に特別の処理をとらなくてはいけないファイルグループが、パスワード保護されたアーカイブです。 パスワードでプロテクトされたアーカイブは、あなたがパスワードを提供しない限りスキャンすることはできません。 このオプションを使ってパスワード保護されたアーカイブ、Windowsの暗号化がされたファイルに対する処理を設定します。

○暗号化された感染ファイルが見つかった際に実行するアクション. Windowsの暗号化されたファイルが感染している場合にとるべき処理を選択します。以下のオプションを指定できます：

アクション	説明
なにもしない	Windowsの暗号化がされた感染ファイルのみ記録する。 スキャン完了後、スキャンログを開いてこれらのファイルの情報をみることができます。
ファイルからウイルスを駆除	検知された感染ファイルからマルウェアのコードを取り除きます。 感染除去はいくつかのケースでは失敗することがあります。例えば感染ファイルが特別な電子メールの形式の中にある場合です。
ファイルを削除	警告なしに即時にディスクから感染したファイルを取り除きます。
ファイルを隔離領域へ移動	感染したファイルをそれがある場所から隔離フォルダへ移動します。 隔離されたファイルは実行されることも開かれることもありません。そのため感染が広がるリスクはそれ以上ありません。

○暗号化された疑わしいファイルが見つかった際に実行するアクション. Windowsの暗号化されたファイルが感染の疑いがある場合にとるべき処理を選択します。 以下のオプションを指定できます：

アクション	説明
なにもしない	Windowsの暗号化がされた、感染の疑いがあるファイルのみ記録する。 スキャン完了後、スキャンログを開いてこれらのファイルの情報をみることができます。
ファイルを削除	警告なしに疑わしいファイルを即時に削除します。
ファイルを隔離領域へ移動	疑わしいファイルを隔離領域へ移動します。 隔離されたファイルは実行されることも開かれる

アクション	説明
	こともありません。そのため感染が広がるリスクはそれ以上ありません。

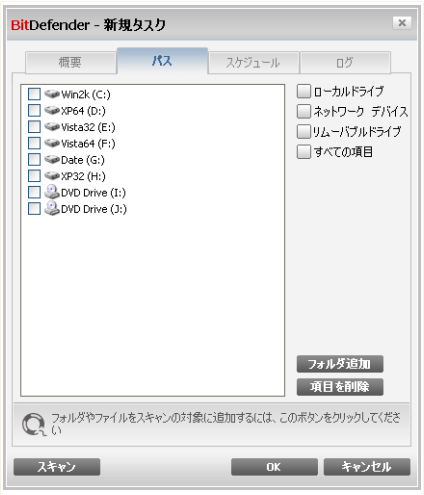
○パスワード保護されたファイルが見つかった際に実行するアクション. パスワードがかかったファイルを検知した場合に対する処理を選択します。 以下のオプションを指定できます：

アクション	説明
スキャン未実施を記録	パスワードがかかっているファイルはスキャンログに記録だけされます。 スキャン完了後、スキャンログを開いてこれらのファイルの情報をみることができます。
パスワードの入力	パスワードがかかったファイルが検知された場合にはそのファイルをスキャンするためにユーザにパスワードを入れるよう要求します。

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。 OKをクリックして変更を保存しウィンドウを閉じます。

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対象を設定するにはそのタスクを右クリックしてパスを選択します。 以下のウィンドウが開きます：



スキャン対象

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、もしあれば以前追加したファイルやフォルダが表示されます。チェックし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、以下のボタンが表示されます：

■項目を追加 – ファイル閲覧ウィンドウが開き、そこでスキャンしたいファイル/フォルダを選択できます。

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 – スキャンす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
後から追加したファイル/フォルダのみ削除することができます。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の選択を素早く行え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。

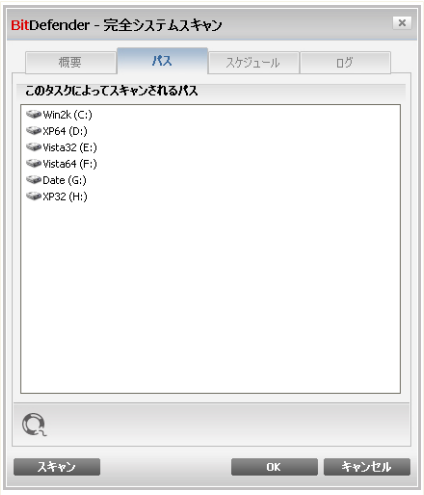
注意
コンピュータ全体をスキャンしたい場合はすべての項目チェックボックスを選択します。

変更を保存してウィンドウを閉じるにはOKをクリックします。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にある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のみ行うことができます。

特定システムのスキャンタスクの対象を表示するには、タスクを右クリックしてタスクのパスを表示を選択します。 例えば完全システムスキャンでは、以下のウィンドウが開きます：



完全システムスキャンのスキャン対象

フルシステムスキャンおよび完全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をクリックしてウィンドウを閉じます。 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は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。そのためコンピューが使われていないアイドル状態の時に実行するよう設定しておくのが最適です。

特定タスクのスケジュール表示または編集を行う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択します。 以下のウィンドウが開きます：

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、以下のオプションのいずれかを選択します：

■スケジュールなし - ユーザが要求した場合のみタスクを起動します。

■指定日 - 特定の日時に一度だけスキャンを起動します。開始日時フィールドに開始日時を指定します。

■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択し、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/年の数を入力します。また開始日時欄に開始日時を指定します。

■システム起動時 -ユーザがWindowsにログオン時、指定した分数が経過した後、スキャンを起動します。

変更を保存してウィンドウを閉じるにはOKをクリックします。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。

12.2.5. ファイルとフォルダをスキャン

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コンピュータをスキャンした場合に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がいつスキャンされたかを確認するためには、詳細設定画面のアップデート>アップデート を開きます。

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。

スキャンの使い方

その他の役に立つスキャンの使い方：

- ハードディスクのサイズによりますが、包括的なコンピュータのスキャン（完全システムスキャンやフルシステムスキャン）は時間がかかります（１時間またはそれ以上）。 そのためこの種のスキャンは長時間コンピュータを使わないとき（例えば夜間）に実行されることをおすすめします。

  スキャンをスケジュール で都合のよいときに実行させることができます。 コンピュータを起動したままにしておいてください。 Windows Vistaをお使いの場合には、コンピュータがタスクがスケジュールされている時間にスリープモードに入っていないようにしてください。

- もしよくインターネットからファイルを特定のフォルダにダウンロードするようなことがあれば、新しいスキャンタスクを作成して、 そのフォルダをスキャン対象に含めてください。 タスクを毎日またはより短い間隔で実行するようにスケジュールします。

- マルウェアの中にはWindowsの設定を変更して、システム起動時に実行されるようにするものがあります。 そのようなマルウェアからコンピュータを守るために、ログイン処理スキャン タスクをシステム起動時に実行するようにスケジュールしてください。 ログイン処理スキャンはシステムパフォーマンスに起動後しばらく影響します。

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 2009でスキャンを選択してください。
■ドラッグ&ドロップによるスキャン - ファイルまたはフォルダをスキャン処理バーへドラッグ&ドロップします。
■手動スキャン - BitDefender手動スキャンを使用してスキャンするファイルまたはフォルダを直接選択します。

即座にスキャン

コンピュータあるいはその一部をスキャンするには、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。

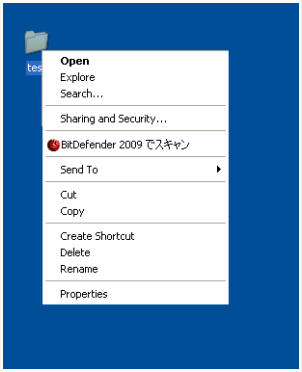
スキャンタスクを実行するには、以下の方法のいずれかを使用します：

■一覧で任意のスキャンタスクをダブルクリックします。
■タスクに対応する 今すぐスキャンボタンをクリックします。
■タスクを選択してタスクを実行をクリックします。

アンチウィルススキャンウィザード が表示されスキャン処理についてガイドします。

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やフォルダをスキャンする場合は、コンテキストメニューを使用できます。 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

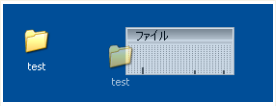
スキャンしたいファイルあるいはフォルダを右クリックし、 BitDefender 2009でスキャンを選択します。 アンチウィルススキャンウィザード が表示されスキャン処理についてガイドします。

コンテキストメニュースキャンタスクのプロパティウィ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の確認を行うことができます。

ドラッグ&ドロップスキャン

スキャンしたいファイルまたはフォルダを、以下のようにスキャン処理バーへドラッグ&ドロップします。

ファイルをドラッグ



ファイルをドロップ

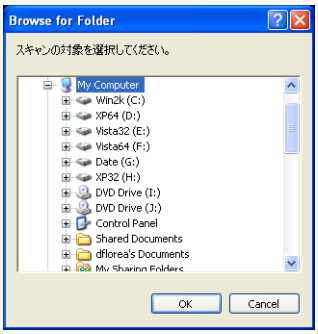
アンチウィルススキャンウィザード が表示されスキャン処理についてガイドします。

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用し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がセーフモードで起動している時でも実行できるので、非常に便利です。

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 2009 → BitDefender 手動スキャンのように選択してください。 以下のウィンドウが開きます：



手動スキャン

スキャンしたいオブジェクトを選択してOKをクリックします。 アンチウィルススキャンウィザード が表示されスキャン処理についてガイドします。

アンチウィルススキャンウィザード

オンデマンドスキャンを開始すると、アンチウィルススキャンウィザードが表示されます。 以下の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。

注意
スキャンウィザードが表示されない場合には、スキャンがバックグラウンドで実行されるように設定されています。 スキャンが進行していることを表すアイコンが システムトレイにあります。 このアイコンをクリックするとスキャンウィンドウが開き、スキャン状況をみることができます。

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。

BitDefenderがスキャンを完了するまでお待ちください。

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。

パスワード保護されたアーカイブ.　BitDefenderがパスワード保護されたアーカイブをスキャン中に発見すると、デフォルトでは パスワード入力プロンプトを表示してパスワードの提供を求めてきます。　パスワードでプロテクトされたアーカイブは、あなたがパスワードを提供しない限りスキャンすることはできません。 以下のオプションを指定できます：

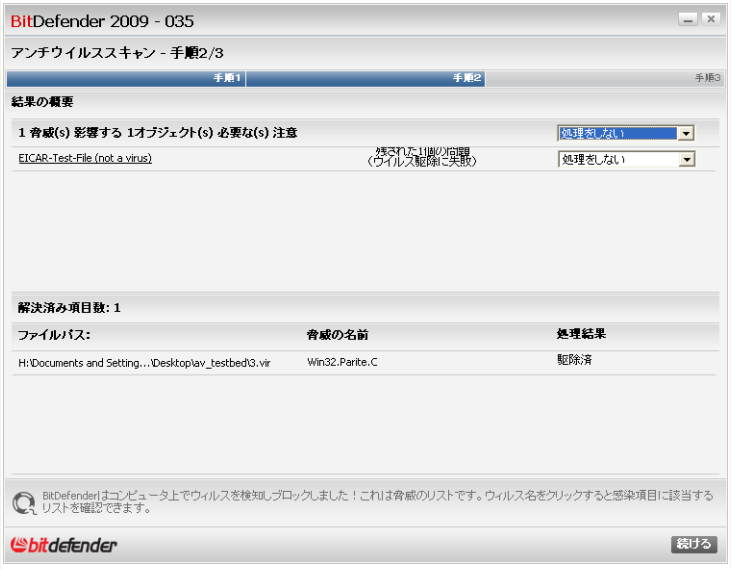
- このオブジェクトのパスワードを入力します。. BitDefenderにこのアーカイブをスキャンさせる場合には、このオプションを選択してパスワードを入力します。パスワードを知らない場合には、他のオプションを選択してください。
- このオブジェクトのパスワードを入力しません（このオブジェクトをスキップ）. このオプションを選択するとこのアーカイブのスキャンをスキップします。
- すべてのオブジェクトのパスワードを入力しません（パスワード保護されたオブジェクト全てをスキップします）. パスワード保護されたパスワードに悩まされたくない場合にはこのオプションを選択します。 BitDefenderはそれらをスキャンできません。しかしログファイルに記録が残されます。

OK をクリックしてスキャンを続けます。

スキャンを停止または一時停止. 停止&はいをクリックしていつでもスキャンを停止することができます。その場合はウィザードの最後の手順に移動します。 スキャン処理を一時的に停止するには一時停止をクリックします。スキャンを再開するには再開をクリックします。

手順 2/3 - アクションを選択

スキャンが完了するとスキャンの結果を示す新しいウィンドウが表示されます。



処理

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に基づくグループごとに表示されます。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。

全ての問題に対して一括した処理を行うか、もしくは個々の問題のグループごとに個別の処理を行うかを選択できます。

１つまたは複数のオプションがメニューで表示されます：

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。スキャン完了後、スキャンログを開いてこれらのファイルの情報をみることができます。

アクション	説明
ウイルスを除去	感染しているファイルからマルウェアのコードを取り除きます。
削除	検出したファイルを削除します。
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。　隔離されたファイルは実行されることも開かれることもありません。そのため感染が広がるリスクはそれ以上ありません。
ファイル名変更	隠しファイルを可視化しました。それらは.bd.ren という拡張子がファイル名に付加されています。 そのような場合には、コンピュータ内のそのようなファイルを検索することで見つけることができます。 これらの隠しファイルはWindwosからお客様が隠したものではありません。このファイルは特殊なプログラムによって隠されており、ルートキットとして知られています。 ルートキットはそのそもは悪意を持つものではありません。しかしウィルスやスパイウェアを通常のアンチウィルスプログラムでは検知されないようにするために使われることが多いです。

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ます。

手順 3/3 - 結果を表示

BitDefenderによる問題の修正が終了すると、スキャンの結果が新しいウィンドウに表示されます。

概要

結果の概要を確認できます。 スキャン処理について包括的な情報をご覧になりたい場合には ログファイルを表示 をクリックしてスキャン履歴を確認してください。

重要項目
削除処理を完了するために必要に応じてシステムを再起動してください。

閉じるをクリックしてウィ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

多くの場合には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。 しかし、解決できない問題もあります。

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、BitDefender研究所へ報告するよう促されます。 OKをクリックすると詳しく分析するためにファイルがBitDefender研究所に送信されます。

12.2.6. 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ログを選択します。 以下のウィンドウが開きます：

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ここで確認できます。ファイルごとに記録されたスキャン処理の状況、スキャンが実行された日時、スキャン結果の概要などの情報が提供されます。

２つのボタンが使用できます：

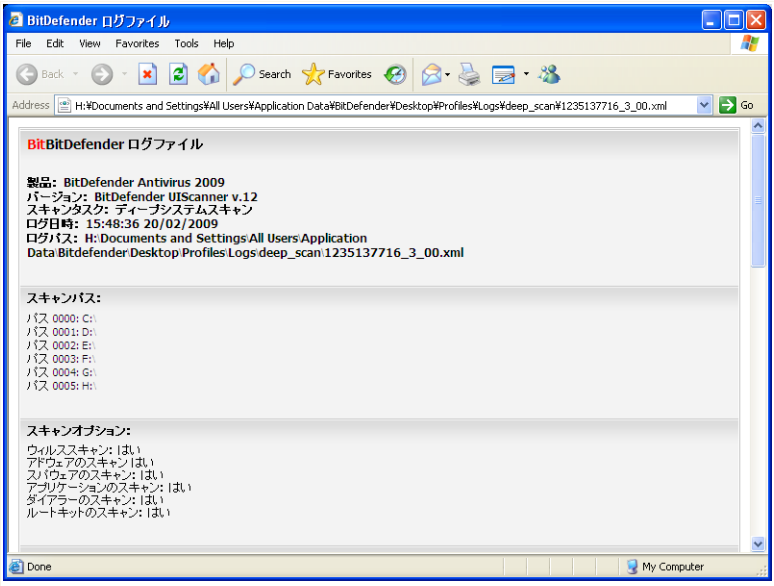
■削除 – 選択したスキャンログを削除します。
■表示 – 選択したスキャンログを表示します。 スキャンログがデフォルトのウェブブラウザで開きます。

注意
ファイルを右クリックし、ショートカットメニューから対応するオプションを選択して、ファイルの表示や削除を行うこともできます。

変更を保存してウィンドウを閉じるにはOKをクリックします。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を示しています：



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，脅威に対して実行されたアクションなどスキャン処理の詳細情報が記載されています。

12.3. 例外

特定のファイルをスキャンから例外と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テストファイルを例外としたり、オンデマンドスキャンから.aviファイルを例外としたい場合です。

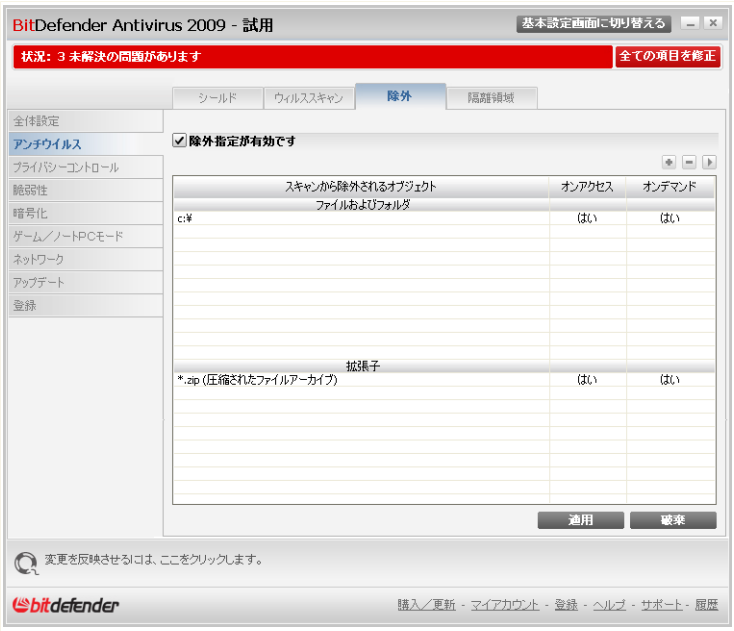
BitDefenderでは、オンアクセススキャンやオンデマンドスキャン、またはその両方でオブジェクトを例外とすることができます。この機能にはスキャンの時間を削減し、他の作業への影響を回避する狙いがあります。

スキャンから２種類のオブジェクトを例外とすることができます：

■パス - 指定したパスが示すファイルやフォルダ（その中のすべてのオブジェクトを含む）をスキャンから例外とします。
■拡張子 - 指定した拡張子を持つすべてのファイルをスキャンから例外とします。

注意
オンアクセススキャンから例外とされたオブジェクトは、ユーザやアプリケーションによってアクセスされた場合もスキャンされません。

スキャンから例外とされたオブジェクトの確認および管理を行うには、設定コンソールでアンチウイルス>例外をクリックします。



例外

スキャンから例外と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。各オブジェクトに関して、オンアクセススキャン，オンデマンドスキャン，あるいはその両方から例外とするのかを確認できます。

注意

ここで指定した例外はコンテキストスキャンには適用されません。 コンテキストスキャンはオンデマンドスキャンのひとつです：スキャンしたいファイルやフォルダを右クリックしてBitDefender 2009でスキャンを選択します。

表から項目を削除するには、項目を選択して 削除ボタンをクリックします。

表の項目を編集するには、項目を選択して 編集ボタンをクリックします。 新しいウィンドウが表示され、そこで例外とされる拡張子やパス、除外したいスキャン形式を必要に応じて変更できます。必要な変更を行いOKをクリックします。

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使用して編集や削除を行うこともできます。

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。

12.3.1. スキャンからパスを例外

スキャンからパスを例外とするには 追加ボタンをクリックします。 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例外にできます。

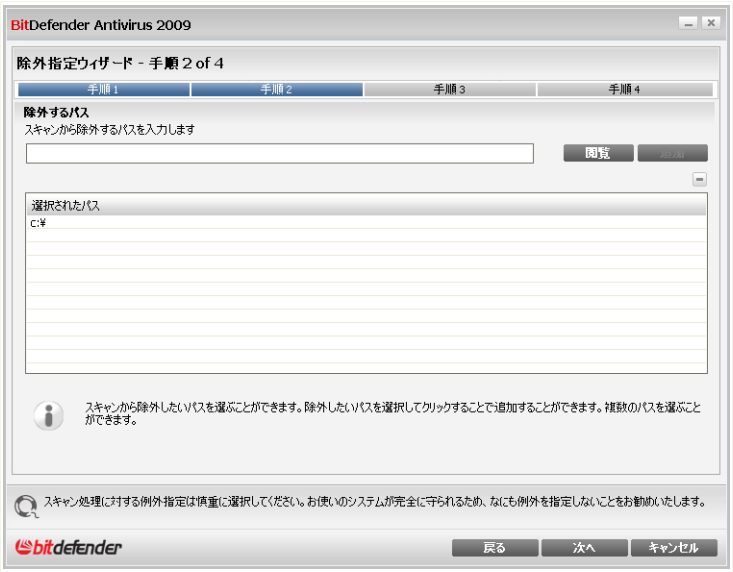
手順 1/4 - オブジェクト形式を選択

オブジェクト形式

スキャンからパスを例外にするオプションを選択します。

次へをクリックします。

手順 2/4 - 例外にするパスを指定



例外にするパス

スキャンから例外にするパスを指定するには、以下のいずれの方法を使用します：

- 参照をクリックしスキャンから例外にしたいファイルまたはフォルダを選択して追加をクリックします。
- スキャンから例外にしたいパスを編集欄に入力して追加をクリックします。

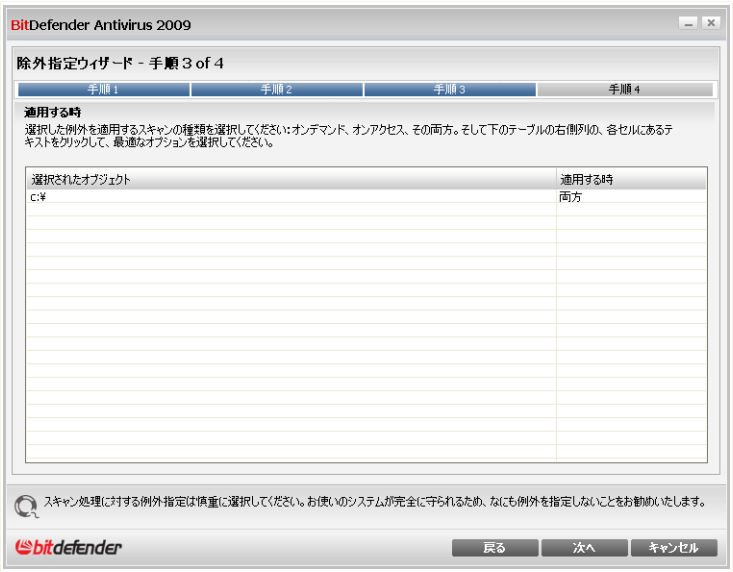
注意
指定したパスが存在しない場合はエラーメッセージが表示されます。OKをクリックしてパスが正しいか確認してください。

パスを追加すると一覧に表示されます。パスは必要な数だけ追加できます。

表から項目を削除するには、項目を選択して 削除ボタンをクリックします。

次へをクリックします。

手順 3/4 - スキャン方式を選択



スキャン方式

スキャンから例外にするパスと例外とするスキャン方式が記載された一覧を確認できます。

デフォルトでは、選択されたパスはオンアクセススキャンとオンデマンドスキャンの両方から例外にされます。例外にする対象を変更するには、右の列をクリックして一覧から対象オプションを選択します。

次へをクリックします。

手順 4/4 - 例外にしたファイルをスキャン

例外にしたファイルをスキャン

指定したパスにあるファイルをスキャンして感染していないことを確認することを強くお勧めいたします。 チェックボックスを選択してスキャン対象から例外にする前にスキャンします。

終了をクリックします。

適用をクリックして変更を保存します。

12.3.2. スキャンから拡張子を例外

スキャンから拡張子を例外にするには 追加ボタンをクリックします。 設定ウィザードが表示され、手順を追ってスキャンから拡張子を例外にできます。

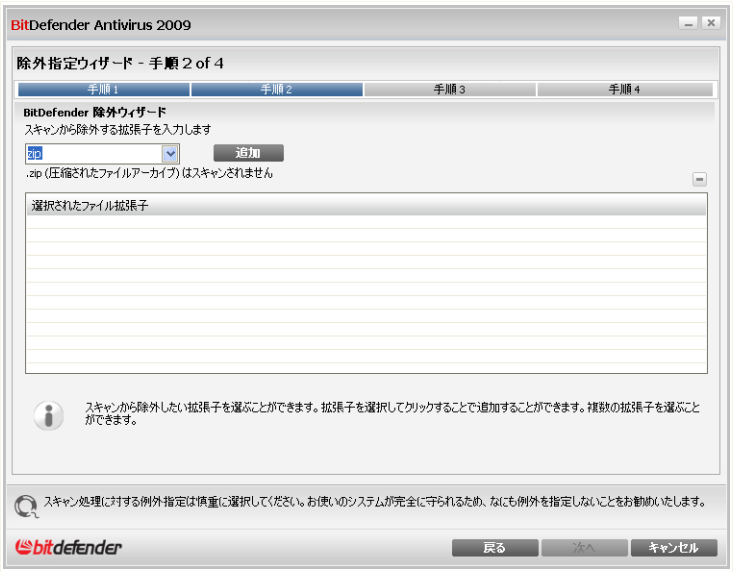
手順 1/4 - オブジェクト形式を選択

オブジェクト形式

スキャンから拡張子を例外にするオプションを選択します。

次へをクリックします。

手順 2/4 - 例外にする拡張子を指定



例外にする拡張子

スキャンから例外にする拡張子を指定するには、以下のいずれかの方法を使用します：

■スキャンから例外にしたい拡張子をメニューから選択して追加をクリックします。

注意
メニューにはシステムに登録されているすべての拡張子が一覧表示されます。拡張子を選択すると、説明があれば表示されます。

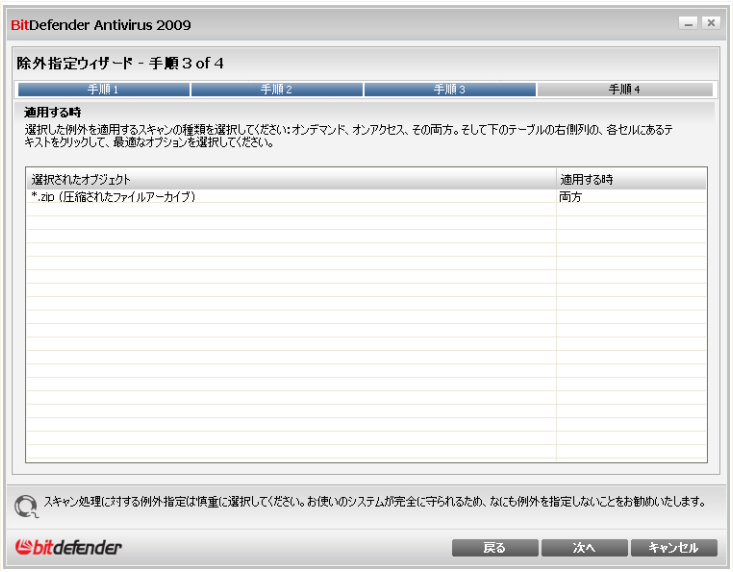
■スキャンから例外にしたい拡張子を編集欄に入力して追加をクリックします。

拡張子を追加すると一覧に表示されます。拡張子は必要な数だけ追加できます。

表から項目を削除するには、項目を選択して 削除ボタンをクリックします。

次へをクリックします。

手順 3/4 - スキャン方式を選択



スキャン方式

スキャンから例外にする拡張子と例外にされるスキャン方式が記載された一覧を確認することができます。

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例外とされます。例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。

次へをクリックします。

手順 4/4 - スキャン方式を選択

スキャン方式

指定した拡張子を持つファイルをスキャンして、感染していないことを確認することを強くお勧めいたします。

終了をクリックします。

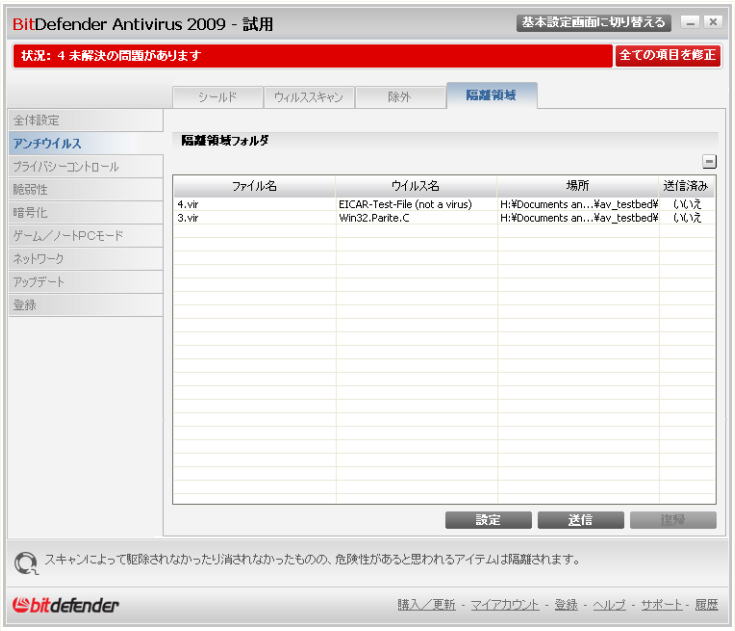
適用をクリックして変更を保存します。

12.4. 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ばれる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できるようになります。

さらにBitDefenderスキャンは隔離したファイルをマルウェアシグネチャアップデート後にスキャンします。 感染が除去されたファイルは自動的に元の場所に戻されます。

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行うには、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ます。



隔離領域

隔離領域セクションでは、隔離フォルダに隔離された全てのファイルを見ることができます。 隔離されたすべてのファイルごとに名前，検出されたウイルス名，元の場所へのパス，検出日が表示されます。

注意
隔離領域にあるウイルスを実行したり読み出したりすることはできないため、ウイルスが被害を及ぼすことはありません。

12.4.1. 隔離されたファイルを管理

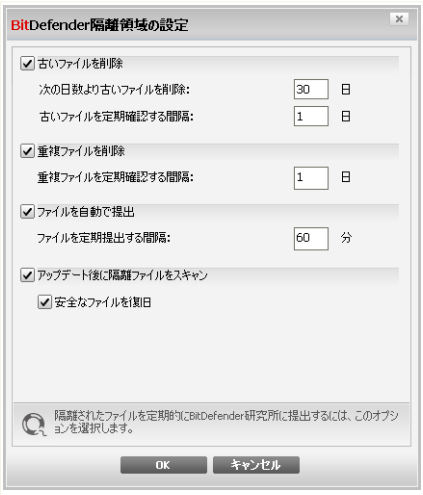
送信をクリックして隔離領域で選択したファイルをBitDefender研究所へ送ることができます。 デフォルトではBitDefenderは隔離ファイルを60分毎に自動的に送信します。

隔離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ます。選択したファイルを元の場所へ戻すには、復元をクリックします。

コンテキストメニュー. 隔離されたファイルの管理が容易に行えるようにコンテキストメニューが用意されています。先に説明したものと同じオプションが使用できます。また、更新を選択して隔離領域画面を更新することもできます。

12.4.2. 隔離領域設定を構成

隔離領域の設定を行うには設定をクリックします。 新しいウィンドウが開きます。



隔離領域の設定

隔離領域設定を使用してBitDefenderが以下のアクションを自動的に実行するように設定することができます：

古いファイルを削除します。. 古い隔離ファイルを自動的に削除するには、対応するオプションをチェックします。 隔離ファイルを削除されるまでの経過日数と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、30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。. 重複する隔離ファイルを自動的に削除するには、対応するオプションをチェックします。 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は重複する隔離ファイルを毎日確認します。

ファイルを自動的に送信します。. 隔離されたファイルを自動的に送信するには、対応するオプションをチェックします。 ファイルを送信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は隔離ファイルを60分毎に自動的に送信します。

アップデート後に隔離されたファイルをスキャン. アップデート後に自動で隔離されたファイルをスキャンするには、対応するオプションをチェックしてください。感染除去されたファイルを自動的に元の場所に戻すには 感染除去ファイルを戻すを選択します。

OKをクリックして変更を保存しウィンドウを閉じます。

13. プライバシーコントロール

BitDefenderは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、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や他のツールをブロックするのに有効です。

13.1. プライバシーコントロールの状態

プライバシー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、設定コンソールのプライバシーコントロール>状態をクリックします。

プライバシーコントロールの状態

ブロックされるアプリケーションが表示される表を確認できます。 プライバシーコントロールの有効/無効を変更したいときには、チェックボックスのチェックを入れたり外したりします。

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

プライバシーコントロールはこれらの重要な保護機能によってコンピュータを守ります：

- 個人情報コントロール - あなたの重要なデータを守るために、外に向けて発信されるweb (HTTP)、メール(SMTP)、そしてインスタントメッセンジャーの通信をフィルタリングします。そのルールの作成を個人情報セクションをで行います。
- レジストリコントロール - あるプログラムがWindows起動時に実行されるようレジストリの変更を試みた場合に、あなたの許可を要求します。
- Cookie 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たびにユーザの許可を要求します。
- スクリプトコントロール - ウェブサイトがスクリプトや他のアクティブなコンテンツを実行しようとするたびにユーザの許可を要求します。

画面の下にはプライバシーコントロールの統計が表示されます。

13.1.1. 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
弱	レジストリコントロールのみが有効です。
デフォルト	レジストリコントロールおよび個人識別情報コントロールは有効です。

保護レベル	説明
強	レジストリコントロール，個人識別情報コントロール、およびスクリプトコントロールは有効です。

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ます。 開いたウィンドウで有効にしたい保護オプションを選択しOKをクリックします。

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ます。

13.2. 個人情報コントロール

機密データの安全な保管はすべての人にとって重要な課題です。データの盗難はインターネット通信が発展するのと同じ速さで増え、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。

メールでもクレジットカード番号でも、悪の手に落ちれば被害が及ぶ可能性があります：迷惑メールの海に溺れるか、残高ゼロの口座に呆然とするかもしれません。

個人情報コントロールは個人情報がネットワークに漏洩することを防ぎます。 個人情報コントロールは、作られたルールに従って、ウェブ、メール、インスタントメッセージから特定の文字列（例えばクレジットカード番号）をスキャンします。もし該当する情報があった場合には、それらが流出するのを防ぎます。

ルールを作る際には電話番号、メールアドレス、口座番号などどれをルールに加えるか決めることができます。 システムを使う他のユーザに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。 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。

個人情報コントロールを使用する理由

- 個人情報コントロールはキーロガータイプのスパイウェアの活動を防ぐのに非常に強力です。 この種の悪意のあるアプリケーションは、あなたのキー入力を記録してそれをインターネットを介して悪意のある人物（ハッカー）に送ります。ハッカーはこの盗んだデータから重要な情報、銀行の口座番号とパスワードなどを見つけることができます。そしてそれを使って資産を取得するのです。

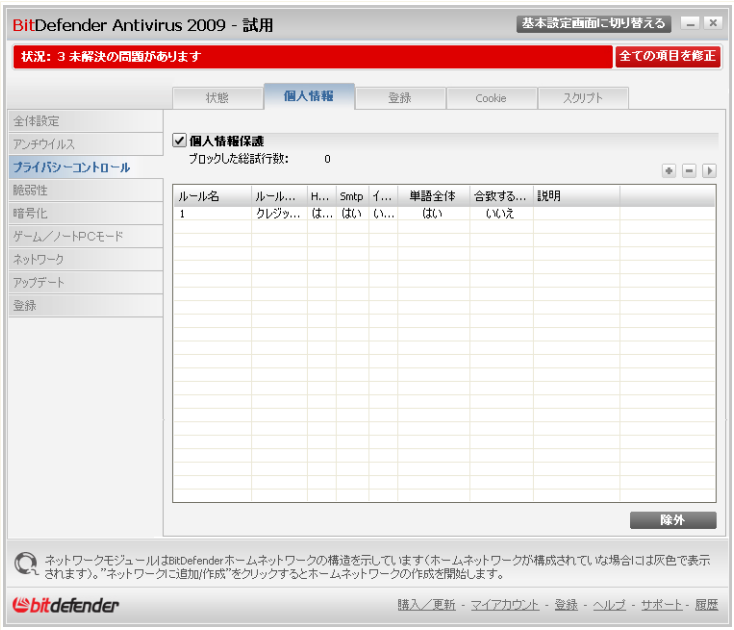
そのようなアプリケーションがアンチウィルスの検知をなんとか逃れたとしても適切な個人情報保護ルールが作成されていれば、盗み出したデータをメールやweb、インスタントメッセンジャーを使って送ることができません。

■個人情報コントロールは フィッシング の攻撃（個人情報を盗み出すような）からあなたを守ります。 もっとも一般的なフィッシング攻撃は、まずあなたを偽のメールでだまして、本物にそっくりなホームページで個人情報を入力させようとするものです。

例えばお使いの銀行からメールで急いで銀行に登録している情報を更新するように要請されます。 このメールにはホームページへのリンクが張られており、そこでは個人情報を入力しなければならないようになっています。 それは本物らしくみえますが、そのメールとホームページはあなたをだますための手段なのです。もしそのメールをクリックして、偽のホームページで個人情報を入力することで、この情報が、このフィッシングを詐欺を行った悪意のある人物に知られることになります。

もし適切な個人情報穂保護ルールが作成されていれば、クレジットカード番号などの個人情報をホームページで送信することはできません。送信するために個々のページごとに例外設定を明示する必要があります。

個人情報保護を設定するには、設定コンソールでプライバシーコントロール>個人情報をクリックしてください。



個人情報コントロール

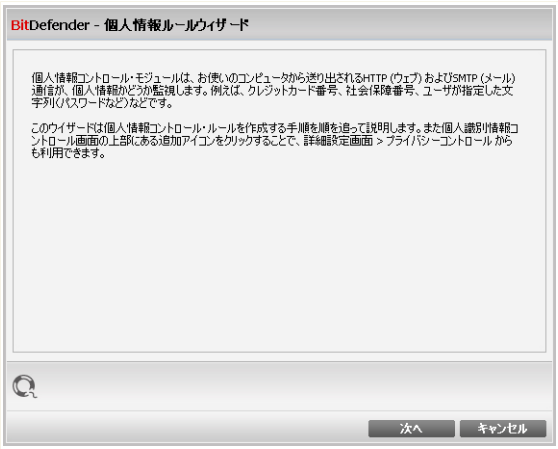
個人情報コントロールを使うには、以下の手順で設定します：

1. 個人情報コントロールチェックボックスを選択します。
2. あなたの重要なデータを守るルールを作成します　詳細については「個人情報のルールを作成」（p. 167）を参照してください。
3. 必要に応じて例外を定義することもできます。　詳細については「例外を定義」（p. 171）を参照してください。

13.2.1. 個人情報のルールを作成

個人情報保護のルールを作成するには 追加ボタンを押してウィザードにそって設定します。

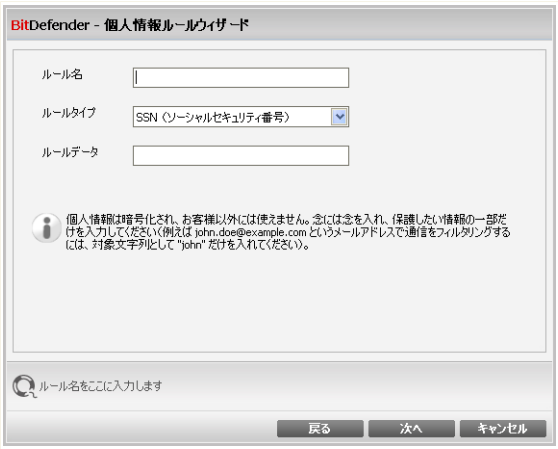
手順 1/4 - はじめに



はじめに

次へをクリックします。

手順 2/4 - 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

以下の内容を設定する必要があります：

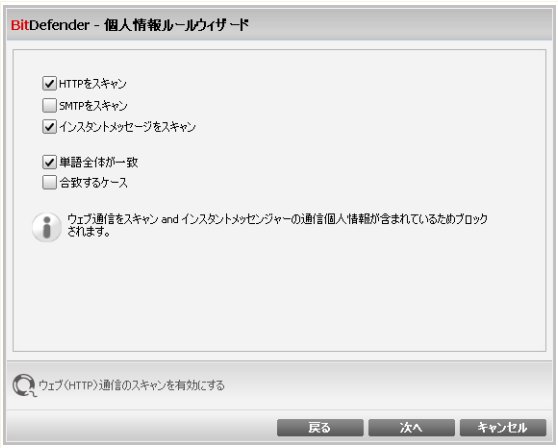
- ルール名 - 編集欄に新しい名前を入力してください。
- ルールの形式 - 住所、名前、クレジットカード、PIN（個人識別番号）、SSN（ソーシャルセキュリティ番号）などのルールの形式を選択してください。
- ルールデータフィールドに、送信したくない文字列の種類を入力します。 例えばクレジットカード番号を保護する場合には、ここに全ての形式または形式の一部を入力します。

> **注意**
> 入力した内容が３文字未満の場合、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文字は入力することをお勧めします。

入力されたデータはすべて暗号化されます。安全性を高めるため保護したいデータをすべて入力することは避けてください。

次へをクリックします。

手順 3/4 - 通信を選択



通信を選択

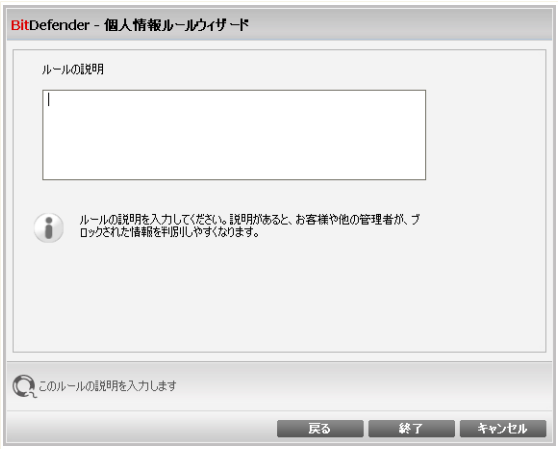
BitDefenderにスキャンさせたい通信形式を選択します。 以下のオプションを指定できます：

- HTTPをスキャン - HTTP（ウェブ）通信をスキャンして、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）通信をスキャンして、ルールのデータと一致する送信メールをブロックします。
- インスタントメッセージをスキャン - インスタントメッセージをスキャンし、ルールのデータと一致するメッセージをブロックします。

ルールのデータが単語全体と一致した場合のみ、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のみ、ルールが適用されるように指定できます。

次へをクリックします。

手順 4/4 - ルールの説明



ルールの説明

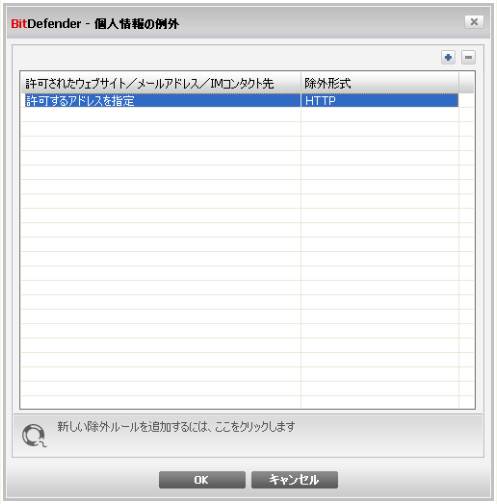
編集欄にルールの簡単な説明を入力します。 ルールに該当してブロックされた情報は表示されないときには、この説明が役に立ちます。

終了をクリックします。 新しいルールが表に表示されます。

13.2.2. 例外を定義

特定の個人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。 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ためのルールを作成した場合を考えてみましょう。この場合は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たびに、対象となるページがブロックされます。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場合には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ィンドウを開くには、例外をクリックします。



例外

例外を追加するには以下の手順に従ってください：

1. 追加をクリックして、表に新しい項目を追加します。
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ホームページアドレス、メールアドレス、ＩＭのコンタクト先名を入力します。
3. 形式を選択をダブルクリックして先に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ます。
   ■ウェブアドレスを指定した場合はHTTPを選択してください。
   ■メールアドレスを指定した場合はSMTPを選択してください。
   ■ＩＭコンタクト先を指定したら IMを選択します。

一覧から例外を削除するには対象を選択して削除をクリックします。

OKをクリックして変更を保存します。

13.2.3. ルールを管理

これまでに作成したルールが表に記載されます。

あるルールを削除するには、それを選択して 削除 ボタンをクリックします。

ルールを編集するには、対象を選択して編集ボタンをクリックするかダブルクリックしてください。新しいウィンドウが開きます。

ルールを編集

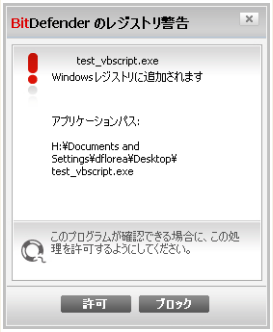
ルールの名前、説明、内容（形式、データ、通信）をここで変更できます。OKをクリックして変更を保存してください。

13.3. 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存する場所です。

レジストリは、Windows起動時に自動的に起動するプログラムを指定するためにも使用されます。ユーザがコンピュータを再起動した時に自動的に起動されるようにウイルスは多くの場合レジストリを利用します。

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のに効果的です。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ユーザに警告します。



レジストリ警告

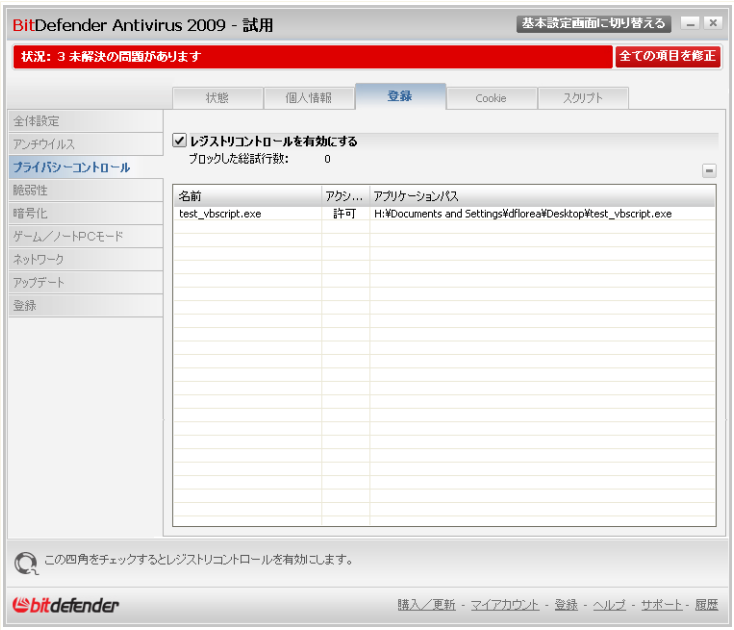
Windowsのレジストリを変更しようとしているプログラムを見ることができます。

もしそのプログラムが不明で疑わしいものでしたら ブロックをクリックしてWindowsレジストリの変更を防ぎます。 もしくは許可をクリックして変更を許可します。

あなたが行った回答に基づいてルールが作成されルール表に表示されます。 このプログラムがレジストリを変更しようとした場合は同じ処理を適用します。

注意
コンピュータが次に起動された後で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はユーザに警告します。ほとんどの場合はこうしたプログラムに問題はなく信頼できます。

レジストリコントロールを設定するには、詳細設定画面の設定コンソールでプライバシーコントロール>レジストリ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。

あるルールを削除するには、それを選択して 削除 ボタンをクリックします。

13.4. 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。コンピュータに保管される小さなファイルでユーザに関する特定の情報を記録するためにウェブサイトが作成します。

Cookieは一般的にユーザの手間を省くために作成されます。例えばウェブサイトがユーザの名前や参照情報を記憶して、ユーザがサイトを訪れるたびに入力しなくてもよいようにすることができます。

しかし、Cookieがユーザのウェブ閲覧行動を監視して、個人情報を漏洩するために使用さ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たびにCookieコントロールがユーザの許可を求めます。

Cookie警告

Cookieを送信しようとしているアプリケーションの名前を確認できます。

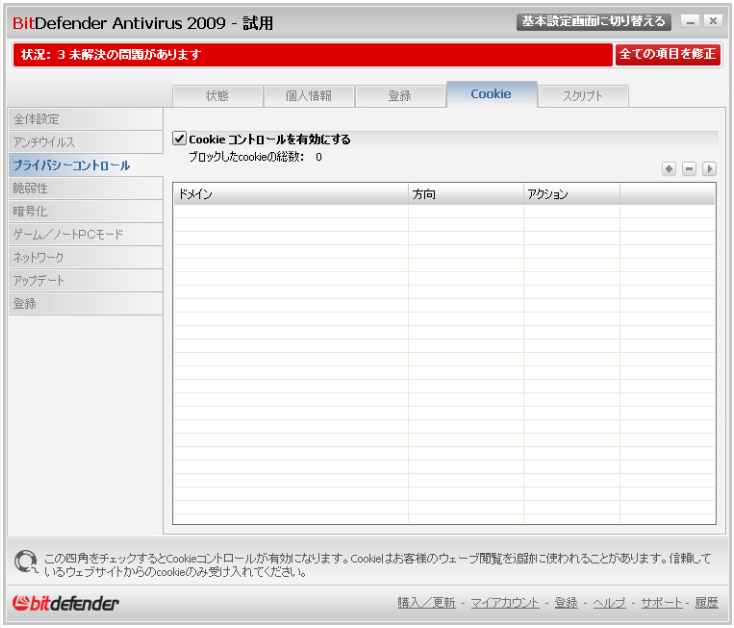
この回答を記憶オプションをチェックし、はいまたはいいえをクリックすると、ルールの作成と適用が行われルール表に記載されます。同じサイトに接続しても次回からは通知されません。

どのウェブサイトを信頼して、どのサイトを信頼しないか、選択するのに役立ちます。

注意

今日では大量のCookieがインターネットで使用されているため、最初はCookieコントロールを煩わしく感じるかもしれません。最初のうちは、コンピュータにCookieを保存しようとするサイトに関して、多くの問い合わせを受けることになります。よく訪問するサイトをルール一覧に追加することで、それまでと同じように容易にサイトを閲覧できるようになります。

Cookieコントロールを設定するには、詳細設定画面の設定コンソールでプライバシーコントロール>Cookie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。

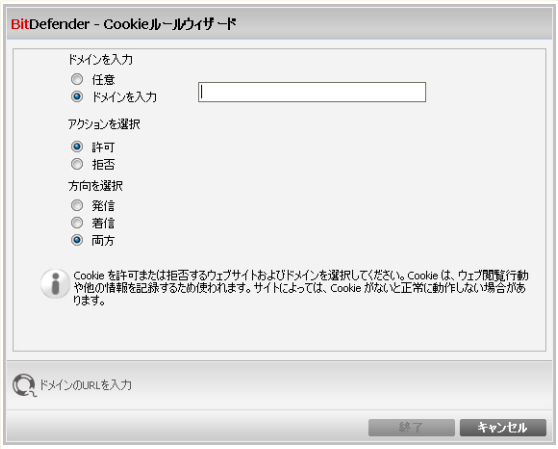
重要項目
ルールは上から順番に、優先度に従って並べられます。つまり、最初のルールが最も高い優先度を持っています。ルールの優先度を変更するにはドラッグ&ドロップで順番を入れ替えます。

あるルールを削除するには、それを選択して 削除 ボタンをクリックします。ルールパラメータを変更するには、そのルールをダブルクリックして設定ウィンドウで変更を行います。

手動でルールを追加する場合には追加ボタンをクリックして設定ウィンドウでルールパラメータを設定します。

13.4.1. 設定ウィンドウ

編集もしくは手動でルールを追加した場合にはこの設定ウィンドウが表示されます。



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 - 通信方向を選択します。

形式	説明
送信	接続されたサイトに送り返されるCookieにのみルールが適用されます。

形式	説明
受信	接続されたサイトから受け取るCookieにのみルールが適用されます。
両方	双方向にルールが適用されます。

注意
Cookieを受け入れても返信はしない場合は、アクションを拒否に、方向を送信に設定します。

終了をクリックします。

13.5. 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用されるActiveX コントロールやJava アプレットなどのコードは、害を与えるようにプログラムすることができます。例えばActiveXエレメントはデータ全体にアクセスして、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、ネットワーク接続中にメッセージを横取りしたりすることができます。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ることをお勧めします。

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、どのサイトを信頼しないかユーザが決定します。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たびにユーザの許可を求めます。

スクリプト警告

リソース名を確認できます。

この回答を記憶オプションをチェックして、はいまたはいいえをクリックすると、ルールの作成および適用が行われ、ルール表に記載されます。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。

スクリプトコントロールを設定するには、詳細設定画面の設定コンソールでプライバシーコントロール>ウェブ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。

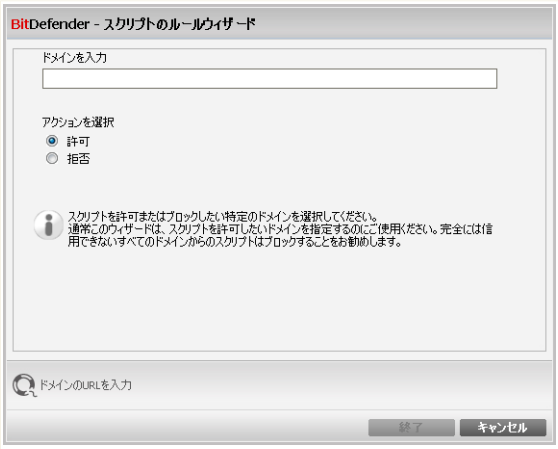
重要項目
ルールは上から順番に、優先度に従って並べられます。つまり、最初のルールが最も高い優先度を持っています。ルールの優先度を変更するにはドラッグ&ドロップで順番を入れ替えます。

あるルールを削除するには、それを選択して 削除 ボタンをクリックします。ルールパラメータを変更するには、そのルールをダブルクリックして設定ウィンドウで変更を行います。

手動でルールを作成するには 追加ボタンをクリックして設定ウィンドウでルールパラメータを設定します。

13.5.1. 設定ウィンドウ

編集もしくは手動でルールを追加した場合にはこの設定ウィンドウが表示されます。



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	ドメインのスクリプトが実行されます。
拒否	ドメインのスクリプトは実行されません。

終了をクリックします。

14. 脆弱性

悪意のある人物、アプリケーションからお使いのコンピュータを守るために重要なことは、OSや普段使うアプリケーションをいつも最新のものにし続けることです。さらにコンピュータへ認証されていない直接的なアクセスを防ぐためには、強力なパスワード（容易に類推されない）が各Windowsユーザ毎に設定されていなければなりません。

BitDefenderは定期的にお使いのシステムの脆弱性をチェックして、存在していればそれをあなたに知らせます。

14.1. 状況

自動的に脆弱性をチェックしたり脆弱性チェックを実行するには、詳細設定画面にある脆弱性>ステータスを表示します。

脆弱性の状況

この表では最近行った脆弱性チェックとそのステータスが表示されています。 各脆弱性に対してどのような対処を行うべきか、それがある場合には確認することができます。 もし なしとなっていればその項目には脆弱性がありません。

重要項目
自動的にシステム、アプリケーションの脆弱性を通知させるには、自動脆弱性チェックを有効の状態にしておいてください。

14.1.1. 脆弱性の解消

特定の脆弱性を解消するには、それを選択して個々の事項に応じて提供される処理を行ってください：

- もしWindowsアップデートが利用可能なら全てのシステムアップデートをインストールをクリックして、それらをインストールしてください。
- もしアプリケーションが古くなっている場合には、ホームページリンクを使って、そのホームページからアプリケーションの最新版をインストールしてください。
- もしあるWindowsユーザアカウントのパスワード強度が弱いものであれば、そのユーザにパスワードを次回のログオン時に変更させるか、強制的にパスワードを変更してください。 強いパスワードを作るためには、大文字と小文字を混ぜる、数字と記号（例えば #, $, @）を使います。

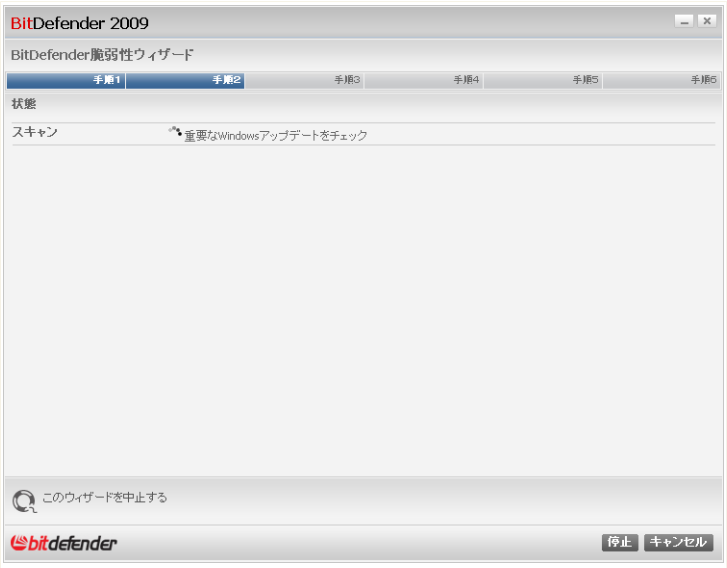
今すぐチェック をクリックして、ウィザードに従ってその脆弱性を手順にそって解消します。

手順 1/6 - 脆弱性チェックを選択

脆弱性

次にをクリックし選択した脆弱性チェックを行います。

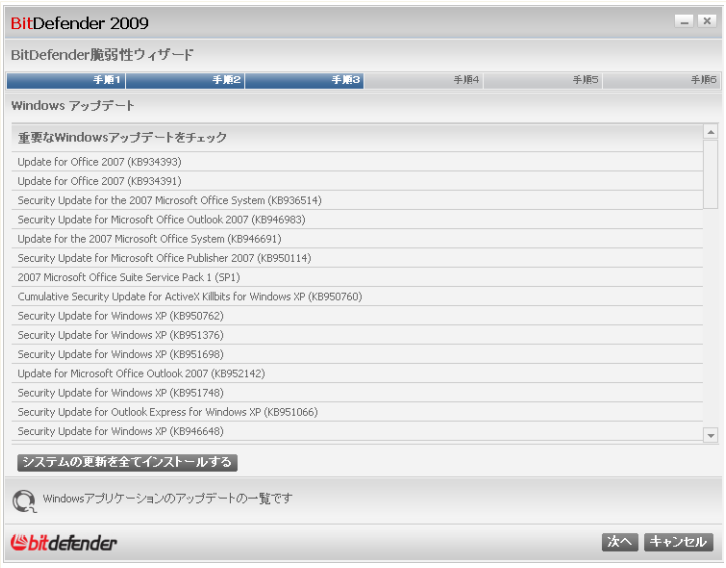
手順 2/6 - 脆弱性チェック



脆弱性チェック

BitDefenderが脆弱性チェックを完了するまでお待ちください。

手順3/6 - Windowsをアップデートする



Windowsアップデート

このコンピュータにインストールされていないアップデート、クリティカルなアップデート、クリティカルではないアップデートがそれぞれ表示されます。　全てのアップデートをインストールするをクリックすると、インストール可能な全てのアップデートをインストールします。

次へをクリックします。

手順 4/6 - アプリケーションのアップデート

アプリケーション

BitDefenderがアップデートが必要なアプリケーションをチェックしリストを作成します。 もしアプリケーションが最新でない場合には、最新版をダウンロードするをクリックします。

次へをクリックします。

手順5/6 - 弱いパスワードを変更

パスワードを入力

このコンピュータのWindowsアカウントに設定されているパスワードに脆弱性がないか確認することができます。 パスワードは 堅固（推測困難）にも 脆弱（容易に悪意をもった人々の特化したソフトウェアにより類推可能)にもなりえます。

修正をクリックして弱いパスワードを変更します。 新しいウィンドウが開きます。

パスワードを変更

この問題を修正する方法を選択してください：

■次のログイン時に強制的にパスワード変更. BitDefenderはユーザが次にWindowsにログインするときにパスワード変更するようにプロンプトを表示します。

■パスワード変更. 入力欄に新しいパスワードを入力します。 パスワード変更するようユーザに通知する

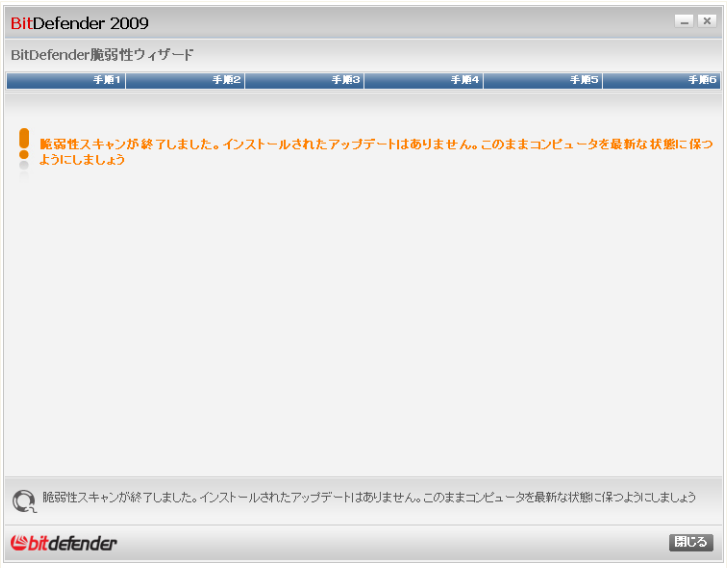
注意

強いパスワードを作るためには、大文字と小文字を混ぜる、数字と記号 （例えば #, $, @）を使います。 堅固なパスワードについてはインターネットを検索すると様々な役立つ情報があります。

OKをクリックするとパスワードが変更されます。

次へをクリックします。

手順 6/6 - 結果を表示する



結果

閉じるをクリックします。

14.2. 設定

自動的に脆弱性チェックを行うよう設定するには、詳細設定画面にある脆弱性>設定を表示します。

自動脆弱性チェックの設定

定期的にチェックしたいシステムの脆弱性に対応するチェックボックスを選択します。

■クリティカルなWindowsアップデート
■通常のWindowsアップデート
■アプリケーションアップデート
■弱いパスワード

注意
もし特定の脆弱性項目のチェックボックスをクリアした場合、BitDefenderは指定項目に関してそれ以上脆弱性の通知を行いません。

15. インスタントメッセージ(IM) 暗号化

初期設定ではBitDefenderは全てのインスタントメッセンジャーでの会話を暗号化します：

■インスタントメッセンジャーの相手がBitDefenderのIM暗号化をサポートしているバージョンを使用している必要があります。

■Yahoo! Messenger（英語版）かMSN Messengerを使用する必要があります。

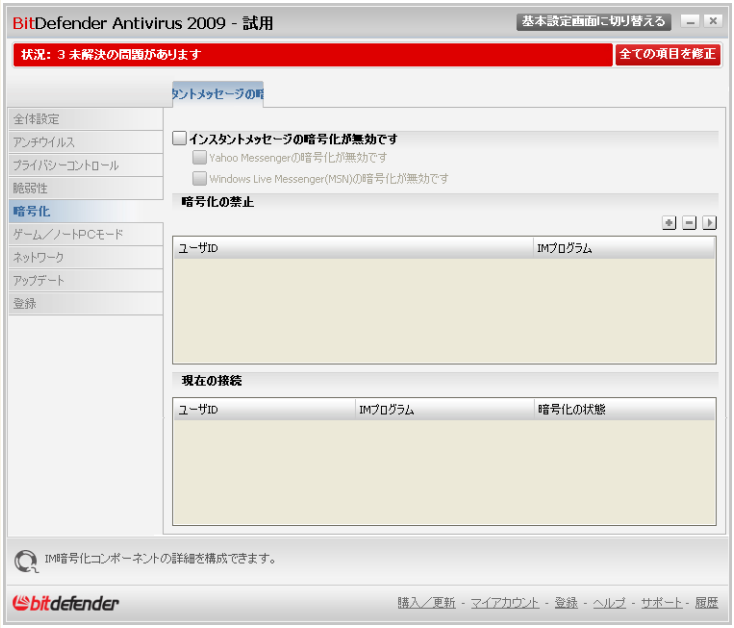
重要項目

BitDefenderはもし相手がウェブベースのチャットアプリケーションを使用している場合、例えば、MeeboやYahoo MessengerやMSNをサポートするチャットアプリケーションでは会話を暗号化しません。

インスタントメッセージの暗号化の設定は、詳細設定画面にある暗号化>IM 暗号化で行います。

注意

インスタントメッセンジャーの暗号化はチャットウィンドウにあるBitDefenderツールバーから簡単に設定することができます。 詳細については「インスタントメッセンジャープログラムへの統合」 (p. 50)を参照してください。



インスタントメッセージ暗号化

デフォルトでは、IM暗号化はYahoo Messenger（英語版）とWindows Live（MSN）で有効になっています。 IM暗号化を特定のチャットアプリケーションだけもしくは全てで、無効にすることができます。

２つの表が表示されています：

■暗号化対象外 - 暗号化が無効になっているユーザIDと関連するIMプログラムが一覧となっています。 一覧からコンタクト先を取り除くには、それを選択して削除ボタンをクリックします。

■現在の接続 - 現在のインスタントメッセンジャーのの接続（ユーザID、関連IMプログラム）の一覧です。暗号化、非暗号化の両方が含まれます。 接続は次の理由のため暗号化されていません：

・ 各コンタクト先に対して暗号化を無効にするように設定されています。

- コンタクト先がIM暗号化をサポートしているBitDefenderをインストールしていません。

15.1. 特定のユーザに対して暗号化を無効にする

特定のユーザに対して暗号化を無効にするには次の手順を行います：

1. 追加ボタンをクリックして設定ウィンドウを開きます。

コンタクト先を追加

2. コンタクト先のユーザIDを編集フィールドに入力します。
3. このコンタクト先に関連するインタスタントメッセージアプリケーションを選択
4. OKをクリックします。

16. ゲーム/ノートＰＣモード

ゲーム/ノートＰＣモジュールはBitDefederを特別な動作モードで動かすことを可能にします。

■ゲームモード は一時的に製品の設定を変更してゲーム中のリソースの消費を最小限にします。

■ノートＰＣモード では、バッテリーで動作している際にはバッテリーを長持ちさせるためにスケジュール実行されるタスクを行いません。

16.1. ゲームモード

ゲームモードは一時的に保護設定を変更してシステムパフォーマンスに与える影響を最小限にします。 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リアルタイムプロテクションレベルは弱に設定されています。

■アップデートはデフォルトでは行いません。

注意
設定を変更するには アップデート>設定においてゲームモードではアップデートをしないチェックボックスのチェックをはずします。

■スケジュールスキャンはデフォルトでは無効となっています。

デフォルトではBitDefenderは、BitDefederが持っている主要ゲームリストにあるゲームを起動した場合、またはアプリケーションがフルスクリーンになった場合に自動的ゲームモードに移行します。 手動でゲームモードに切り替えるには、デフォルトではCtrl+Alt+Shift+Gキーで行います。 ゲームを終えたらただちにゲームモードを終了してください(同じくデフォルトでは Ctrl+Alt+Shift+Gキーで行えます)。

注意
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。

ゲームモードの設定を行うには、詳細設定画面のゲーム/ノートPCモード>ゲームモードを表示します。

ゲームモード

このセクションの一番上でゲームモードのステータスを確認することができます。ゲームモードを開始またはゲームモードを終了をクリックして現在のステータスを変更することができます。

16.1.1. 自動ゲームモードの設定

自動ゲームモードではBitDefenderがゲームを検知すると自動的にゲームモードに移行します。 以下のオプションを設定することができます：

■BitDefenderが提供するデフォルトのゲームリストを使用 - BitDefenderが持っている主要なゲームリストにあるゲームが起動されると自動的にゲームモードに移

行します。 このリストを見る場合には ゲーム管理をクリックして許可されているゲームを見るを選択します。

- フルスクリーン時にゲームモードに移行する - アプリケーションがフルスクリーン表示になった場合に自動的にゲームモードに移行します。
- ゲームリストに追加するかを確認 - フルスクリーンを終えたときにユーザにアプリケーションを追加するかの確認を行います。 ゲームリストに新しいアプリケーションを追加すると、次回以降それを起動するとBitDefenderは自動的にゲームモードに切り替わります。

注意
BitDefenderが自動的にゲームモードに切り替わるのを止めるには自動ゲームモードチェックボックスを外します。

16.1.2. ゲームリストを管理

BitDefenderはゲームリストからアプリケーションを起動すると自動的にゲームモードに移行します。 ゲームリストを管理するためにはゲーム管理をクリックします。 新しいウィンドウが開きます。

ゲームリスト

新しいアプリケーションは次の場合に自動的にこのリストに追加されます：

■BitDefenderが持つ主要ゲームリストからゲームを起動する。 このリストをみるには許可されているゲームをみるをクリックします。

■フルスクリーンから戻る際にそのアプリケーションを確認画面でゲームリストに追加する。

自動ゲームモードをゲームリストにある特定のアプリケーションで無効にする場合には、該当するチェックボックスを外します。 通常フルスクリーンに移行するアプリケーションの場合には自動ゲームモードを無効にすべきです。たとえばwebブラウザーやムービープレイヤーなどです。

ゲームリストを管理するには、この表の一番上にあるボタンを使用します：

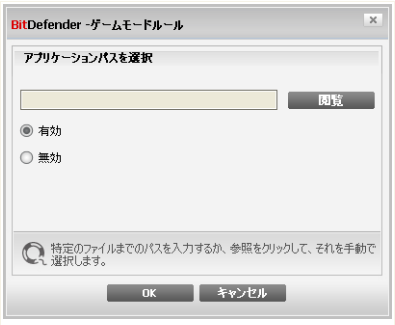
■ 追加 - 新しいアプリケーションをゲームリストに追加します。

■ 除去 - ゲームリストからアプリケーションを取り除きます。

■ 編集 - ゲームリストにある項目を編集します。

ゲームの追加、編集

ゲームリストにある項目に追加、編集すると、次の画面が表示されます：



ゲームの追加

表示をクリックしてアプリケーションを選択またはアプリケーションまでのフルパスをテキスト欄に入力します。

選択したアプリケーションの起動時に自動的にゲームモードに移行させたくない場合には 無効を選択します。

OKクリックしてゲームリストにその項目を追加します。

16.1.3. ゲームモードの設定

スケジュールタスクのふるまいを設定するには次のオプションを使用します：

■スキャンタスク － ゲームモードで実行している場合にはスケジュールされたスキャンタスクを行いません。 以下のオプションから選択できます：

オプション	説明
タスクをスキップ	スケジュールタスクを全く実行しない。
タスクの延期	ゲームモードが終了したタイミングでスケジュールされたタスクを実行します。

16.1.4. ゲームモードのホットキーを変更

手動でゲームモードに切り替えるには、デフォルトではCtrl+Alt+Shift+Gキーで行います。 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. 詳細設定 新しいウィンドウが開きます。

詳細設定

2. 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)

   ■入力欄に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
   ホットキーを使うのチェックを外すことで、ホットキーを無効にすることができます。

3. OKをクリックして変更を保存します。

16.2. ノートＰＣモード

ノートＰＣモードはノートパソコンユーザ向けに特別に設計されたモードです。目的はパソコンがバッテリーで動作している際に、BitDefenderが消費電力に与える影響を最小限にすることです。

ノートＰＣモードでは、スケジュールされたタスクはデフォルトでは延期されます。

BitDefenderがノートパソコンがバッテリーに切り替わったことを検知すると、自動的にノートＰＣモードに移行します。 同様にBitDefenderはノートパソコンがバッテリーから通常電源に戻ったことを検知するとノートＰＣモードを終了します。

ノートＰＣモードを設定するには、詳細設定画面のゲーム/ノートＰＣモード>ノートＰＣモードを表示します。

ノートＰＣモード

ノートＰＣモードが有効かそうでないかを確認できます。 ノートＰＣモードが有効な場合、BitDefenderはバッテリーで動作している場合は指定された設定を適用します。

16.2.1. ノートＰＣモードの設定

スケジュールタスクのふるまいを設定するには次のオプションを使用します：

■スキャンタスク - ノートＰＣモードで実行している場合にはスケジュールされたスキャンタスクを行いません。 以下のオプションから選択できます：

オプション	説明
タスクをスキップ	スケジュールタスクを全く実行しない。

オプション	説明
タスクの延期	ノートＰＣモードが終了したタイミングでスケジュールされたタスクを実行します。

17. ネットワーク

ネットワークモジュールを使うとBitDefender製品がインストールされているご家庭内のコンピュータを一元管理することができます。

ネットワークマップ

BitDefender製品がインストールされている家庭内のコンピュータを管理するには、次の手順を行ってください：

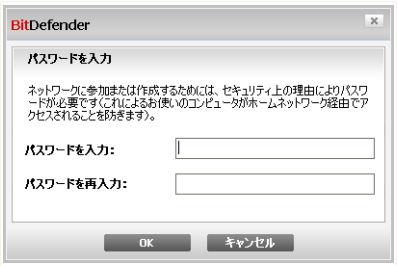
1. コンピュータからBitDefenderネットワークに参加する ネットワークに加わるためにはホームネットワーク管理のための管理者パスワードを必要とします。
2. 管理したいコンピュータをそれぞれネットワークに参加させます(パスワードを設定してください)

3. コンピュータに戻って管理したいコンピュータを追加してください

17.1. BitDefenderネットワークに参加する

BitDefender home networkに参加するには、以下の手順に従ってください：

1. ネットワークに参加する/つくるをクリックする ホームネットワークを管理するパスワードを決めます。



パスワード設定

2. それぞれの入力欄に同じパスワードを入力します。
3. OKをクリックします。

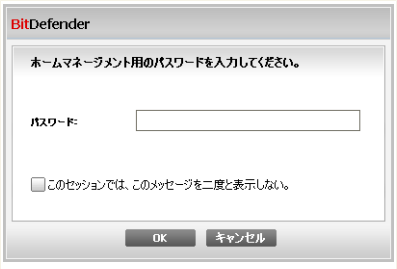
ネットワークマップ上にコンピュータ名が表示されます。

17.2. BitDefenderネットワークにコンピュータを追加する

BitDefenderホームネットワークにコンピュータを追加するには、はじめにBitDefenderホームネットワークを管理するためのパスワードを個々のコンピュータへ設定しなければなりません。

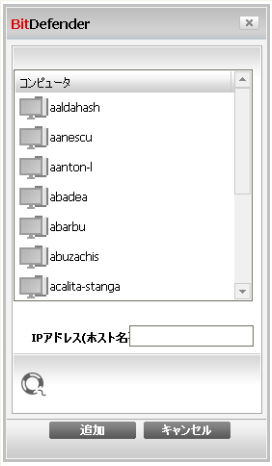
BitDefenderホームネットワークにコンピュータを追加するには、次の手順を行ってください：

1. ネットワークを管理するをクリックしてください。 ホームネットワークを管理するためのパスワードを決めます。



パスワードを入力

2. ホームネットワークを管理するパスワードを入力してOKをクリックします。 新しいウィンドウが開きます。



コンピュータを追加

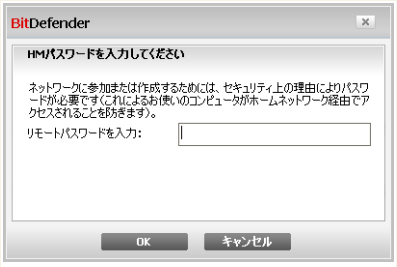
ネットワークに参加しているコンピュータの一覧を確認できます。 アイコンの意味は次の通りです：

■ オンラインでBitDefenderがインストールされていないコンピュータ

■ オンラインでBitDefenderがインストールされているコンピュータ

■ オフラインでBitDefenderがインストールされているコンピュータ

3. 以下のいずれかを実行します：
   ■ネットワークに追加するコンピュータ名を選択します
   ■IPアドレスかコンピュータ名を入力します。
4. 追加をクリックします。　それぞれのコンピュータを管理するパスワードを決めます。



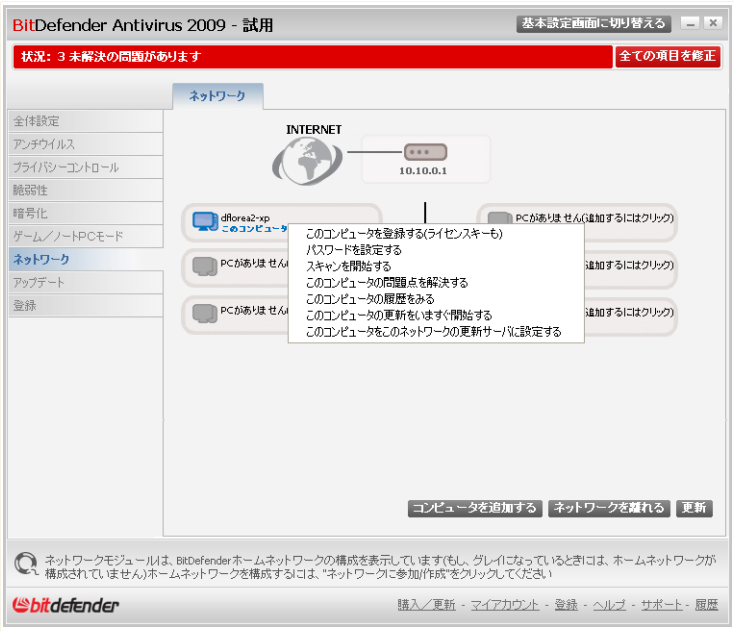
認証

5. ホームネットワーク管理者パスワードはそれぞれのコンピュータに設定します。
6. OKをクリックします。　正しいパスワードを入力すると選択したコンピュータがネットワークマップに表示されます。

注意
コンピュータを最大５台までネットワークマップに追加することができます。

17.3. BitDefenderネットワークを管理する

BitDefenderホームネットワークを作成すると１台のコンピュータから全てのBitDefender製品を管理することができます。



ネットワークマップ

ネットワークマップ上のコンピュータにマウスカーソルを当てるとコンピュータ名・IPアドレス・セキュリティに関する問題点の数・BitDefender製品登録の状態などの情報を見ることができます。

ネットワークマップのコンピュータ名の上で右クリックをするとリモートのコンピュータに対して管理作業を行うことができます。

■このネットワークから削除

■このコンピュータを登録

■パスワードの設定

■スキャンを実行

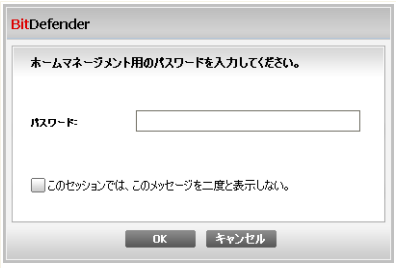
■このコンピュータの問題点を修正

■このコンピュータの履歴を表示

■このコンピュータをすぐにアップデートする

■このコンピュータをこのネットワークのアップデートサーバにする

特定のコンピュータでタスクを実行する前に管理用のパスワードを入力する必要があります。



パスワードを入力

ホームネットワークを管理するパスワードを入力してOKをクリックします。

注意

いくつかのタスクを実行させる場合には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。　このオプションを選択した場合には、このセッションの間にもう一度パスワードを入力する必要があります。

18. アップデート

毎日のように新しいマルウェアが発生・検出されており、それに対処するにはBitDefenderを最新のマルウェアのシグネチャで更新することがとても重要です。

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。デフォルトではコンピュータの起動時、およびその後は１時間ごとにアップデートをチェックします。

アップデートファイルを見つけた場合に更新を確認するか自動的に更新をするかは自動更新設定に依存します。

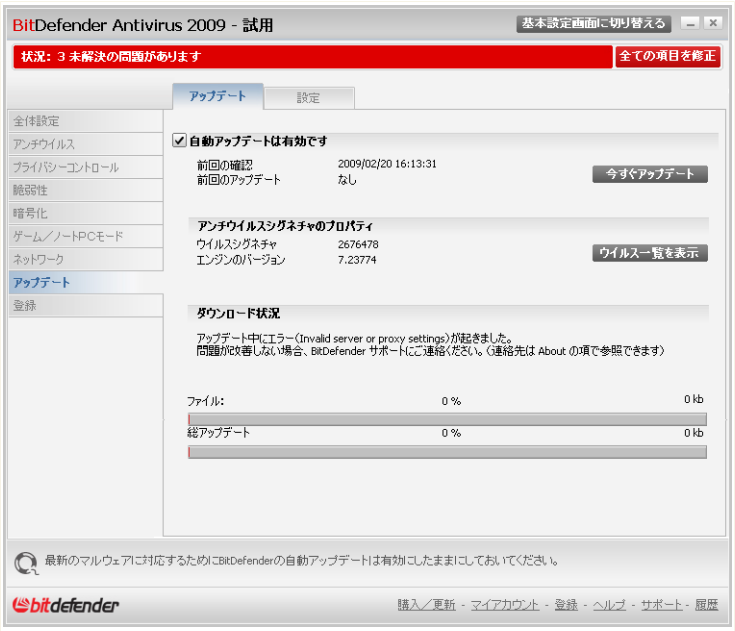
アップデート処理はその場で実行されます。つまりアップデートされるファイルは、順次上書きされていきます。この方法によりアップデート処理は製品の動作に影響せず、同時に脆弱性も除外されます。

アップデートは以下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時、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。

18.1. 自動アップデート

アップデート関連の情報を表示して、自動アップデートを実行するには、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。エンジンのバージョンやシグネチャの数も表示されます。

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するには自動アップデートを有効にしておいてください。

お使いのBitDefenderがもっているマルウェアの定義はウィルスリストの表示をクリックすることで知ることができます。全ての利用可能な定義を含んだHTMLファイルが作成されブラウザで表示されます。また特定のマルウェアの定義をデータベースで検索したり、BitDefender ウィルスリストをクリックすることでオンラインのBitDefnder定義データベースに行くことができます。

18.1.1. アップデートを要求

自動アップデートは今すぐアップデートをクリックすることでいつでも実行できます。このアップデートはユーザによるアップデートとしても知られています。

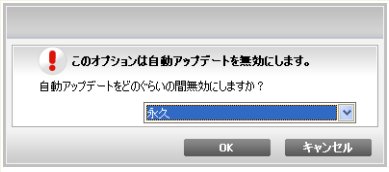
アップデートモジュールは、BitDefenderのアップデートサーバに接続しアップデートがあるかどうか確認します。アップデートが見つかると手動アップデートの設定画面で指定したオプションに応じてアップデートの実行を確認するか自動でアップデートが実行されます。

重要項目
アップデート完了時にコンピュータの再起動が必要な場合があります。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場合は、ユーザ要求によってBitDefenderのアップデートを定期的に行うことをお勧めします。

18.1.2. 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ィンドウが開きます。



自動アップデートを無効にする

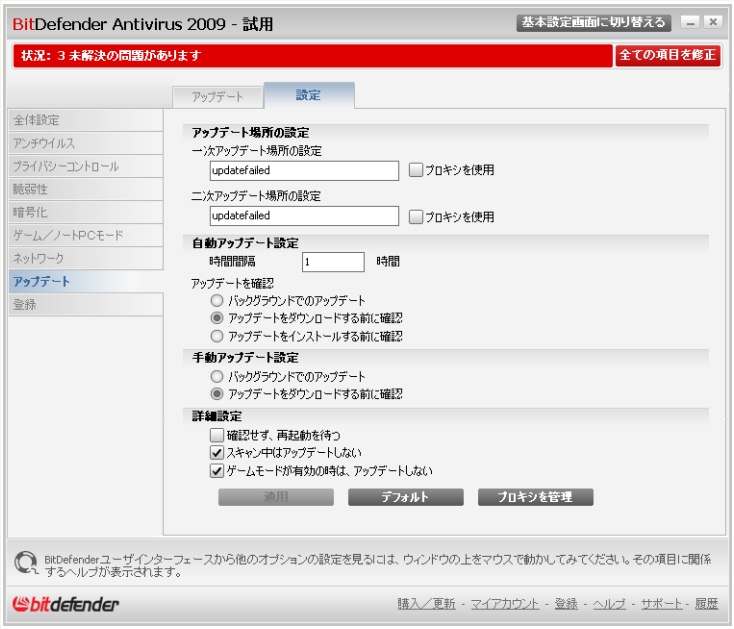
自動アップデートを無効にする期間をメニューから選択して、この選択項目を確認してください。5, 15, 30分、１時間、永続的、または次のシステム再起動まで、のいずれかの期間自動アップデートを無効にできます。

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最新の脅威から保護することができません。

18.2. 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時間ごとにアップデートを確認しユーザ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つのカテゴリに分類されています（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。

18.2.1. 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用してください。

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のみ、これらの設定を行ってください。

アップデートの場所を２ヶ所設定して、さらに安定した高速のアップデートを実現できます：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、同じ場所が設定されます：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を入力します。

注意
ローカルミラーが使えなくなった場合を想定して、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。 詳細については「プロキシを管理」 (p. 216)を参照してください。

18.2.2. 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用してください。

時間間隔入力欄でアップデートの時間間隔を指定できます。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、以下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ユーザに確認します。
■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ユーザに確認します。

18.2.3. 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以下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 - 手動アップデートは、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ユーザに確認します。

18.2.4. 詳細設定

BitDefenderのアップデート処理がユーザ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には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はありません。
■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にBitDefenderはアップデートを行いません。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はありません。

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。

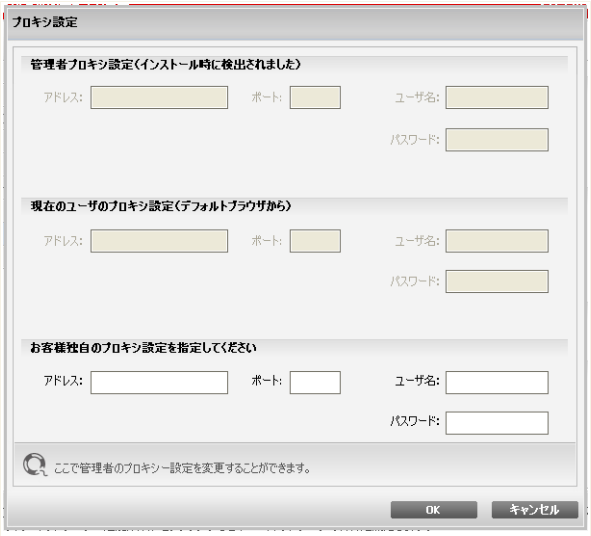
■ゲームモードがオンのときはアップデートしない - ゲームモードがオンの時はBitDefenderはアップデートを行いません。 これによりゲーム中のシステム処理能力に与える影響を最小限にできます。

18.2.5. プロキシを管理

会社でインターネット接続にプロキシサーバを使用している場合、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。指定しない場合は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種類あります：

■管理者プロキシ設定（インストール時に検出されます） - インストール時に管理者アカウントで検出されたプロキシ設定で、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には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。

■独自のプロキシ設定 - 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。

以下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アドレスを入力します。
- ポート - プロキシサーバへの接続時に 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ます。
- パスワード - 先に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。

インターネットへ接続しようとする時は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。

まず始めに、独自のプロキシ設定で指定した設定がインターネット接続で使用されます。失敗した場合は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。これもうまくいかなかった場合は、最終的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に使われます。

OKをクリックして変更を保存しウィンドウを閉じます。

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。

19. 製品登録

お使いのBitDefender製品の完全な情報および登録ステータスをみるには、詳細設定画面製品登録 を表示させます。

製品登録

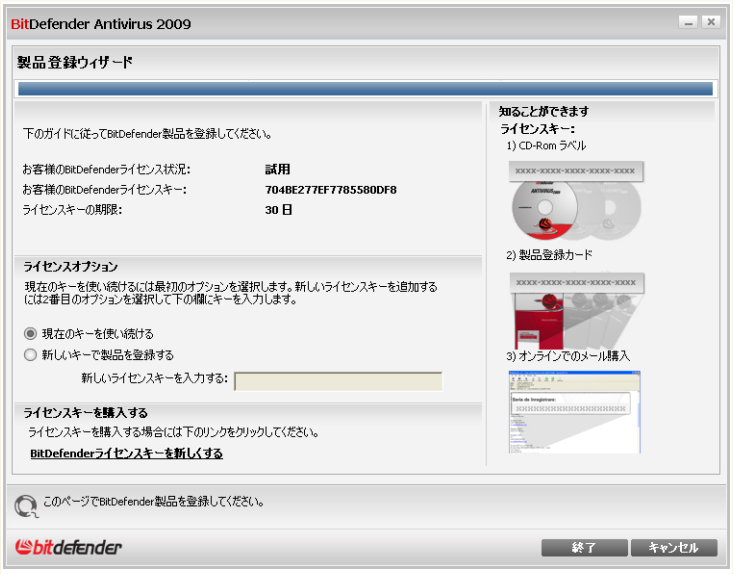
このセクションでは次の内容が表示されます：

■製品情報：BitDefender製品名とバージョン

■製品登録情報：（登録済みの場合）BitDefenderアカウントにログインするためのメールアドレス、現在のライセンスキー、有効期限が切れるまでの日数。

19.1. BitDefender Antivirus 2009を登録

今すぐ登録をクリックすると製品登録画面が開きます。



製品登録

BitDefender registration statusでは、お使いのライセンスキーが切れるまであと何日あるのか確認することができます。

BitDefender Antivirus 2009を登録する

1. この製品を登録を選択します。
2. ライセンスキーを入力します。

注意
ライセンスキーはこちらに書かれています：
■CDラベル
■製品登録カード

■オンラインストアからのメール

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

終了をクリックします。

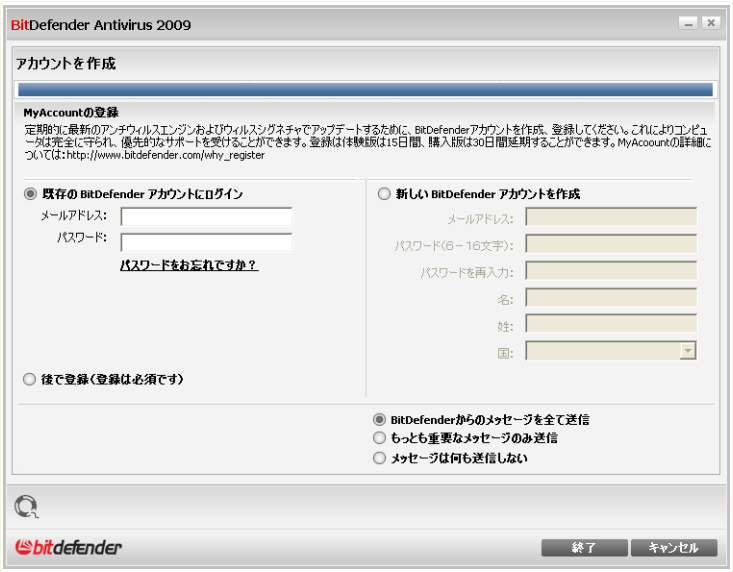
19.2. BitDefenderアカウントを作成

製品登録においてBitDefenderアカウントを作成する必要があります。 BitDefenderアカウントを持つことでBitDefenderの各種アップデート、無料のテクニカルサポート、また製品をお得に購入できるご案内を受けることができます。　登録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からマイページにログインすることができます。

重要項目

BitDefenderをインストールして15日以内にBitDefenderアカウントを作成してください。（ライセンスキーを登録した場合、BitDefenderアカウントの作成期限は30日まで延長されます） 登録がない場合にはBitDefenderは更新されなくなります。

まだBitDefenderアカウントをお持ちでない場合にはアカウントを作成するをクリックして登録画面を開きます。



アカウント作成

もし、いまBitDefenderアカウントを作成しない場合には、登録をスキップを選択し、終了をクリックします。 それ以外の場合は、このまま進めます：

■ 「まだBitDefenderアカウントをお持ちでない場合」（p. 221）

■ 「既にBitDefenderアカウントを持っている場合」（p. 222）

まだBitDefenderアカウントをお持ちでない場合

新しい BitDefenderアカウントを作成を選択して必要な情報を入力してください。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。 パスワードは６文字から１６文字の間である必要があります。

■パスワードを再入力 - 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 - 名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
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からマイページ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アクティブ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。

BitDefenderは製品の特別価格での販売のご案内やプロモーションをアカウントとして登録していただいたメールアドレスに送ることがあります。 以下のオプションから選択できます：

■BitDefenderからの全ての案内を受け取る
■大切なメッセージだけ受け取る
■全てのメッセージを受け取らない

終了をクリックします。

既にBitDefenderアカウントを持っている場合

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。 この場合はアカウントのパスワードを入力してください。

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。

パスワードを忘れた場合は、パスワードを忘れたら？をクリックし指示に従ってください。

BitDefenderは製品の特別価格での販売のご案内やプロモーションをアカウントとして登録していただいたメールアドレスに送ることがあります。 以下のオプションから選択できます：

■BitDefenderからの全ての案内を受け取る
■大切なメッセージだけ受け取る
■全てのメッセージを受け取らない

終了をクリックします。

方法

20. BitDefenderアカウントの作成方法

BitDefenderアカウントが必要な理由.
BitDefenderアカウントの作成はすぐにできます。また次のようなメリットがあります：

■カスタマケアへの優先的なアクセス

■毎時のアンチウィルスシグネチャのアップデート

■新しいPCに移行したり、製品を再インストールした際に、ライセンスキーを取得できます。

■その他BitDefender製品についての優待

このような利便を受けるには、試用版はインストール後、15日以内にアカウントを作成するか、30日以内（購入版）にアカウントを作成する必要があります。

警告

その期間内にBitDefenderアカウントを作成されなかた場合は、その後定期的なマルウェアシグネチャの更新を受け取ることができません。 マルウェアシグネチャが古くなると、最新のマルウェアからコンピュータが守られない場合があります。

BitDefenderアカウントの作成方法.
BitDefenderアカウントを作成する前に、まずBitDefender製品をコンピュータにインストールしなければなりません。 すでにコンピュータにBitDefender Antivirus 2009をインストールされている場合は、次の手順でBitDefenderアカウントを作成します：

1. BitDefenderを開く。  Windowsのスタートメニューから、 スタート → プログラム → BitDefender 2009 → BitDefender Antivirus 2009 を辿るか、または  BitDefender アイコンが システムトレイにありますのでダブルクリックします。
2. BitDefender画面の右下にはいくつかのリンクがあります。 登録 リンクをクリックします。 登録ウィザードが表示されます。
3. 次へ をクリックするとマイアカウントの登録に進みます。

注意

完了 ボタンが代わりに表示されている場合には、コンピュータでBitDefenderアカウントがすでに登録されています。 お客様のアカウントの情報について確認する場合には、詳細設定画面に切り替えて 左メニューにある製品登録 をクリックします。

4. 新しいBitDefenderアカウントを作成を選択し、必要な情報をご入力ください。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。 アカウントが作成され次第、確認の電子メールがこのメールアドレスに送信されます。
   - ■パスワード - BitDefenderアカウント指定したパスワードを入力してください。 パスワードは６文字から１６文字の間である必要があります。
   - ■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。
5. BitDefenderは製品の特別価格での販売のご案内やプロモーションをアカウントとして登録していただいたメールアドレスに送ることがあります。 以下のオプションから選択できます：
   - ■BitDefenderからの全ての案内を受け取る
   - ■大切なメッセージだけ受け取る
   - ■全てのメッセージを受け取らない
6. 完了 をクリックすると入力した情報が送信され、お客様のBitDefenderアカウントを作成します。
7. OKをクリックしてアカウントを有効にすることを承認します。
8. アカウントを有効にする。. アカウントを利用する前に、それを有効にする必要があります。 メールをチェックして、BitDefender登録サービスから送られたメールに書かれている案内に従ってください。

有効にすると、 マイアカウント リンクをクリックして、アカウントページにログインできるようになります。 このリンクはBitDefender画面の右下にあります。

21. ファイルとフォルダのスキャン方法

BitDefenderのスキャンは容易にかつ柔軟に行えます。 ウィルスや他のマルウェアに対してでBitDefenderは４つの方法でファイルやフォルダをスキャンできます：

■Windowsのコンテキストメニューを使う

■スキャンタスクを使う

■BitDefenderの手動スキャンを使う

■スキャンアクティビティバーを使う

スキャンをはじめると、アンチウィルススキャンウィザードが表示され、スキャン処理をガイドします。 詳細については次を参照してください。 「アンチウィルススキャンウィザード」 (p. 39)

21.1. Windowsコンテキストメニューを使う

これはもっとも簡単にコンピューター上のファイルやフォルダをスキャンできるお勧めの方法です。 スキャンしたいオブジェクトを右クリックしてBitDefender 2009でスキャン をメニューから選びます。 アンチウィルススキャンウィザードに従ってスキャンを完了します。

このスキャン方式は次の場合に使うことができます：

■あるファイル、フォルダが感染しているのではないかとおもう。

■インターネットからダウンロードしたファイルで危険とおもわれる場合。

■コンピュータにコピーする前にネットワーク共有フォルダをスキャン。

21.2. スキャンタスクを使う

コンピュータまたは特定のフォルダを定期的にスキャンしたい場合には、スキャンタスクを使用します。 スキャンタスクはBitDefenderにどの場所をスキャンするか、どのオプションで行うか、どの処理を行うかを指示するものです。さらにスケジュール することで定期的にまた特定の時間で実行させることができます。

スキャンタスクを使ってコンピュータをスキャンするには、BitDefenderを開いて、希望するスキャンタスクを実行します。 画面モード（基本設定画面または詳細設定画面）に応じて、スキャンタスクの実行方法が異なります。

基本設定画面でスキャンタスクを実行する

基本設定画面ではあらかじめ定義されたスキャンタスクだけを実行できます。 基本設定画面でのスキャンタスクの実行手順：

1. アンチウィルスタブをクリックします
2. 右にあるタスク 領域で、実行したいタスクをクリックすると実行されます。 利用可能なスキャンタスク：

スキャンタスク	説明
完全システムスキャン	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 などシステムのセキュリティを脅かすあらゆる種類のマルウェアをスキャンします。
フルシステムスキャン	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 などシステムのセキュリティを脅かすあらゆる種類のマルウェアをスキャンします。
マイドキュメントスキャン	カレントユーザの重要なフォルダをスキャンする場合にはこのタスクを使用します： マイドキュメント，デスクトップ，スタートアップ。これにより文書，作業環境，起動されるアプリケーションの安全を確認することができます。

3. アンチウィルススキャンウィザードに従ってスキャンを完了します。

詳細設定画面でスキャンタスクを実行する

詳細設定画面では、事前定義されたすべてのスキャンタスクを実行でき、そのスキャンオプションの変更もできます。また、コンピューター上の特定の場所をスキャン

するカスタマイズされたスキャンタスクを作成することができます。 詳細設定画面でのスキャンタスクの実行手順：

1. 左メニューにあるアンチウィルスをクリックします。
2. ウィルススキャン タブをクリックします。 デフォルトのスキャンタスクを確認できます。また独自のスキャンタスクを作成することもできます。 利用できるデフォルトのスキャンタスク：

デフォルトタスク	説明
完全システムスキャン	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 などシステムのセキュリティを脅かすあらゆる種類のマルウェアをスキャンします。
フルシステムスキャン	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 などシステムのセキュリティを脅かす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 と Program Files のフォルダをスキャンする。 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対象にスキャンしますが、メモリ，レジストリ，Cookieはスキャンしません。
マイドキュメント	カレントユーザの重要なフォルダをスキャンする場合にはこのタスクを使用します： マイドキュメント，デスクトップ，スタートアップ。これにより文書，作業環境，起動されるアプリケーションの安全を確認することができます。

3. 実行したいスキャンタスクをダブルクリックします。
4. アンチウィルススキャンウィザードに従ってスキャンを完了します。

21.3. BitDefender手動スキャンを使う

BitDefender手動スキャンでは、ハードディスクパーティション上の特定のフォルダを、新たにタスクを作成することなく実施できます。 このモードはWindowsがセーフモードで動作している場合の使用を想定しています。 もしシステムが耐久性のあるウィルスに感染している場合には、このウィルスをWindwosをセーフモードで起動して、各ハードディスクのパーティションからBitDefender手動スキャンによって除去を試みてください。

BitDefender手動スキャンを使ってコンピュータをスキャンするには次の手順を行います：

1. On the  Windowsのスタートメニューから、 スタート → すべてのプログラム → BitDefender 2009 → BitDefender手動スキャン. 新しいウィンドウが開きます。
2. スキャン対象を選択します：
   ■デスクトップをスキャンするには デスクトップを選択します。
   ■ハードディスクのパーティション全体をスキャンするには、マイコンピュータからそれを選択します。
   ■特定のフォルダをスキャンするには、フォルダを辿り、該当するフォルダを選択します。
3. OKをクリックしてスキャンを開始します。
4. アンチウィルススキャンウィザードに従ってスキャンを完了します。

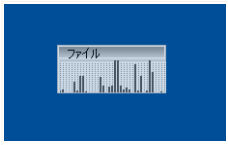
セーフモードとは？.
セーフモードは特殊なWindowsの起動方法です。主に通常のWindowsの動作に影響する問題の解決のために使われます。その問題にはドライバーの衝突から、ウィルスによってWindwosが通常に起動できないなどさまざまのものがあります。 セーフモードでは、Windowsは必要最小限のOSコンポーネントとドライバしかロードしません。セーフモードではわずかなアプリケーションしか動作しません。このためセーフモードのWindowsではほとんどのウィルスが活動できず、よって除去もしやすくなります。
Windwosをセーフモードで動作させるには、再起動してF8 キーを押し続け Windows Advanced Options Menu を表示させます。セーフモードで起動できるオプションから選択することができます。セーフモード（ネットワーク） を選ぶことでインターネットへのアクセスが可能です。

注意

セーフモードについてより詳細はWindowsのヘルプとサポートセンターにアクセスします（スタートメニューからヘルプとサポート）をクリックします。 インターネットを検索することで役に立つ情報をみつけることができます。

21.4. スキャン処理バーを使う

スキャンアクティビティバーはシステムのスキャン処理をグラフにより視覚化したものです。 小さな画面だけが詳細設定画面では利用できます。



スキャンアクティビティバー

スキャンアクティビティバーを使ってファイルとフォルダをスキャンできます。 スキャンしたいファイルやフォルダをスキャンアクティビティバーにドラッグ & ドロップします。 アンチウィルススキャンウィザードに従ってスキャンを完了します。

注意

詳細については 「スキャンアクティビティバー」 (p. 35) を参照してください。

22. コンピュータスキャンをスケジュールする方法

コンピュータを定期的にスキャンすることは、マルウェアからコンピュータを守るのに最適な方法です。 BitDefenderでスキャンタスクをスケジュールして自動的にコンピュータをスキャンさせるようにすることができます。

コンピューターのスキャンをBitDefenderにスケジュールさせるには次の手順で行います：

1. BitDefenderを開く。 Windowsのスタートメニューから、 スタート → プログラム → BitDefender 2009 → BitDefender Antivirus 2009 を辿るか、または BitDefender アイコンが システムトレイにありますのでダブルクリックします。
2. 画面が標準設定画面の場合には詳細設定画面　ボタンをクリックしてください。画面の右上にあります。
3. 左メニューにあるアンチウィルスをクリックします。
4. ウィルススキャン タブをクリックします。 デフォルトのスキャンタスクを確認できます。また独自のスキャンタスクを作成することもできます。

   ■システムタスクが利用可能で、Windowsのユーザごとに実行することができます。

   ■ユーザタスクはそれを作成したユーザのみが実行でき、有効です。

   スケジュールできるデフォルトのスキャンタスク：

デフォルトタスク	説明
完全システムスキャン	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 などシステムのセキュリティを脅かすあらゆる種類のマルウェアをスキャンします。
フルシステムスキャン	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，

デフォルトタスク	説明
	アドウェア，Rootkit などシステムのセキュリティを脅かす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 と Program Files のフォルダをスキャンする。 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対象にスキャンしますが、メモリ，レジストリ，Cookieはスキャンしません。
自動ログオン スキャン	ユーザがWindowsにログオンしてきた際に動作している項目をスキャン　このタスクを使用するには、システム起動時に実行するようスケジュールしなければなりません。　デフォルトでは自動ログオンスキャンは無効になっています。
マイドキュメント	カレントユーザの重要なフォルダをスキャンする場合にはこのタスクを使用します：　マイドキュメント，デスクトップ，スタートアップ。これにより文書，作業環境，起動されるアプリケーションの安全を確認することができます。

ここにあるスキャンタスクで合ったものがなければ、新しくスキャンタスクを作成して、必要に応じてスケジュール実行させることができます。

5. 実行したいタスクスケジュールを右クリックして、 スケジュールを選択します。新しいウィンドウが開きます。
6. 必要に応じてタスクを実行するようスケジュール：
   - ■スキャンタスクを１度だけ実行するには、　１度を選択して開始日時を指定します。
   - ■システム起動時にスキャンタスクを実行するには 起動時を選択します。 起動からどのぐらい時間が経過してからその処理を開始するかを指定（分）できます。
   - ■スキャンタスクを定期的に実行させるには、 定期的 を選択して、周期と開始日時を指定します。

注意
例えば、コンピュータを毎土曜日の午前２時に実行させたい場合には、次のようにスケジュールを設定します：

a. 定期的を選択します。

b. 値 欄に１と入力して 週 をメニューから選択します。 このようにしてタスクを毎週実行させます。

c. 開始日付を次の土曜日にセットします。

d. 開始時間を 02:00:00にセットします。

7. OK をクリックしてこのスケジュールを保存します。 このスキャンタスクは自動的に作成したスケジュールに従って実行されます。 もしスケジュールした時間にコンピュータが停止している場合、そのタスクは次にコンピュータを起動した時間に実行されます。

問い合わせ先

23. サポート

BitDefenderは、速くて正確なサポートをお客様に提供するよう努力しています。BitDefender Knowledge Baseでは、BitDefenderに関する問題や質問についての解決策を提供しています。このKnowledge Baseで解決策が得られなった場合には、BitDefenderのカスタマケーアに問い合わせることができます。サポートではご質問にできるだけはやく回答し、お役に立てるよう努力いたします。

23.1. BitDefender Knowledge Base

BitDefender Knowledge Baseは、BitDefender製品に関するオンラインの情報データベースです。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てウイルス保護や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は一般に開放されており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。

23.2. ヘルプを依頼

ヘルプに問い合わせるためには、BitDefenderウェブセルフサービスを使う必要があります。次の手順に従ってください：

1. http://www.bitdefender.com/helpにアクセスします。 ここでBitDefender Knowledge Baseをみつけることができます。 BitDefender Knowledge BaseはBitDefenderに関する数多くの解決策を提供しています。
2. BitDefender Knowledge Baseでお困りの問題に対する解決策を検索してください。
3. 関連事項をご覧になり、提示されてる解決策を試してみてください。

4. その解決策で問題が解決されなかった場合には、そのページ内のリンクからBitDefenderカスタマーケアーにお問い合わせください。
5. お客様の BitDefender アカウントにログインしてください
6. BitDefenderサポートにメールでお問い合わせください。

23.3. 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。

23.3.1. ウェブアドレス

営業：sales@bitdefender.jp
テクニカルサポート: www.bitdefender.jp/help
文書制作：documentation@bitdefender.jp
パートナープログラム：partners@bitdefender.jp
マーケティング：marketing@bitdefender.jp
広報：pr@bitdefender.jp
求人：jobs@bitdefender.jp
ウイルスの連絡：virus_submission@bitdefender.com
迷惑メールの連絡：spam_submission@bitdefender.com
悪用の報告：abuse@bitdefender.jp
製品のウェブサイト：http://www.bitdefender.jp
製品のアーカイブ：http://download.bitdefender.jp/pub
各地の代理店：: http://www.bitdefender.com/site/Partnership/list/
BitDefender Knowledge Base（英文）：http://kb.bitdefender.com

23.3.2. BitDefender事業所

BitDefenderの支店およびその代理店は、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
電話(事務所&営業): 1-954-776-6262
営業部門: sales@bitdefender.com
Technical support: http://www.bitdefender.com/help
ウェブサイト: http://www.bitdefender.com

Germany

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
事務所: +49 2301 91 84 222
営業部門: vertrieb@bitdefender.de
Technical support: http://kb.bitdefender.de
ウェブサイト: http://www.bitdefender.de

UK and Ireland

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
メール: info@bitdefender.co.uk
電話: +44 (0) 8451-305096
営業部門: sales@bitdefender.co.uk
Technical support: http://www.bitdefender.com/help
ウェブサイト: http://www.bitdefender.co.uk

Spain

BitDefender España SLU
C/ Balmes, 191, 2°, 1ª, 08006
Barcelona

Fax： +34 932179128
電話： +34 902190765
営業部門： comercial@bitdefender.es
Technical support: http://kb.bitdefender.es
ウェブサイト http://www.bitdefender.es

Romania

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Fax： +40 21 2641799
営業： +40 21 2063470
営業宛メールアドレス： sales@bitdefender.ro
Technical support: http://kb.bitdefender.ro
ウェブサイト http://www.bitdefender.ro

BitDefender Rescue CD

24. 概要

BitDefender Antivirus 2009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には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元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/

24.1. システム要件

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512MB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。

24.2. 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。ファイルの復元に使えます。

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は送受信される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。

25. 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。

25.1. 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。

注意

Rescue CD動作にあたり使用する言語を利用可能リストから選択します。

起動画面

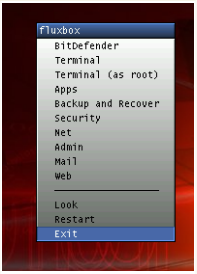
起動時にウイルスシグネチャのアップデートが自動で行われます。この処理にしばらくかかります。

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

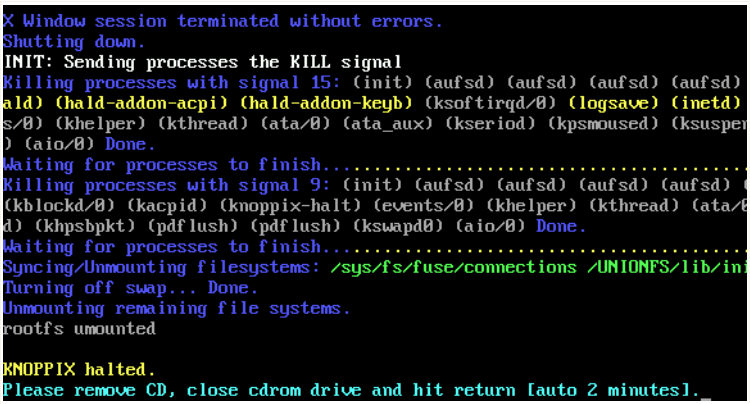
25.2. BitDefender Rescue CDの停止

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。

25.3. 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をフルスキャンできます。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。

以下の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. 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。

問題のグループごとに一括して実行するアクションを選ぶか、問題ごとに個別のアクションを選択できます。

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。

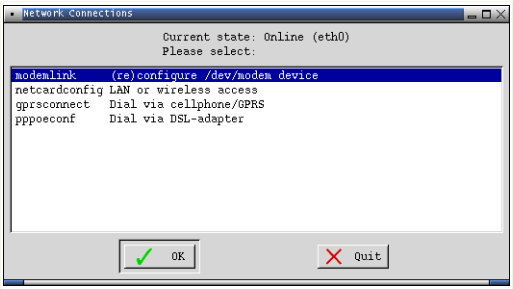
あるいはTerminalで、rootとして次のコマンドを発行してください。選択したファイルあるいはフォルダをデフォルトのスキャン対象としてBitDefender Antivirus Scannerが開始します。

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

25.4. インターネット接続の設定方法

もしDHCPネットワーク環境の中にあり、イーサーネットワークカードをお持ちなら、インターネット接続はすでに検知された設定されているはずです。手動の設定は次の手順を行います。

1. デスクトップにあるNetwork Connections（ネットワーク接続）のショートカットをダブルクリックします。



ネットワーク接続

2. お使いの接続タイプを選択してOKをクリックします。

接続	説明
モデム接続	モデムと電話線を使ってインターネットにアクセスしている場合にはこの接続タイプを選択してください。
ネットカード設定	ローカルエリアネットワーク（LAN）を使ってインターネットにアクセスしている場合には、この接続タイプを選択してください。ワイアレス接続されている場合にもこちらを選択してください。
gprs接続	GPRS（汎用パケット無線システム）プロトコルによるモバイルフォンを介してインターネットにアクセスしている場合には、この接続タイプを選択してください。モバイルフォンではなく、FPRSモデムを使っている場合にもこのタイプを選択します。
pppoeconf	DSL（デジタル加入者線）モデムを使ってインターネットにアクセスしている場合にはこの接続タイプを選択してください。

3. 画面の指示に従ってください。何を書き込むかわからない場合にはシステム管理者またはネットワーク管理者に詳細をお尋ねください。

重要項目
さきほどオプションで選択したモデムのみを有効にしてください。ネットワーク接続を設定するには次の手順に従ってください。

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：

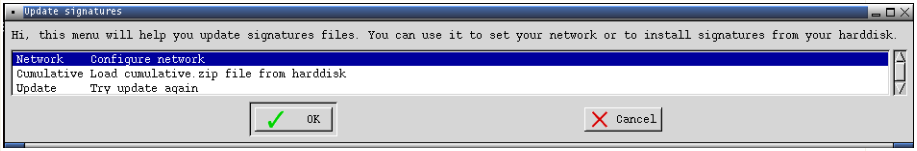
```
# pppconfig
```

4. 画面の指示に従ってください。何を書き込むかわからない場合にはシステム管理者またはネットワーク管理者に詳細をお尋ねください。

25.5. BitDefederのアップデート方法

起動時に、ウィルス定義は自動的に更新されます。もしこのステップをスキップした場合に、あとからどのようにBitDefenderをアップデートするかを説明いたします。

1. デスクトップにあるUpdate Signatures(定義アップデート）をダブルクリックします。すると次の画面が表示されます。



定義のアップデート

2. 以下のいずれかを実行します：
   ■Cumulative（累積）を選択すると既にハードディスクに保存されている定義を検索してcumulative.zipファイルを読み込んでインストールします。
   ■Update（アップデート）を選択するとインターネットに接続して最新のウィルス定義をダウンロードします。
3. OKをクリックします。

25.5.1. 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は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

25.6. 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が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、必要であれば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。

   注意

   もしメモリスティックを後で差し込む場合には、次の手順でリムーバブルデバイスをマウントしなければなりません。

   a. デスクトップにあるターミナルエミュレータのショートカットをダブルクリックします。
   b. 次のコマンドを入力します：

      ```
      # mount  /media/sdb1
      ```

      お使いのコンピュータの構成によってはsda1をsdb1の代わりに指定しなくてはなりません。

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。

重要項目

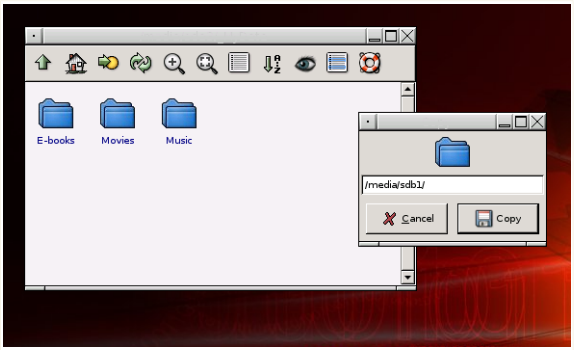
もしコンピュータが正常に終了していない場合は、あるパーティションが自動でマウントされないことがあります。パーティションをマウントするには次の手順で行ってください。

a. デスクトップにあるターミナルエミュレータのショートカットをダブルクリックします。

b. 次のコマンドを入力します：

```
# mount  /media/partition_name
```

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。

   お使いのコンピュータの構成によってはsda1をsdb1の代わりに指定しなくてはなりません。

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低下させます。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に関する問題につながる恐れがあります。

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。

ブートセクター
ディスクの構造（セクタサイズ、クラスタサイズなど）を記録した、各ディスクの開始場所にあたるセクタです。起動ディスクの場合はブートセクタ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に感染するウイルスです。起動セクタ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。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
インターネットの世界では、Cookieはユーザ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および利用する、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、ユーザ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。ユーザ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、そのためにユーザ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。

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
プログラムが検出するアクションまたは事象です。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。

誤って迷惑メールとしてしまう
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、"疑わしいとしてしまう"と報告す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されますが、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
文書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文書にマクロを埋め込んで文書を開くたび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
メールクライアントは、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、疑わしいと警告を生成しないことです。

圧縮されたプログラム
: 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たど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かさせるために詐欺メールを送る行為です。こうしたメールではユーザをウェブサイトへ誘導し、本来の企業が既に持っているパスワード，クレジットカード番号，社会保障番号，銀行口座番号などの個人情報を更新するよう促します。しかし、そのウェブサイトは偽物で、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
: 感染させ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ので、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
発生したアクションを一覧にしたファイルです。BitDefenderはスキャンしたパス、フォルダ、スキャンした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にしたレポートファイルを管理します。

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、多くの場合は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対する大きな脅威となります。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検出されないようにします。

スクリプト
マクロや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、ユーザの操作なしに実行されます。

スパム
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メールを指します。

スパイウェア
多くの場合は広告宣伝の目的で、ユーザが知らないうち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、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，コンピュータを初めて起動した時に再生されるサウンドファイル，カレンダの通知，アプリケーションプログラムが、起動項目として使用できます。通常は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、システム機能を簡単に呼び出すための小さなアイコンを表示します。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、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、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
コンピュータに知らない間に読み込まれ、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。コンピュータウイルスはすべて、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。