bitdefender
internet security 2010

# ユーザガイド

# BitDefender Internet Security 2010
# ユーザガイド

発行 2009.09.15



## 法的通知

# 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等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、譲渡や移転、サブライセンスを認め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。

データ収集技術- BitDefenderは、特定のプログラムや製品で個人を特定しない技術情報の収集（疑わしいファイルも含む）のためにデータ収集技術を使用することがあります。製品の改善や関連するサービスの提供を通じて、ライセンス許諾されていない製品の違法な使用、またはマルウェア製品からの被害を防ぎます。お客様は、ライセンスに同意することでお使いのコンピュータでマルウェアプログラムの実行を阻止または停止するために、BitDefenderが技術情報を収集し使用することに同意したと見なされます。

BitDefenderがアップデート及びプログラムや製品の追加を、自動的にお使いのコンピュータにダウンロードを行って提供することを承認及び許可します。

このライセンス契約に同意した場合、BitDefenderがスキャンするためにお使いのＰＣに保存されている実行ファイルをBitDefenderにアップロードすることに合意したことになります。また、このプログラムの使用許諾のためにお客様はBitDefenderに一部の個人情報を提供する必要があります。BitDefenderは現在の適用する法律及びプライバシーポリシーに基づいて、お客様の個人情報を取り扱います。

データ収集：製品やサービスの取得、ツールの利用又は個人情報の扱いを含んでいるウェブサイトを通じたコンテンツのウェブサイトへユーザが行うアクセス。個人情報、公共サービスの情報、電子商取引を規制する法律に準拠していることは、BitDefenderにとって最も重要なことです。製品やサービスコンテンツにアクセスする中には、お客様の一部の個人情報の詳細を提供する必要があります。個人情報、公共サービスの情報、電子商取引を規制する法律に従って、BitDefenderはこのようなデータを機密情報として取り扱います。

BitDefenderは、適用するデータ保護法に準拠し、収集した個人情報の保護を保障するために必要な管理および技術的な手続きを実施しています。

お客様が提供された全ての情報は真実で正しく、内容に変更がある場合はBitDefenderに通知する責任があります。お客様は、契約の合意に必要でない個人情報の扱いに反対する権利および、契約上の関係の維持以外の目的で個人情報を使用することに反対する権利を所有しています。

第三者の詳細情報を提供する場合、BitDefenderは情報や合意の原則に準拠する責任を負いません。それゆえに、お客様がデータの所有者に、事前に連絡を取って、このようなデータの通信に関する合意を交わす責任があります。

BitDefenderとその関連会社及びパートナーは、電子メール又は他の電子的手段を使用して、販売情報のみを、BitDefender製品やサービス、ニュースレターに関する情報を受信することを同意したユーザに送信します。

BitDefenderのプライバシーポリシーは、次の宛先に電子メールで連絡することで、お客様がアクセス、改正、削除、およびデータの扱いに反対する権限を持つことを保証します：juridic@bitdefender.com.

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。

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、24, Preciziei Boulevard, West Gate Building H2, ground floor, Sector 6, Bucharest, Romania, あるいは 電話番号：40-21-206.34.70 または FAX：40-21-264.17.99、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：03-4360-6947　　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ためのセキュリティソリューションとして、BitDefender Internet Security 2010を選択したすべてのユーザを対象に書かれています。本書に書かれた情報は、コンピュータに詳しいユーザだけでなく、Windows が使えれば誰でも利用可能なものです。

本書では、BitDefender Internet Security 2010のインストール手順を追って、設定方法を説明します。BitDefender Internet Security 2010の使い方、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ています。きっとBitDefenderを最大限有効利用する方法がお分かりいただけることでしょう。

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

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

| 表記 | 解説 |
|---|---|
| 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。 |
| sales@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. xvii) | これは、文書内の別のロケーション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。 |
| 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. 本書の構成

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。

インストールと削除. BitDefenderをパソコンにインストールするための手順を説明しています。インストールにあたっての必要事項からインストール手順の全容、そしてBitDefenderのアンインストール方法について記載されています。

使い方. BitDefenderを起動するために必要な全ての情報が含まれています。BitDefender のインターフェース、問題の修正方法、基本設定や登録方法が提示されています。

中級者モード. BitDefenderの中級者モードです。

上級者モード. BitDefenderの上級者モードの詳細です。 お使いのコンピュータをあらゆる種類の脅威（マルウェア、迷惑メール、ハッカー、不適切なコンテンツなど）から効率よく保護するために、すべてのBitDefenderモジュールの設定方法と使い方を説明します。

Windowsと第三者ソフトウェアの統合. Windows のコンテキストメニューにあるBitDefenderオプションの使用方法、及びサポートされた第三者プログラムに統合されてるBitDefenderツールバーの使用方法を表示します。

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。

トラブルシューティングとヘルプ機能. 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.com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。

# インストールと削除

# 1. システム要件

BitDefender Internet Security 2010 は、以下のオペレーティングシステムが動作しているコンピュータで動作いたします：

- Windows XP (32/64 bit)サービスパック2以上
- Windows Vista (32/64 bit) 又は Windows Vista Service Pack 1又はそれ以上
- Windows 7 (32/64 bit)

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. 必須システム要件

- 450 MBのハードディスク空き容量
- 800 MHz プロセッサ
- RAM メモリ:
  - Windows XP用 512MB
  - 1 GB ( Windows Vista及びWindows 7)
- Internet Explorer 6.0
- .NET Framework 1.1(インストーラーに含まれています)

## 1.2. 推奨されるシステム要件

- 600 MBのハードディスク空き容量
- Intel CORE Duo (1.66 GHz) 又は それに相当するプロセッサ
- RAM メモリ:
  - 1 GB(WindowsXP及びWindows 7)
  - 1.5 GB(Windows Vista)
- Internet Explorer 7 以上
- .NET Framework 1.1(インストーラーに含まれています)

## 1.3. サポートされたソフトウェア

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 2.5
- Yahoo Messenger 8.5

●Windows Live Messenger 8

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 8.5
●Windows Live Messenger 8

アンチスパム保護は全てのPOP3/SMTPメールクライアントに対応しています。
BitDefenderアンチスパムツールバーは、以下の製品に対応しています。

●Microsoft Outlook 2000 / 2003 / 2007
●Microsoft Outlook Express
●Microsoft Windows Mail
●Thunderbird 2.0.0.17

# 2. インストールの準備

BitDefender Internet Security 2010をインストールする前に、インストールが問題なく実行するために次の準備を完了してください：

- BitDefenderをインストールするコンピュータが、最低限のシステム要件を満たしているかどうかをご確認ください。 コンピュータが全ての最低限のシステム要件を満たすことができない場合は、BitDefenderは、インストールされないか、もしくはインストールされたとしても正しく動作せず、システムが遅くなったり不安定になるかもしれません。 システム要件の一覧を確認するには、「システム要件」 (p. 2)をご参照ください。
- 管理者アカウントを使用してコンピュータにログオンしてください。
- コンピュータから他のセキュリティのソフトウェアを削除してください。 2つのセキュリティプログラムを同時に実行すると、オペレーションに影響を与えて、システムに重要な問題を引き起こすかもしれません。 Windows Defenderはデフォルトではインストール開始時にに無効になります。
- コンピュータで実行しているかもしれないファイアーウォールプログラムを、無効又は削除してください。 2つのファイアーウォールプログラムを同時に実行すると、オペレーションに影響を与えて、システムに重要な問題を引き起こすかもしれません。 Windowsファイアーウォールは、インストールが開始される前にデフォルトで無効になります。

# 3. BitDefenderのインストール

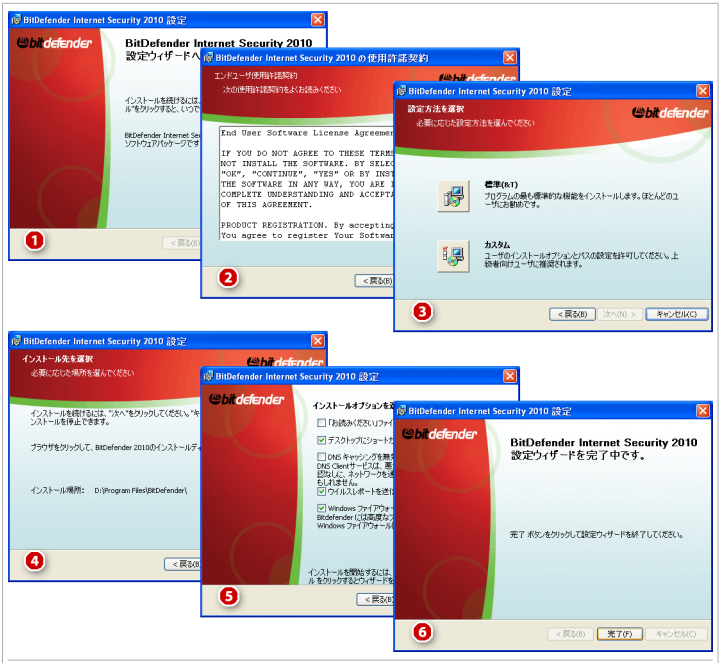
BitDefenderは、BitDefenderインストールCDやBitDefenderウェブサイト、あるいは許可された他のウェブサイト（例えば、BitDefender パートナのウェブサイトやオンラインショップ）から、インストールファイルをダウンロードして、インストールを実行することができます。 次のアドレスのBitDefenderウェブサイトから、インストールファイルをダウンロードをすることができます：http://www.bitdefender.jp.

- CDからBitDefenderをインストールをして、ドライブにCDを挿入します。ウェルカム画面がしばらく表示されます。説明に従って、インストールを開始してください。

  ウェルカム画面が表示されない場合は、CDのルートディレクトリからこのパス製品¥インターネットセキュリティ¥インストール¥en¥にアクセスして、 runsetup.exe をダブルクリックしてください。

- お使いのコンピュータでダウンロードされたインストールファイルを使用してBitDefenderをインストールするには、ファイルを指定してそれをダブルクリックしてください。

インストーラは、最初にお使いのシステムのインストール検証を行います。 インストールが検証されると、セットアップウィザードが表示されます。 セットアップウィザードの手順を次の画像で表示します。




インストール手順

以下の手順に従ってBitDefender Internet Security 2010をインストールしてください：

1. 次へをクリックします。 キャンセルをクリックすると、いつでもインストールをキャンセルすることができます。

   お使いのコンピュータへインストールする際に、他のアンチウィルス製品が既に存在すると、BitDefender Internet Security 2010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ィ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つ以上のアンチウィ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。

2. 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。

3. 実行するインストールの形式を選択してください。
   - 標準 - デフォルトのインストールオプションを使用して、今すぐプログラムをインストールします。 このオプションを選択すると、手順6にスキップします。
   - カスタム - インストールオプションを設定して、プログラムをインストールします。 このオプションでインストールのパスを変更することができます。
4. デフォルトでは、BitDefender Internet Security 2010 はC:¥Program Files¥BitDefender¥BitDefender 2010にインストールされています。 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保存 - インストールの最後で、BitDefender Internet Security 2010のショートカットをお使いのデスクトップ上に作成します。
   - 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。
   - DNSキャッシングを無効にする - DNS(ドメインネームシステム)キャッシングを無効にする DNS Clientサービスは、悪意のあるアプリケーションが、ユーザの確認なしに、ネットワークを通じて情報を送信することに使用されるかもしれません。
   - Windowsファイアウォールを無効にする - Windowsファイアウォールを無効にします。

     **重要項目**
     BitDefender Internet Security 2010には先進のファイアウォールが内蔵されていますから、Windows ファイアウォールは無効にすることをお勧めします。同じコンピュータ上で２種類のファイアウォールを実行すると、問題を起こす原因となり得ます。

- 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。

6. インストールが完了するまでお待ちください。次に 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 Internet Security 2010 の設定ウィザードを完了させて、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、 プログラムファイルに、BitDefenderという新しいフォルダが作成され、 その中にBitDefender 2010というサブフォルダがあります。

## 3.1. 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。

### 3.1.1. 手順 1 - BitDefender Internet Security 2010を登録


製品登録

BitDefender Internet Security 2010 には 30 日間の試用期間が設けられています。 製品の評価を継続するには、BitDefenderを評価する を選択して、次へをクリックします。

BitDefender Internet Security 2010を登録:

1. ライセンスキーでBitDefenderを登録するを選択します。
2. ライセンスキーを入力します。

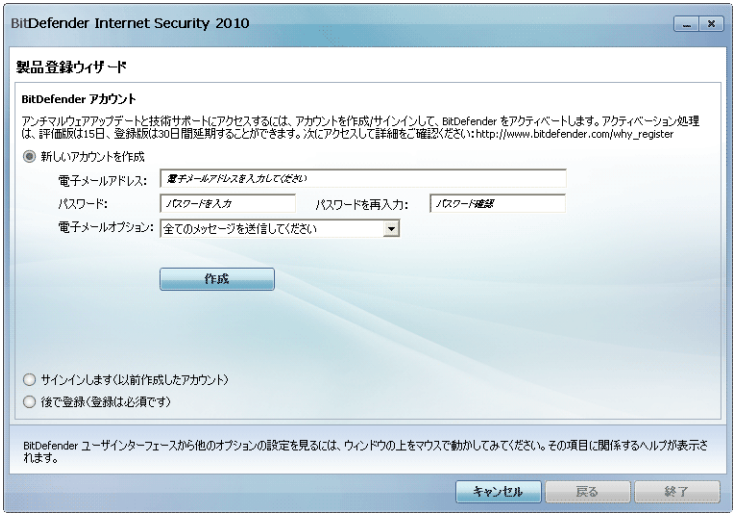
**注意**
ライセンスキーは以下に記載されています：
- CDラベル
- 製品登録カード
- オンラインストアからのメール

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。

3. 今すぐ登録するをクリックします。
4. 次へをクリックします。

有効なBitDefenderライセンスキーがお使いのシステムで検出された場合、次へをクリックすると、継続してこのキーを使用することができます。

### 3.1.2. 手順 2 - BitDefenderアカウントを作成




アカウント作成

もし、いまBitDefenderアカウントを作成されない場合には、後で登録を選択し、終了をクリックしてください。 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. 11)

**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

正しくBitDefenderアカウントを作成するには、次の手順に従ってください：

1. 新しいアカウントを作成するを選択します。
2. 該当する欄に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。

注意
アカウントが有効になると、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からアカウントにログインしてください。

3. 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お客様のメールアドレスに送信することがあります。 メニューから有効なオプションを選択してください：
   - 全てのメッセージを受信
   - 製品に関するメッセージだけを受信
   - 全てのメッセージを受け取らない
4. 作成をクリックしてください。
5. 終了をクリックして、ウィザードを閉じてください。
6. 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。

## 既にBitDefenderアカウントを持っている場合

お客様が既に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、お客様のアカウントのパスワードを入力して、サインインをクリックしてください。 終了をクリックして、ウィザードを閉じてください。

有効なアカウントを持っていて、BitDefenderがそれを検出しない場合は、そのアカウントで製品を登録するために次の手順に従ってください。

1. サインイン（以前に作成されたアカウント）を選択してください。
2. 該当欄にお使いのアカウントの電子メールアドレスとパスワードを入力してください。

注意
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。

3. 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お客様のメールアドレスに送信することがあります。 メニューから有効なオプションを選択してください：
   - 全てのメッセージを受信
   - 製品に関するメッセージだけを受信
   - 全てのメッセージを受け取らない
4. サインインをクリックしてください。
5. 終了をクリックして、ウィザードを閉じてください。

## 3.2. 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。 このウィザードは、主なBitDefender設定及びユーザインターフェースの設定を手助けするので、お使いのシステム要件により適応します。ウィザードの終了時、製品ファイル及びマルウェアシグネチャをアップデートすることが可能で、システムのファイルやアプリケーションがウィルスに感染していないかを確認するためにスキャンを実行することができます。

ウィザードは数少ない簡単な手順で構成されています。お客様の選択に応じて手順の数が決まります。 全ての手順がここに表示されていますが、お客様の選択に応じて手順の数が変更されると通知いたします。

ウィザードの完了は必須ではありません。しかし、時間を節約し、BitDefender Internet Security 2010 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、ウィザードの利用をお勧めします。 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。

### 3.2.1. 手順 1 - 使用プロファイルの選択


使用プロファイル

このコンピュータで実行される業務をもっとよく説明しているボタンをクリックします。（使用プロファイル）

| オプション | 解説 |
|---|---|
| Typical | ブラウジングやマルチメディア用にこのPCをお使いになる場合は、ここをクリックしてください。 |
| Parent | お子様がこのPCを使用している場合や、ペアレンタルコントロールモジュールを使用して、インターネットへの接続をコントロールしたい場合は、ここをクリックします。 |
| ゲーマー | このPCが主にゲーム用で使用されている場合は、ここをクリックしてください。 |
| カスタム | BitDefenderの全ての主な設定を行いたい場合は、ここをクリックしてください。 |

後で製品のインターフェースから、使用プロファイルをリセットすることができます。

### 3.2.2. 手順 2 - コンピュータの記述


コンピュータの説明

お使いのコンピュータに適用するオプションを選択します：

- このコンピュータはホームネットワーク内にあります。. このコンピュータにインストールしたBitDefender製品をリモートから（別のコンピュータから）管理したい場合は、このオプションを選択してください。 追加のウィザード手順で、ホームネットワーク管理機能を設定することができます。
- このコンピュータはノートPCです. デフォルトでノートPCモードを有効にしたい場合は、このオプションを選択してください。 ノートPCモード中は、スケジュールされたスキャンタスクは実行されません。なぜならば、より多くのシステムリソースを要求するので、電力消費が暗黙的に増加するからです。

次へをクリックしてください。

### 3.2.3. 手順 3 - ユーザインターフェースの選択


ユーザインタフェース設定モード

お使いのコンピュータスキルを最も良く説明しているボタンをクリックして、適切なユーザーインターフェースを選択してください。　お客様のコンピュータスキルや、BitDefenderを使用していた過去の経験に合わせて、以下の3つのユーザインターフェイスからモードを選択できます。

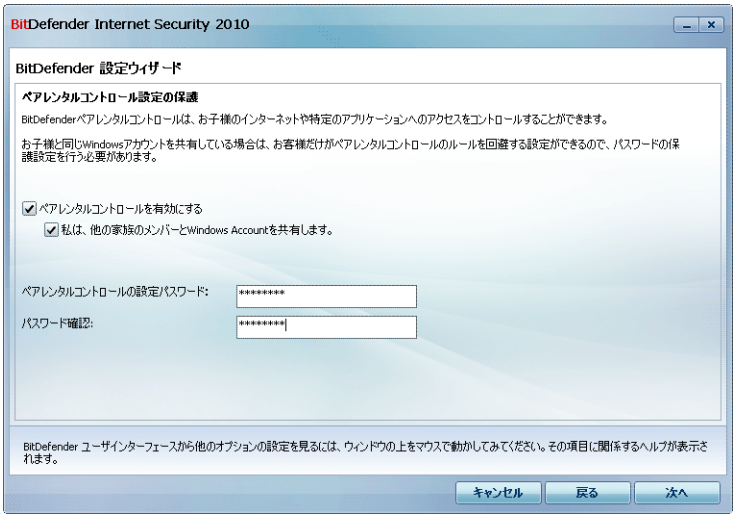
| モード | 解説 |
|---|---|
| 初級者モード | コンピュータの初心者及び、簡単な設定でBitDefenderがコンピュータとデータを保護してほしいユーザに適しています。このモードは、使い方が簡単で、最小限のやり取りで設定が可能です。<br><br>お客様に行っていただくことは、BitDefenderが表示した既存の問題を修復するだけです。使いやすく段階を追った手順のウィザードが、問題修復の手助けをします。　さらに、BitDefenderウィルスシグネチャ、製品ファイル、またはコンピュータのスキャンのアップデート等、共通のタスクを実行することができます。 |
| 中級者モード | コンピュータスキルが標準なユーザに適しています。このモードは、初級者モードで出来る内容を拡張しています。 |

| モード | 解説 |
| --- | --- |
| | 問題を別々に修復することが出来、どの問題を監視するかを選択します。 さらには、リモートから、ご自宅のコンピュータにインストールされている BitDefender 製品を管理することができます。 |
| 上級者モード | このモードは、上級者ユーザに適しており、BitDefenderの各機能を全面的に設定することができます。 また、お使いのコンピュータやデータを保護するため、提供されている全てのタスクを使用することができます。 |

### 3.2.4. 手順 4 - ペアレンタルコントロールの設定

**注意**

この手順は、手順1でカスタムオプションを選択した場合のみ表示されます。




ペアレンタルコントロールの設定

BitDefenderペアレンタルコントロールは、お使いのシステムのアカウントごとにアクセスできるサイト、アプリケーションをコントロールすることができます。

ペアレンタルコントロールを有効にするには、次の手順を実行してください：

1. ペアレンタルコントロールを有効にするを選択してください。

2. お使いのWindowsユーザアカウントをお子様と共有している場合は、該当するチェック欄を選択して、ペアレンタルコントロール設定を保護するためにパスワードを入力してください。　ペアレンタルコントロールの設定を変更しようとする際には、セットされたパスワードを入力するように求められます。

次へをクリックしてください。

### 3.2.5. 手順 5 - BitDefenderネットワークの設定

**注意**
この手順は、手順2でコンピュータがホームネットワークに接続するように指定した場合にだけ表示されます。


BitDefenderネットワーク設定

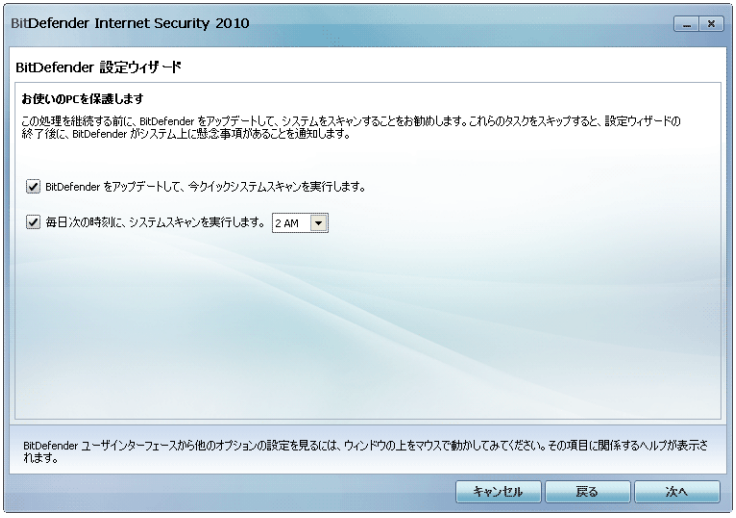
BitDefenderは家庭内にあるコンピュータで仮想ネットワークを構成することができ、BitDefender製品のインストールや管理を行うことができます。

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. ネットワークを有効にするを選択してください。
2. 入力欄に同じ管理者パスワードをを入力します。　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。

## 3.2.6. 手順 6 - 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が重要なタスクを実行するよう、BitDefender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をアップデートして、今すぐクイックシステムスキャンを実行します - 次の手順の間、BitDefenderのウィルスシグネチャ及び製品ファイルが、最新の脅威に対してお使いのコンピュータを保護するためにアップデートされます。 また、アップデートの完了後直ぐに、BitDefenderはWindows と プログラムファイルフォルダからファイルをスキャンして、ウィルスに感染していないかを確認します。 これらのフォルダには、オペレーティングシステムのファイル、及びインストールされたアプリケーションのファイルが入っていて、通常最初にウィルスに感染します。
- 毎日午前2時にシステムスキャンを実行する - BitDefenderが毎日午前2時にお使いのコンピュータで標準スキャンを実行するように設定します。 スキャンを実行する時間を変更するには、メニューをクリックして、希望する開始時間を選択します。 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、そのスキャンは次にコンピュータを起動した時間に実行されます。

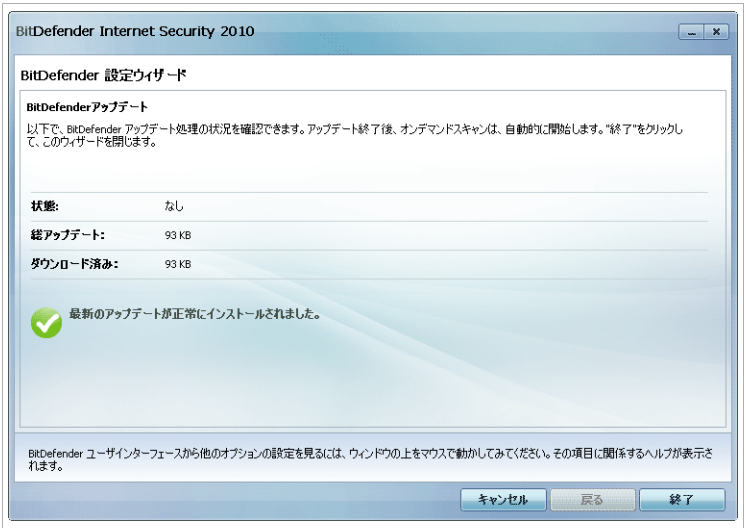
**注意**
後でスキャンを実行する時間を変更したい場合は、次の手順に従ってください：

1. BitDefenderを開いて、ユーザインターフェイスを'上級者モード'に切り替えてください。
2. 左メニューにあるアンチウィルスをクリックします。
3. ウィルススキャン タブをクリックします。
4. 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。
5. 頻度と開始時間を必要に応じて変更する。
6. 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。 次へをクリックしてください。

最初のチェック欄を削除すると、ウィザードの最終手順で実行するタスクはありません。 終了をクリックして、ウィザードを閉じてください。

### 3.2.7. 手順 7 - 終了




タスクの状況

BitDefender がマルウェアシグネチャや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すると、クイックシステムスキャンが起動します。 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示する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。

終了をクリックして、ウィザードを閉じてください。 スキャン完了まで、待つ必要はありません。

注意

スキャンにはしばらく時間がかかります。終了時にスキャン画面を開いて、お使いのシステムがクリーンかどうかスキャン結果をご確認ください。 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。

# 4. アップグレード

BitDefender Internet Security 2010 ベータ版、あるいは2008、2009のバージョンを使用している場合は、BitDefender Internet Security 2010 をアップグレードすることができます。

アップグレードを実行する二つの方法があります：

- BitDefender Internet Security 2010を、古いバージョンから直接インストールします。 2009バージョンを直接インストールする場合は、友人及び迷惑メール送信リスト、隔離領域は自動的に読み込まれます。
- 古いバージョンを削除して、コンピュータを再起動し、 「BitDefenderのインストール」 (p. 5)章に記述されている新しいバージョンをインストールしてください。 製品設定は保存されません。 他の方法が上手くいかない場合は、このアップグレード方法をお使いください。

# 5. BitDefenderの修復または削除

BitDefender Internet Security 2010を修復又は削除したい場合は、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 2010 → 修復又は削除。

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。

  表示が出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、BitDefender Internet Security 2010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ィンドウが開きます。 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

  **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**
  BitDefenderを削除するとウィルス、スパイウェア、ハッカーから、もはや保護されなくなります。 BitDefenderのアンインストール後、WindowsファイアウォールおよびWindows Defender (Windows Vistaのみ) を有効にするには、対応するチェックボックスを選択してください。

  お使いのコンピュータから BitDefender Internet Security 2010 を削除開始するには、削除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ィンドウが開きます。 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。

# 使い方

# 6. 概要

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。 特定した問題に関して、BitDefenderが警告を出さないように設定することが可能です。

製品登録（BitDefenderアカウントの作成を含む）をしていない場合には、試用期間終了までに登録を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. 52).

## 6.1. BitDefenderを開く

BitDefender Internet Security 2010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 2010 → BitDefender Internet Security 2010 を選ぶか、又はより早い方法として、次の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。

## 6.2. ユーザインタフェース設定モード

BitDefender Internet Security 2010 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。

お客様のコンピュータスキルや、BitDefenderを使用していた過去の経験に合わせて、以下の3つのユーザインターフェイスからモードを選択できます。

| モード | 解説 |
| --- | --- |
| 初級者モード | コンピュータの初心者及び、簡単な設定でBitDefenderがコンピュータとデータを保護してほしいユーザに適しています。このモードは、使い方が簡単で、最小限のやり取りで設定が可能です。<br><br>お客様に行っていただくことは、BitDefenderが表示した既存の問題を修復するだけです。使いやすく段階を追った手順のウィザードが、問題修復の手助けをします。 さらに、BitDefenderウィルスシグネチャ、製品 |

| モード | 解説 |
| --- | --- |
| | ファイル、またはコンピュータのスキャンのアップデート等、共通のタスクを実行することができます。 |
| 中級者モード | コンピュータスキルが標準なユーザに適しています。このモードは、初級者モードで出来る内容を拡張しています。<br>問題を別々に修復することが出来、どの問題を監視するかを選択します。 さらには、リモートから、ご自宅のコンピュータにインストールされている BitDefender 製品を管理することができます。 |
| 上級者モード | このモードは、上級者ユーザに適しており、BitDefenderの各機能を全面的に設定することができます。 また、お使いのコンピュータやデータを保護するため、提供されている全てのタスクを使用することができます。 |

ユーザインターフェースモードは、設定ウィザードで選択されています。 このウィザードは、登録ウィザード（製品のインストール後、最初にコンピュータを開くと表示）の後に表示されます。 登録ウィザードをキャンセルすると、ユーザインターフェースは、デフォルトで'中級者モード'に設定されます。

ユーザインターフェースモードを変更するには、以下の手順に従ってください：

1. BitDefenderを開く。
2. ウィンドウの右上にある設定 ボタンをクリックしてください。
3. ユーザインターフェイスの設定カテゴリ内の、にある矢印をクリックして、メニューから対象のモードを選択します。
4. OKをクリックして、変更を保存し、それを適用してください。

### 6.2.1. 初心者モード

お客様のコンピュータスキルが初級者の場合は、表示されているユーザインターフェイスの'初心者モード'は、最も適しています。 このモードは使い方が簡単で、最低限の設定のみです。


初心者モード

このウィンドウは、4つの主なセクションで構成されています：

- セキュリティの状態 が、お使いのコンピュータセキュリティに影響を与える問題をお知らせし、それを修復する手助けをします。 全ての問題を解決するをクリックすると、ウィザードが、お客様のコンピュータやデータセキュリティに対する脅威を、簡単に削除します。 詳細については、「問題を修正」 (p. 40)を参照してください。
- PCを保護する では、お使いのコンピュータやデータを保護するために必要なタスクを検出することができます。 実行可能な有効なタスクは、選択した使用プロファイルに応じて異なります。
  - 今すぐスキャン ボタンは、ウィルス、スパイウェア、他のマルウェアに対して、お使いのシステムに標準スキャンを開始します。 アンチウィルス スキャン ウィザードは、スキャン処理を通して表示されます。 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. 57)
  - 今すぐアップデートボタンは、BitDefenderのウィルスシグネチャ及び製品ファイルのアップデートを手助けをします。 アップデート状況を表示するウィンドウが新たに開きます。 アップデートが検出されると、お使いのコンピュータに自動的にダウンロードされて、インストールを実行します。
  - 標準 プロファイルが選択されると、脆弱性チェック ボタンがウィザードを開始して、期限切れのソフトウェアや行われていないWindowsアップデート等の、システムの脆弱性を発見して修復します。 詳細については、次を参照してください。「脆弱性チェックウィザード」 (p. 69).

- ペアレントプロファイルを選択すると、ペアレンタルコントロール ボタンで、ペアレンタルコントロールを設定します。 ペアレンタルコントロールは、お客様が定義したルールに基づいて、お子様のコンピュータ及びオンライン活動を制限します。 各種制限には、不適切なウェブサイトのブロックの他に、指定したスケジュールに従ったゲームやインターネットのアクセス制限を含んでいます。 ペアレンタルコントロールの設定方法について詳細は、「ペアレンタルコントロール」 (p. 191)を参照してください。
- ゲーマープロファイルが選択されると、 ゲームモードをオン/オフに切り替えるボタンで ゲームモードを有効/無効に切り替えることができます。 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。

●お使いのPCの性能を維持 では、お使いのコンピュータやデータを保護するために追加のタスクを見つけることができます。

- ファイル金庫に追加 ウィザードを開始して重要なファイル、ドキュメントを暗号化された特別の金庫ドライブに格納します。
- 完全システムスキャン は、全ての種類のマルウェアに対して、お使いのシステム全体のスキャンを開始します。
- マイドキュメントのスキャンは、最も良く使用されているフォルダのウィルスや他のマルウェアをスキャンします : マイドキュメント 及び デスクトップ. これは、お使いのドキュメントの安全性、安全なワークスペース、及び起動時にクリーンなアプリケーションが実行することを保つことができます。

●使用プロファイル は、現在選択している使用プロファイルを表示します。 使用プロファイルは、コンピュータで実行された主な処理を示します。ユーザプロファイルに応じて、製品インターフェースは、希望するタスクへ簡単にアクセスすることができるように構成されています。

別のプロファイルに切り替える、または現在使用しているものを修正するには、プロファイルをクリックして、この設定ウィザードに従ってください。

ウィンドウの右上にある、設定ボタンで確認することができます。ユーザインターフェースモードの変更や、 BitDefenderの主な設定を有効/無効に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。 「Basic 設定 」 (p. 44).

ウィンドウの右下に、複数の便利なリンクがあります。

| リンク | 解説 |
|---|---|
| 購入／更新 | ウェブページを開いて、そこでBitDefender Internet Security 2010のライセンスキーを購入できます。 |

| リンク | 解説 |
| --- | --- |
| 登録 | 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 & サポート | BitDefenderの使い方を表示するヘルプファイルです。 |

### 6.2.2. 中級者モード

中級者モードは、標準的なコンピュータスキルのユーザが対象で、基本レベルで、全てのモジュールに対してアクセスできる簡単なインターフェイスです。ユーザは、通知や重大な警告を追跡して、望ましくない問題を解決する必要があります。


中級者モード

中級者モード画面は、5つのタブで構成されています。以下のテーブルで、各タブを簡単に説明しています。 詳細については、この「中級者モード」 (p. 94) ユーザガイドの一部を参照してください。

| タブ | 解説 |
| --- | --- |
| ダッシュボード | お使いのシステムのセキュリティの状態を表示して、使用プロファイルをリセットしてください。 |
| セキュリティ | セキュリティモジュール（アンチウィルス、アンチフィッシング、ファイアウォール、アンチスパム、IM暗号化、プライ |

| タブ | 解説 |
| --- | --- |
| | バシー、脆弱性チェック、アップデートモジュール）の状態を表示します。またアンチウィルス、アップデート、脆弱性チェックタスクへのリンクがあります。 |
| ペアレンタル | ペアレンタルコントロールモジュールの状態を表示します。ペアレンタルコントロールはお子様のインターネットへのアクセスや指定したアプリケーションの利用に、使用を制限することができます。 |
| ファイル金庫 | ファイル金庫の状態とそこへのリンクを表示します。 |
| 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。 |

ウィンドウの右上にある、設定ボタンで確認することができます。ユーザインターフェースモードの変更や、 BitDefenderの主な設定を有効/無効に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。 「Basic 設定 」 (p. 44).

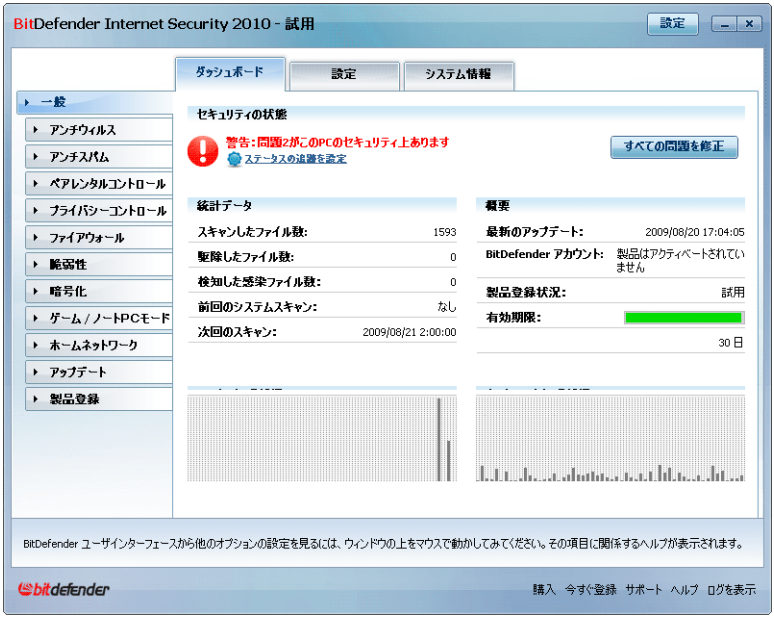
ウィンドウの右下に、複数の便利なリンクがあります。

| リンク | 解説 |
| --- | --- |
| 購入／更新 | ウェブページを開いて、そこでBitDefender Internet Security 2010のライセンスキーを購入できます。 |
| 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。 |
| サポート | BitDefenderのサポートウェブページを開きます。 |
| ヘルプ | BitDefenderの使い方を表示するヘルプファイルです。 |
| ログを表示 | 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。 |

### 6.2.3. 上級者モード

上級者モードでは、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を設定することができます。

**注意**
上級者モードは、標準的なコンピュータスキル以上のユーザが対象で、コンピュータの脅威の種類や、どのようにセキュリティプログラムが実行するかを理解している方です。



上級者モード

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： 各モジュールには、該当するセキュリティ設定を行えるタブが1つ以上あり、セキュリティ又は管理タスクを実行します。 以下のテーブルは、各モジュールを簡単に説明しています。詳細については、この「上級者モード」（p. 119）ユーザガイドの一部を参照してください。

| モジュール | 解説 |
|---|---|
| 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。 |

| モジュール | 解説 |
| --- | --- |
| アンチスパム | 受信箱をいつもスパムメールがない状態にするためにアンチスパム設定を詳細に構成します。 |
| ペアレンタルコントロール | 構成されたコンピュータアクセスルールに基づき、お子さまを不適切なコンテンツから守ります。 |
| 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。 |
| ファイアウォール | お使いのコンピュータを、許可していない外部への接続、また外部から内部への接続を保護します。これは入り口にいるガードマンに似ています。インターネット接続を監視して、インターネットへアクセスを許可する人、ブロックする人を管理します。 |
| 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、Windows Live(MSN)メッセンジャーの通信を暗号化します。また重要なファイル、フォルダ、パーティションも暗号化します。 |
| 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時にスケジュールされているタスクを延期したり、ゲームを楽しんでいる時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。 |
| 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 Internet Security 2010 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ことができます。 |

ウィンドウの右上にある、設定ボタンで確認することができます。ユーザインターフェースモードの変更や、 BitDefenderの主な設定を有効/無効に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。 「Basic 設定 」 (p. 44).

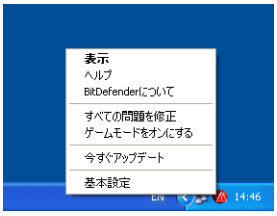
ウィンドウの右下に、複数の便利なリンクがあります。

| リンク | 解説 |
| --- | --- |
| 購入／更新 | ウェブページを開いて、そこでBitDefender Internet Security 2010のライセンスキーを購入できます。 |

| リンク | 解説 |
|---|---|
| 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。 |
| サポート | BitDefenderのサポートウェブページを開きます。 |
| ヘルプ | BitDefenderの使い方を表示するヘルプファイルです。 |
| ログを表示 | 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。 |

## 6.3. システムトレイのアイコン

製品全体をより早く管理するには、システムトレイ内にある、この BitDefender アイコンを使用することができます。 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。




トレイアイコン

- 表示 – BitDefenderのメイン画面を開きます。
- ヘルプ – ヘルプファイルを開きます。ヘルプにはBitDefender Internet Security 2010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、「問題を修正」 (p. 40)を参照してください。
- ゲームモードをオン / オフ –ゲームモードを アクティブ / 非アクティブ に設定します。
- 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ィンドウが新たに開きます。

- 基本設定 - ウィンドウを開くと、ユーザインターフェースモードが変更でき、製品の主な設定を有効/無効に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。「Basic 設定 」 (p. 44).

BitDefenderシステムトレイアイコンは、問題がお使いのコンピュータに影響を与えるとき、あるいは、製品がどのように動作するか、以下のような特別な記号でお知らせします：

感嘆符付きの赤い三角: 重大な問題がお使いのシステムのセキュリティに影響を与えています。至急、対応が求められており、修正する必要があります。
感嘆符付きの黄色い三角: お使いのシステムのセキュリティに影響する重大な問題はありません。お時間があるときに、それを確認して修正を行ってください。
文字G: この製品はゲームモードに設定されています。

BitDefenderが実行していない場合は、システムトレイのアイコンは、グレーで表示されます。 これは通常、ライセンスキーの期限切れの際に発生します。BitDefenderサービスが応答していない時や、別のエラーがBitDefenderの処理に影響を与えるときにも発生します。

## 6.4. 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。 この小さなウィンドウは、デフォルトで、上級者モードにのみ有効です。

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。 ネット帯域に表示されるオレンジ色のバーは転送されたデータの秒あたりのキロバイト数（インターネットからの送受信）を0から100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、リアルタイム保護やファイアウォールが無効の時に対応する（ファイル領域またはネット領域）部分に赤いバツ印を表示してユーザに通知します。

### 6.4.1. 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アクティビティバーへドラッグ&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 ウィザードは、スキャン処理を通して表示されます。 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. 57）

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）を試みます。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指示します。 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。

### 6.4.2. スキャンアクティビティバーを無効/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. ウィンドウの右上にある設定 ボタンをクリックしてください。
3. 一般設定で、スキャンアクティビティバーに該当する、チェック欄を選択します。
4. OKをクリックして、変更を保存し、それを適用してください。

## 6.5. 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。 もしシステムが強力な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 2010 → 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

フォルダを追加をクリックして、スキャンしたい場所を選択して、 OKをクリックします。 複数のフォルダをスキャンしたい場合は、それぞれ追加した場所に、この処理を繰り返してください。

選択した場所のパスが、スキャン対象に表示されます。 スキャンの対象を変更する場合には、削除ボタンをクリックします。 全てのパスを削除ボタンをクリックすると、リストに追加された全ての保存場所を削除します。

保存場所を選択すると、継続をクリックします。 アンチウィルス スキャン ウィザードは、スキャン処理を通して表示されます。 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. 57)

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）を試みます。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指示します。 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。

## 6.6. ゲームモードとノートＰＣモード

ゲームやプレゼンテーション等、いくつかのコンピュータ活動は、システムのレスポンスやパフォーマンスの向上が必要で、割り込みができません。 お使いのノートPCがバッテリー充電で実行されていると、追加充電を不要とする状態は、ノートPCがA/C 充電に戻って接続されるまで、継続されます。

このような特別な状況に適応するために、BitDefender Internet Security 2010 は次のような２つのオペレーションモードがあります：

- ゲームモード
- ノートPCモード

### 6.6.1. 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：

- 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。

## ゲームモードを使用

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。 BitDefender は、ゲーム終了時、又は検出されたアプリケーションがフルスクリーンを終了するとき、自動的に通常処理モードに戻ります。

ゲームモードを手動で有効にしたい場合は、以下のいずれかの方法を使用してください：

- 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。

## 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を開いて、ユーザインターフェイスを'上級者モード'に切り替えてください。
2. 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。
3. ゲームモードタブをクリックします。
4. 詳細設定ボタンをクリックします。
5. 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。

6. OKをクリックして変更を保存します。

### 6.6.2. 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用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モード中は、スケジュールされたスキャンタスクは実行されません。なぜならば、より多くのシステムリソースを要求するので、電力消費が暗黙的に増加するからです。

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モードを使用するには、この設定ウィザードで、ノートPCを使用していることを指定してください。　ウィザードの実行中に、適したオプションを選択しなかった場合は、以下に従い、ノートPCモードを後で有効にすることができます：

1. BitDefenderを開く。
2. ウィンドウの右上にある設定 ボタンをクリックしてください。
3. 一般設定で、ノートPCモード検出に該当するチェック欄を選択します。
4. OKをクリックして、変更を保存し、それを適用してください。

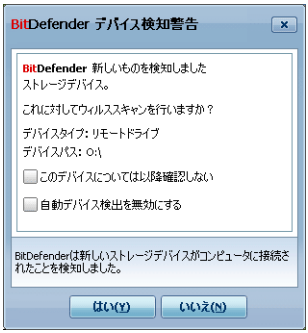
## 6.7. 自動検出装置

BitDefenderは、取り外し可能なストレージデバイスをお使いのコンピュータに接続すると、自動的にそれを検出して、ファイルにアクセスする前にスキャンを行います。 これは、お使いのコンピュータを、ウィルスや他のマルウェアの感染から保護するため、推奨されます。

検出されたデバイスは、これらのカテゴリの１つに該当します：

- CDs/DVDs
- USBストレージデバイス、フラッシュペンや外付けハードドライブ等
- マップされた(リモート) ネットワークドライブ

デバイスが検出されると、警告ウィンドウが表示されます。




デバイス検知報告

ストレージデバイスをスキャンするには、 ”はい”をクリックしてください。 アンチウィルス スキャン ウィザードは、スキャン処理を通して表示されます。 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. 57)

デバイスをスキャンしたくない場合は、 スキャンしないをクリックしてください。 この場合、次のオプションから適するものを選択してください：

- 今後この形式のデバイスに関して表示しない - 今後BitDefender は、お使いのコンピュータに接続時、この形式のストレージデバイスをスキャンしません。
- 自動デバイス検出を無効にする - 新しいストレージデバイスがコンピュータに接続された時、スキャンを行いません。

誤って無効にしてしまった自動デバイス検知を有効にするには、またその構成を設定するには次の手順に従ってください：

1. BitDefenderを開いて、ユーザインターフェイスを'上級者モード'に切り替えてください。
2. アンチウィルス>ウィルススキャンへ進む。
3. スキャンタスクのリスト内で、このデバイス検出をスキャンタスクを探します。
4. タスクを右クリックして、開くを選択します。 新しいウィンドウが開きます。
5. 概要タブで、必要に応じてスキャンオプションを設定します。 詳細については、「スキャン設定を行う」 (p. 144)をご参照ください。
6. 検索タブで、どの形式の記憶デバイスを検出するかを選択します。
7. OKをクリックして、変更を保存し、それを適用してください。

# 7. 問題を修正

BitDefenderは、問題追跡システムを使用して、お使いのコンピュータやデータのセキュリティに影響を与えているかもしれない問題に関して、検出及び通知を行います。デフォルトで、大変重要とみなされる一連の問題のみを監視します。また一方で、必要に応じて、どの問題を通知するかを選択することが可能です。

このようにして未解決の問題が通知されます：

- 特別な記号は、システムトレイ内のBitDefenderアイコン上に表示されて、未解決の問題をお知らせします。

  感嘆符付きの赤い三角：重大な問題がお使いのシステムのセキュリティに影響を与えています。至急、対応が求められており、修正する必要があります。
  感嘆符付きの黄色い三角：お使いのシステムのセキュリティに影響する重大な問題はありません。お時間があるときに、それを確認して修正を行ってください。

  また、アイコン上でマウスカーソルを移動すると、ポップアップ画面で、未解決の問題を表示します。

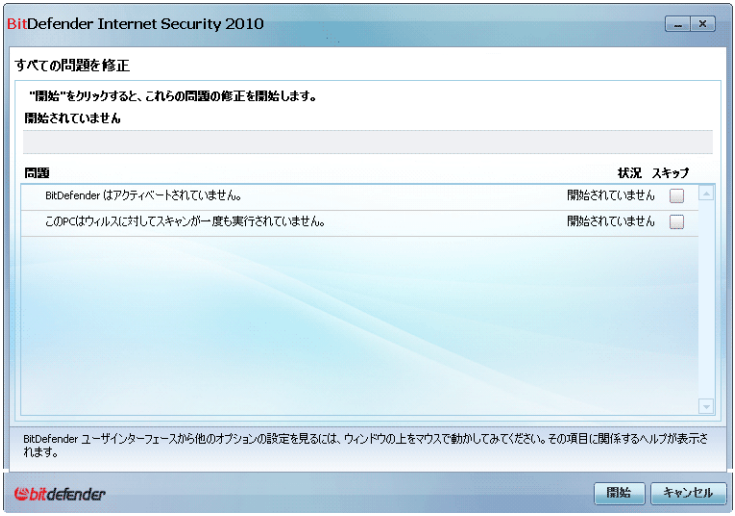
- BitDefenderを開くと、セキュリティステータスがお使いのシステムに影響を与える問題の数を表示します。
  - 中級者モードで、セキュリティステータスがダッシュボートタブに表示されます。
  - 上級者モードの、一般設定>ダッシュボードへ進み、セキュリティステータスを確認します。

## 7.1. 全ての問題を修正するウィザード

既存の問題を修正する最も簡単な方法は、段階的に全ての問題を修復する ウィザードに従います。 ウィザードで、お使いのコンピュータのあらゆる脅威を簡単に削除し、データセキュリティの手助けをします。 ウィザードを開いて、次のいずれかを実行してください：

- 右クリックします。これはシステムトレイ内のBitDefenderアイコンです。そして全ての問題を修正するを選択します。
- BitDefenderを開く。 ユーザインターフェースモードに応じて、次の処理を行ってください：
  - 初級者モードでは、全ての問題を修復をクリックしてください。
  - 中級者モードで、ダッシュボードタブに進み、全ての問題を修復するをクリックしてください。

- 上級者モードの、一般設定>ダッシュボードへ進み、全ての問題を修復するをクリックしてください。




全ての問題を修正するウィザード

このウィザードは、お使いのコンピュータに既存するセキュリティの脆弱性の一覧を表示します。

全ての現在の問題が選択されて修正されました。修正したくない問題がある場合は、該当するチェック欄を選択してください。そうすると、その状態はスキップに変更になります。

**注意**
特定の問題に関して通知されたくない場合は、次の項で記載されている通りに従って、追跡システムを設定してください。

選択された問題を修正するには、開始をクリックします。いくつかの問題が直ぐに修正されます。その他の問題は、ウィザードに従って修正してください。

このウィザードに従って修正する問題は、主に次のカテゴリに分類することができます。

- セキュリティ設定を無効にする. このような問題は、それぞれのセキュリティ設定を有効にして、直ちに修正されます。
- 実行する必要がある予防手段のセキュリティタスク. この場合のタスク例は、お使いのコンピュータのスキャンです。少なくとも週に1回はコンピュータをスキャ

ンすることをお勧めします。BitDefenderは、ほとんどの場合に自動的にスキャンを行いますが、スキャンスケジュールを変更したり、あるいはスケジュール設定が完了していないと、この問題に関して通知されます。

このような問題が修正されると、問題なくこのタスクを終了するようにウィザードが導きます。

- システムの脆弱性. BitDefenderは、お使いのシステムの脆弱性を自動的に確認をして、警告を行います。 以下を含むシステムの脆弱性：
  - Windowsユーザアカウントに対する弱いパスワード
  - お使いのコンピュータの期限切れのソフトウェア
  - Windowsアップデートが行われていません
  - Windows自動アップデートは無効です

  このような問題が修正されると、脆弱性スキャンウィザードが開始します。このウィザードは、検出されたシステムの脆弱性の修復を手助けします。 詳細については、次を参照してください。「脆弱性チェックウィザード」 (p. 69).

## 7.2. 問題の監視を設定

問題追跡システムは、監視するために事前に設定されていて、お使いのコンピュータやデータのセキュリティに影響を与えうる最も重要な問題に関して警告します。追加の問題は 設定ウィザード内で行った選択に基づいて監視されます。(使用プロファイルの設定時). デフォルトで監視された問題の他に、通知されるいくつかの問題があります。

どの問題を通知するかの選択次第で、セキュリティに最も必要な追跡システムを設定することができます、これは中級者モード、または上級者モードのいずれかで設定することができます。

- 中級者モードで、追跡システムは別の場所から設定することができます。 次の手順に従ってください：
  1. セキュリティ、ペアレンタル あるいはファイル金庫タブを選択してください。
  2. ステータスの追跡を設定をクリックしてください。
  3. 監視されたい項目に該当するチェック欄を選択します。

  詳細については、この「中級者モード」 (p. 94) ユーザガイドの一部を参照してください。

- 上級者モードでは、追跡システムは中心地から設定することができます。 次の手順に従ってください：
  1. 一般情報>ダッシュボードへ進む。
  2. ステータスの追跡を設定をクリックしてください。
  3. 監視されたい項目に該当するチェック欄を選択します。

詳細については、次を参照してください。「ダッシュボード」 (p. 120).

# 8. Basic 設定

基本設定ウィンドウから、製品の主要な設定を行います。（ユーザインターフェース設定モードの変更を含む）それを開くには、以下のいずれかを行ってください：

- BitDefenderを開いて画面右上にある 設定ボタンをクリックしてください。
- を右クリックします。これは システムトレイ内のBitDefenderアイコンです。そして基本設定を選択します。

**注意**

詳細の設定を行うには、上級者モードのインターフェースを使用してください。 詳細については、この「上級者モード」（p. 119）ユーザガイドの一部を参照してください。


基本設定

設定項目は３つの項に分類されます：

- ユーザインターフェースの設定
- セキュリティ設定
- 一般的な設定

設定変更を有効にして、保存するには、OKをクリックします。変更の保存をしないでウィンドウを閉じるには、 キャンセルをクリックします。

## 8.1. ユーザインターフェイス設定

この領域では、ユーザインターフェース画面を切り替えて、使用プロファイルを再設定することができます。

ユーザインターフェース設定モードを切り替えます。. 「ユーザインタフェース設定モード」 (p. 24)内に保存されているように、 ユーザインターフェースには３つの形式があります。それぞれのユーザインターフェースモードは、ユーザのコンピュータスキルに基づき、明確なユーザのカテゴリに対して設計されています。 このように、ユーザインターフェースは、コンピュータの初級者から、上級者まであらゆるユーザに対応します。

最初のボタンは、現在のユーザインターフェース設定を表示します。 ユーザインターフェースモードを変更するには、にある矢印をクリックして、メニューから対象のモードを選択します。

| モード | 解説 |
|---|---|
| 初級者モード | コンピュータの初心者及び、簡単な設定でBitDefenderがコンピュータとデータを保護してほしいユーザに適しています。このモードは、使い方が簡単で、最小限のやり取りで設定が可能です。<br>お客様に行っていただくことは、BitDefenderが表示した既存の問題を修復するだけです。使いやすく段階を追った手順のウィザードが、問題修復の手助けをします。 さらに、BitDefenderウィルスシグネチャ、製品ファイル、またはコンピュータのスキャンのアップデート等、共通のタスクを実行することができます。 |
| 中級者モード | コンピュータスキルが標準なユーザに適しています。このモードは、初級者モードで出来る内容を拡張しています。<br>問題を別々に修復することが出来、どの問題を監視するかを選択します。 さらには、リモートから、ご自宅のコンピュータにインストールされている BitDefender 製品を管理することができます。 |
| 上級者モード | このモードは、上級者ユーザに適しており、BitDefenderの各機能を全面的に設定することができます。 また、お使いのコンピュータやデータを保護する |

| モード | 解説 |
| --- | --- |
| | ため、提供されている全てのタスクを使用することができます。 |

使用プロファイルを再設定する。. 使用プロファイルは、コンピュータで実行された主な処理を示します。ユーザプロファイルに応じて、製品インターフェースは、希望するタスクへ簡単にアクセスすることができるように構成されています。

使用プロファイルを再設定するには、使用プロファイルを再設定するをクリックして、設定ウィザードに従ってください。

## 8.2. セキュリティ設定

ここで、コンピュータの多様な側面やデータセキュリティを保護する製品の設定を有効又は無効にすることができます。 現在の設定状況は、次のアイコンのいずれかを使用して表示されています:

チェックマーク付きの緑色の丸: 設定は有効です。
感嘆符付きの赤い丸: 設定は無効です。

設定を有効又は無効にするには、 該当する有効にする チェックボックスを選択又はクリアにします。

**警告**

リアルタイムアンチウィルスプロテクション、ファイアーウォール、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。

設定とその詳細の全リストは、次の表に記載されています :

| 設定 | 解説 |
| --- | --- |
| アンチウィルス | リアルタイムプロテクションは、お客様がアクセスするファイル、あるいはこのシステム上で実行しているアプリケーションの全てのファイルをスキャンします。 |
| 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製品とシグネチャファイルを、自動的にダウンロードしインストールします。 |
| 脆弱性を確認 | 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。 |

| 設定 | 解説 |
| --- | --- |
| アンチスパム | アンチスパムは、受信した電子メッセージをフィルタして、未承諾メールや迷惑メールをスパムとしてマークします。 |
| アンチフィッシング | アンチフィッシングは、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、ユーザの確認なしに、インターネット上で個人情報を送信することを妨げます。ユーザが定義した許可しない受信者（アドレス）から情報を保護するために、インスタントメッセージ、電子メールメッセージ、又はウェブ形式のデータをブロックします。 |
| インスタントメッセージ暗号化 | IM(インスタントメッセージ）暗号化は、IMの相手先がBitDefender製品とIMソフトウェアに互換性があるという条件で、Yahoo!メッセンジャーやWindows Live Messenger 経由のユーザの会話を保護します。 |
| ペアレンタルコントロール | ペアレンタルコントロールは、お客様が定義したルールに基づいて、お子様のコンピュータ及びオンライン活動を制限します。 各種制限には、不適切なウェブサイトのブロックの他に、指定したスケジュールに従ったゲームやインターネットのアクセス制限を含んでいます。 |
| ファイアウォール | ファイアウォールはお使いのコンピューターをハッカーや悪意のある外部からの攻撃から守ります |
| ファイル暗号化 | ファイル金庫はドキュメントを、暗号化して、特別な保管ドライブに保持することで隠遁します。 ファイル金庫を無効にすると、全ての金庫のファイルがロックされるため、その金庫にあるファイルにアクセスすることができなくなります。 |

これらの設定のステータスの中には、BitDefenderが問題を追跡するシステムによって監視されるものもあります。 監視される設定が無効の場合は、BitDefenderは、修正が必要な問題として表示します。

問題として表示しない設定を監視されたくない場合は、それに応じて追跡システムを設定しなければなりません。その設定は中級者モード、又は上級者モードで行うことができます。

- 中級者モードで、追跡システムは設定カテゴリに基づいて、離れた場所から設定することができます。 詳細については、この「中級者モード」 (p. 94) ユーザガイドの一部を参照してください。
- 上級者モードでは、追跡システムは中心地から設定することができます。 次の手順に従ってください：
  1. 一般情報>ダッシュボードへ進む。
  2. ステータスの追跡を設定をクリックしてください。
  3. 監視されたくない項目に該当するチェック欄を削除します。

  詳細については、次を参照してください。「ダッシュボード」 (p. 120).

## 8.3. 全体設定

ここでは、製品ビヘイビアやユーザ体験に影響する設定を有効/無効にできます。設定を有効又は無効にするには、 該当する有効にする チェックボックスを選択又はクリアにします。

設定とその詳細の全リストは、次の表に記載されています：

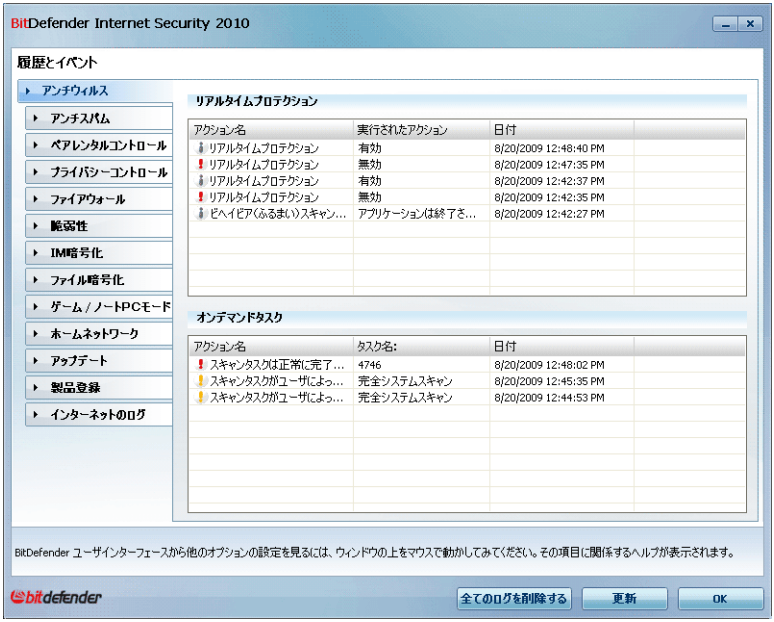
| 設定 | 解説 |
|---|---|
| ゲームモード | ゲームモードはゲームの処理への影響を最小限にするよう保護設定を一時的に変更します。 |
| ノートＰＣモードを検出 | ノートＰＣモードはバッテリ消費への影響を最小限にするよう保護設定を一時的に変更します。 |
| パスワード設定 | パスワードを知っている人だけが設定変更ができるようになります。<br>このオプションを有効にすると、パスワードの設定が求められます。 両方の該当欄にパスワードを入力して、OKをクリックして、パスワードを設定します。 |
| BitDefender News | このオプションを有効にするとBitDefender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。 |
| 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く、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. 33) を参照してください。 |

| 設定 | 解説 |
| --- | --- |
| 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. 履歴とイベント

BitDefender メインウィンドウの下にあるログを表示リンクは、BitDefender の履歴&イベントを表示する別のウィンドウを開きます。このウィ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。

**注意**
このリンク先は中級者モードか上級者モードでのみ接続することが可能です。




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：

- アンチウィルス
- アンチスパム
- ペアレンタルコントロール
- 個人情報コントロール

- ファイアウォール
- 脆弱性
- IM暗号化
- ファイル暗号化
- ゲーム/ノートＰＣモード
- ホームネットワーク
- アップデート
- 登録
- インターネットログ

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、それが発生した際にBitDefenderが実行したアクション、発生した日時、です。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全ての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。

# 10. 登録とマイアカウント

BitDefender Internet Security 2010 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。

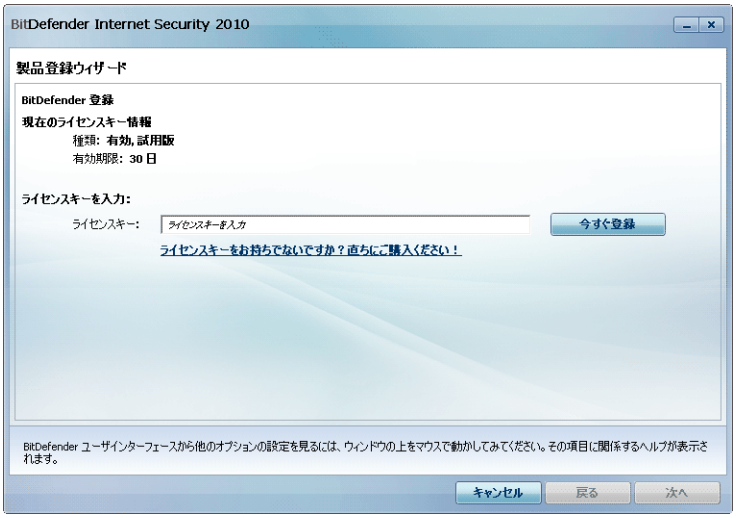
   **重要項目**

   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。

## 10.1. BitDefender Internet Security 2010を登録

ライセンスキーで製品を登録、または現在のライセンスキーを変更したい場合は、BitDefenderウィンドウの下にある今すぐ登録するをクリックしてください。 製品登録ウィンドウが表示されます。




製品登録

BitDefender 登録状況では、お使いのライセンスキーが切れるまでの残日数を確認することができます。

BitDefender Internet Security 2010を登録:

1. ライセンスキーを入力します。

   **注意**
   ライセンスキーは以下に記載されています：
   ●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。

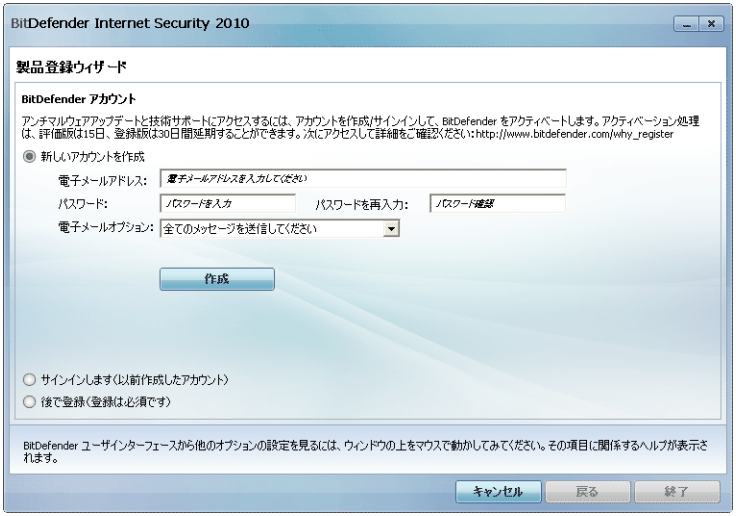
2. 今すぐ登録するをクリックします。
3. 終了をクリックします。

## 10.2. BitDefenderをアクティベート

BitDefenderをアクティベートするには、 BitDefenderアカウントを作成してサインインする必要があります。 最初の登録ウィザードでBitDefenderアカウントを登録していない場合は、以下に従って登録することができます：

- 初級者モードでは、全ての問題を修復をクリックしてください。 このウィザードは、製品のアクティベートを含めて、全ての未解決の問題を修正する手助けをします。
- 中級者モードで、セキュリティ タブで、製品のアクティベーションに関する問題の修正ボタンをクリックしてください。
- 上級者モードの、登録へ進み、製品のアクティベートボタンをクリックしてください。

アカウント登録ウィンドウが開きます。 ここで製品をアクティベートするBitDefenderアカウントを作成、サインインをすることができます。




アカウント作成

もし、いまBitDefenderアカウントを作成されない場合には、後で登録を選択し、終了をクリックしてください。 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. 55)
- 「既にBitDefenderアカウントを持っている場合」 (p. 55)

### 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

正しくBitDefenderアカウントを作成するには、次の手順に従ってください：

1. 新しいアカウントを作成するを選択します。
2. 該当する欄に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。

   **注意**
   アカウントが有効になると、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からアカウントにログインしてください。

3. 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お客様のメールアドレスに送信することがあります。 メニューから有効なオプションを選択してください：
   - ●全てのメッセージを受信
   - ●製品に関するメッセージだけを受信
   - ●全てのメッセージを受け取らない
4. 作成をクリックしてください。
5. 終了をクリックして、ウィザードを閉じてください。
6. 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。

## 既にBitDefenderアカウントを持っている場合

お客様が既に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、お客様のアカウントのパスワードを入力して、サインインをクリックしてください。 終了をクリックして、ウィザードを閉じてください。

有効なアカウントを持っていて、BitDefenderがそれを検出しない場合は、そのアカウントで製品を登録するために次の手順に従ってください。

1. サインイン（以前に作成されたアカウント）を選択してください。

2. 該当欄にお使いのアカウントの電子メールアドレスとパスワードを入力してください。

注意
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。

3. 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お客様のメールアドレスに送信することがあります。 メニューから有効なオプションを選択してください：
   - 全てのメッセージを受信
   - 製品に関するメッセージだけを受信
   - 全てのメッセージを受け取らない
4. サインインをクリックしてください。
5. 終了をクリックして、ウィザードを閉じてください。

## 10.3. ライセンスキーの購入

試用期間は、間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。

## 10.4. 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ることができます。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。

# 11. ウィザード

BitDefenderを簡単にご使用いただくために、数種類のウィザードが特定のセキュリティタスクの実行を手助けし、複雑な製品設定を行います。 この章では、BitDefenderで問題を解決、又は特定したタスクを実行するときに、表示されるウィザードに関して記載しています。 「上級者モード」 (p. 119)内に、他の設定ウィザードが個別に記載されています。

## 11.1. アンチウィルススキャンウィザード

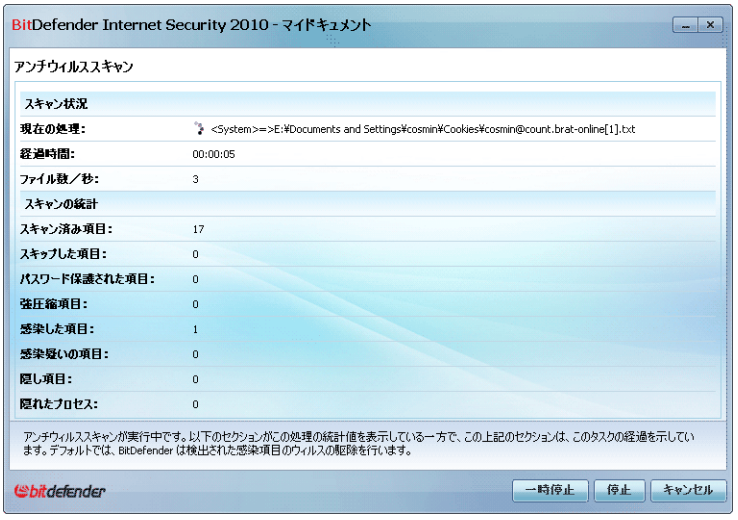
オンデマンドスキャンを実行すると（フォルダを右クリックして BitDefenderでスキャンを選択）、BitDefender アンチウィルススキャンウィザードが表示されます。以下の３つの手順に従ってスキャン処理を完了させてください。

**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。

### 11.1.1. 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。 パスワードで保護されたアーカイブは、お客様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。

### 11.1.2. 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：

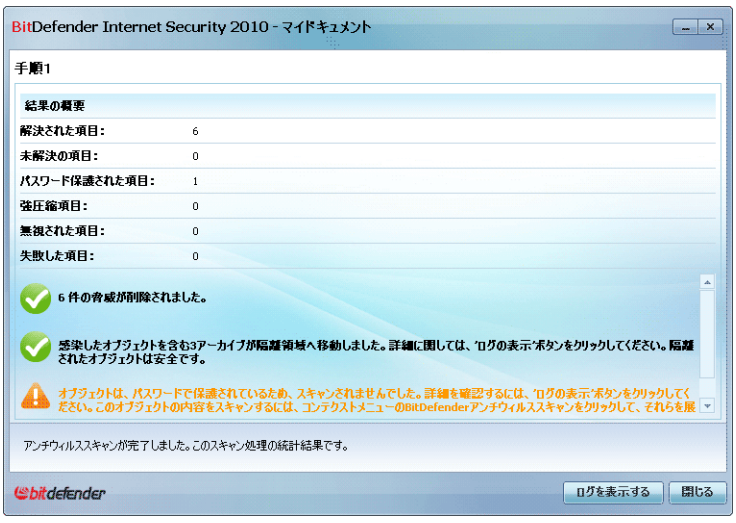
| アクション | 解説 |
|---|---|
| アクションなし | 検出したファイルに対してアクションを実行しません。スキャン完了後、スキャンログを開いてこれらのファイルの情報をみることができます。 |
| ウィルスを駆除 | 感染しているファイルからマルウェアのコードを取り除きます。 |
| 削除 | 検出したファイルを削除します。 |
| ファイルを隔離領域へ移動 | 感染ファイルを隔離領域へ移動します。　隔離されたファイルは実行されることも開かれることもありませ |

| アクション | 解説 |
| --- | --- |
| | 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。<br>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。

### 11.1.3. 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。 スキャン処理関して、全ての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駆除、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。

## 11.2. カスタムスキャンウィザード

カスタムスキャンウィザードは、カスタムスキャンタスクの作成及び実行へと導きます。中級者モードでBitDefenderを使用する際は、クイックタスクでそれを任意に保存します。

カスタムスキャンウィザードを使用して、カスタムスキャンタスクを実行するには、次の手順に従ってください：

1. 中級者モードのセキュリティタブをクリックしてください。
2. クイックタスクでは、カスタムスキャンをクリックしてください。
3. 以下の6つの手順に従って、スキャン処理を完了させてください。

### 11.2.1. 手順 1/6 - はじめに

これは初期設定画面です。


はじめに

今後、このウィザードの実行中にこのウィンドウを表示しない場合は、今後このウィザードの実行中にこの手順を表示しない欄を選択してください。

次へをクリックします。

### 11.2.2. 手順 2/6 - 対象を選択

ここでは、スキャンするファイルやフォルダを指定する他に、スキャンオプションを指定することができます。


選択対象

対象を追加をクリックして、スキャンしたいファイルやフォルダを選択し、OKをクリックします。選択した場所のパスは、スキャン対象欄に表示されます。 スキャンの対象を変更する場合には、削除ボタンをクリックします。 全てを削除 ボタンをクリックすると、リストに追加された全ての保存場所を削除します。

保存場所の選択を行うと、スキャンオプションの設定を行います。次の内容が設定可能です：

| オプション | 解説 |
|---|---|
| すべてのファイルをスキャン | このオプションを選択して、選択されたフォルダにある全てのファイルのスキャンを行います。 |
| アプリケーションの拡張子がある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。 |

| オプション | 解説 |
| --- | --- |
| ユーザが指定した拡張子のみをスキャン | ユーザが指定した拡張子を持つファイル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。 |

次へをクリックします。

### 11.2.3. 手順 3/6 - アクションを選択

ここで、スキャン設定やスキャンレベルを指定できます。


アクションを選択

- 検出された感染ファイルや疑わしいファイルに対するアクションを選択してください。 以下のオプションを指定できます：

| アクション | 解説 |
| --- | --- |
| 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。 |
| ファイルからウィルスを駆除 | 検出された感染ファイルからマルウェアコードを除去します。 |
| ファイルを削除 | 警告なしで感染ファイルを即時に削除します。 |

| アクション | 解説 |
| --- | --- |
| 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。 |

●隠しファイル(rootkit) に対するアクションを選択してください。 以下のオプションを指定できます：

| アクション | 解説 |
| --- | --- |
| 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。 |
| 名前を変更する | 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。 |

●スキャナの強さを設定 3つのレベルが選択できます。スライダをドラッグして、適切な保護レベルを設定します：

| レベルをスキャン | 解説 |
| --- | --- |
| 弱 | アプリケーションファイルだけが、ウィルスに対してのみスキャンされます。リソース消費のレベルは低いです。 |
| デフォルト | リソース消費のレベルは中位です。全てのファイルはウィルスやスパイウェアに対してスキャンされます。 |
| 強 | 全てのファイル（アーカイブを含む）は、ウィルスやスパイウェアに対してスキャンされます。隠しファイルやプロセスはスキャンに含まれます。リソース消費レベルはより高くなります。 |

上級者ユーザは、BitDefenderが提供するスキャン設定を活用したいかもしれません。スキャナは指定したマルウェアの脅威に対してのみを検索する設定が可能です。これによって大幅にスキャンの時間が削減されて、スキャン中のコンピュータのレスポンスが向上します。

スライダーをドラッグして、カスタムを選択し、 カスタムレベルボタンをクリックしてください。 ウィンドウが表示されます。 適切なオプションを選択して、BitDefenderがスキャンしたいマルウェアの種類を指定してください：

| オプション | 解説 |
| --- | --- |
| ウィルスを対象にスキャン | 既知のウィルスを対象にスキャンします。<br>BitDefenderは不完全なウィ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。 |
| キーロガーを対象にスキャン | キーストロークを記録する悪意のあるアプリケーションをスキャンします。 |

OKをクリックしてウィンドウを閉じます。

次へをクリックします。

### 11.2.4. 手順4/6 - 追加設定

スキャンを開始する前に、次の追加オプションが有効です：


追加設定

- 今後使用するために作成しているカスタムタスクを保存するには、中級者ユーザインターフェースでこのタスクを表示欄を選択して、入力欄にタスク名を入れてください。

  タスクはセキュリティタブ内の、既に有効なクイックタスクの一覧に追加されます。上級者モード> アンチウィルス > ウィルススキャン内にも表示されます。

- スキャンが終了した後、コンピュータの電源を切るには、スキャン終了後に脅威が発見されない場合は、コンピュータの電源を切る欄を選択してください。

スキャンを開始をクリックしてください。

### 11.2.5. 手順 5/6 - 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

**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。 をクリックします。これはスキャンが進行していることを表すアイコンで、システムトレイ内にあり、スキャンウィンドウを開いて、スキャンの進行を確認します。

### 11.2.6. 手順 6/6 - 結果を表示する

BitDefender がスキャンプロセスを完了したら、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

スキャンの結果を確認することができます。スキャン処理に関して全ての情報をご覧になりたい場合には、 ログを表示 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。

## 11.3. 脆弱性チェックウィザード

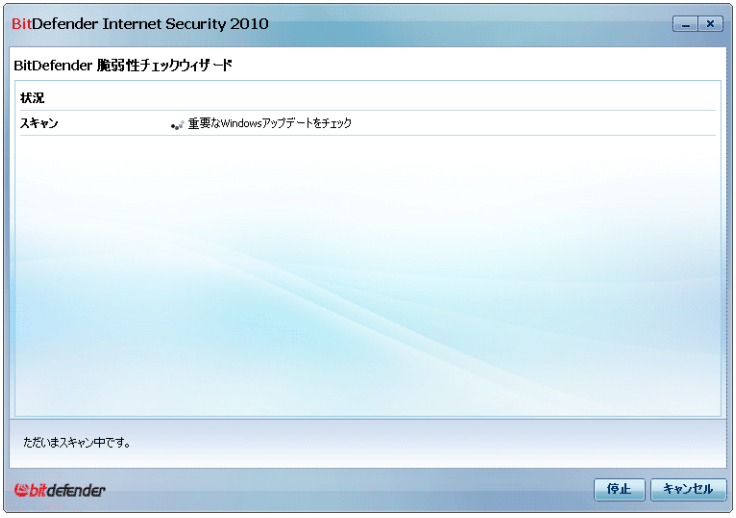
このウィザードはシステムの脆弱性をチェックして、それを修正する手助けをします。

### 11.3.1. 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。

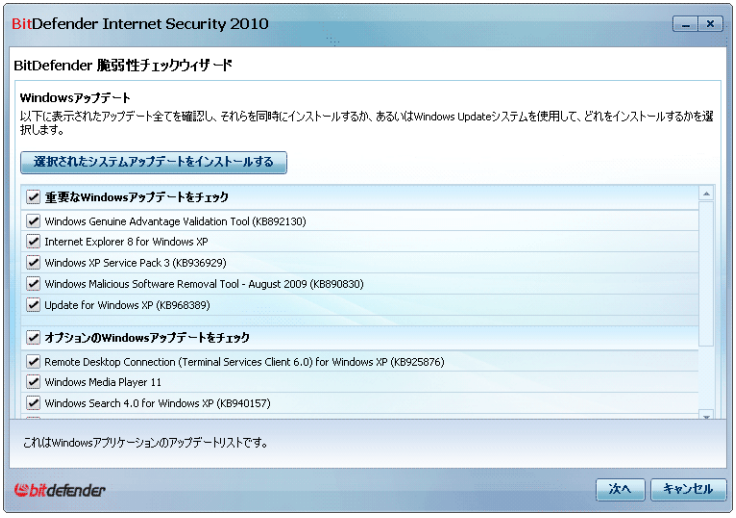
### 11.3.2. 手順 2/6 - 脆弱性チェック




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。

### 11.3.3. 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。

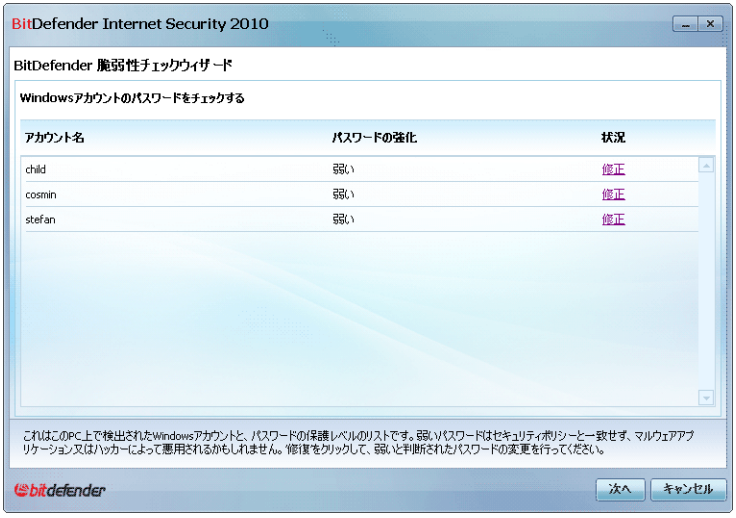
### 11.3.4. 手順 4/6 - アプリケーションのアップデート


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。

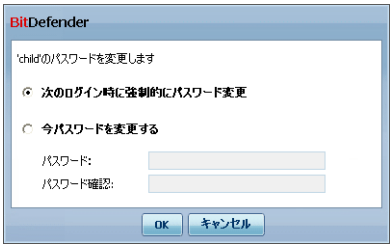
### 11.3.5. 手順5/6 - 弱いパスワードを変更




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にログインする際に、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。

### 11.3.6. 手順 6/6 - 結果を表示する


結果

閉じるをクリックします。

## 11.4. ファイル金庫ウィザード

ファイル金庫ウィザードは、BitDefenderファイル金庫の作成、管理の手助けをします。 ファイル金庫は、お使いのコンピュータ上で、重要なファイル、ドキュメント、全てのフォルダを安全に保管できる場所で、暗号化して保管します。

これらのウィザードは、問題を修正するときには表示されません。なぜならば、ファイル金庫はデータを保護する任意の方法だからです。次のBitDefenderの中級者モードの、ファイル金庫タブからのみ開始することができます。

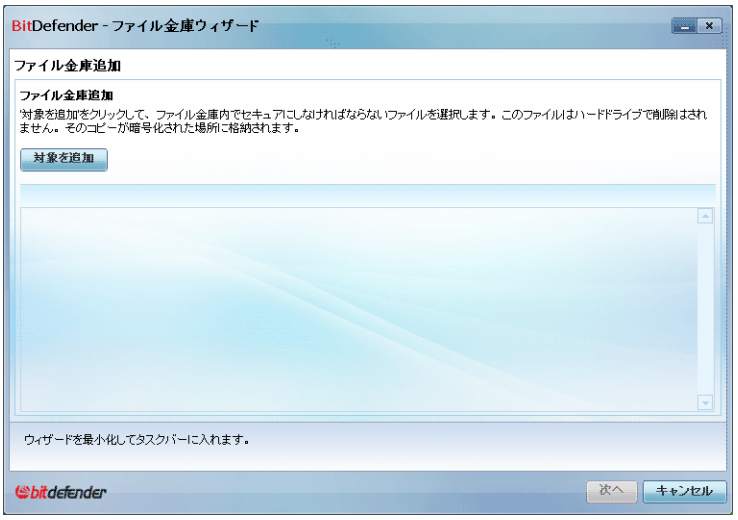
- ファイル金庫に追加 - ウィザードを開始して重要なファイル、ドキュメントを暗号化された特別の金庫ドライブに格納します。
- 金庫のファイルを除去 - ウィザードによってファイル金庫からデータを削除します。
- ファイル金庫表示 - ウィザードを開始して、ファイル金庫にある内容を表示します。
- ファイル金庫をロック - ウィザードを開始して、コンテンツを保護するためにオープンファイル金庫をロックします。

### 11.4.1. ファイルを金庫に追加

このウィザードは、ファイル金庫の作成やファイルの追加の手順を導いて、お使いのコンピュータにそれらを安全に保管する手助けをします。

#### 手順 1/6 - 対象を選択

ここでファイル金庫に追加したいファイル、フォルダを指定します。




対象

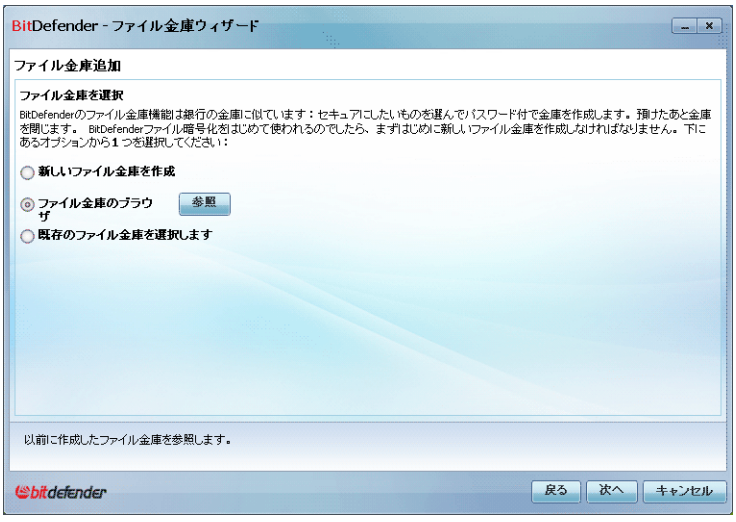
対象を追加をクリックして追加したいファイルやフォルダを選択し、OKをクリックします。 選択した場所がパス列に表示されます。 スキャンの対象を変更する場合には、削除ボタンをクリックします。

注意
１つあるいは複数の場所を選択できます。

次へをクリックします。

## 手順 2/6 - ファイル金庫を選択

新しい金庫の作成と既存の金庫の選択




ファイル金庫を選択

ファイル金庫を参照を選択して参照をクリック、ファイル金庫を選択します。もし選択した金庫がオープン（マウント中）であればここから手順５へ、ロック（アンマウント状態）であれば手順４に行きます。

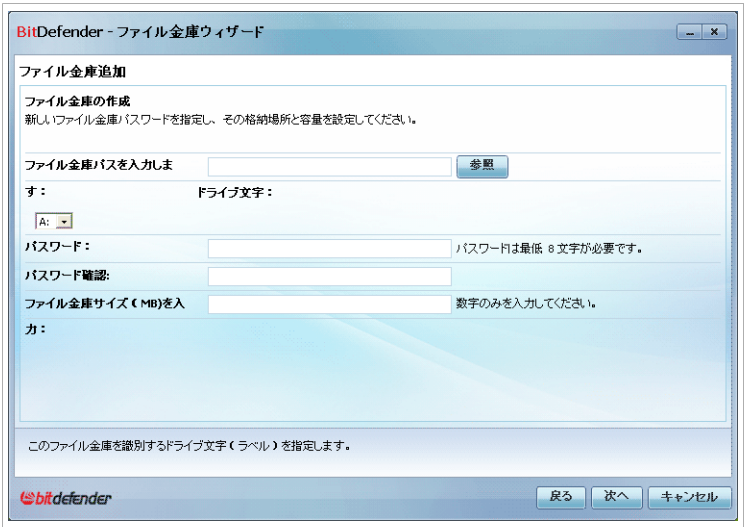
既存のファイル金庫を選択をクリックして金庫の名前をクリックします。もし選択した金庫がオープンして（マウント）いるなら手順５へ、ロックされて（アンマウント状態）なら手順４へ進みます。

もし目的に合う金庫がなければ新しくファイル金庫を作成を選択します。手順３にすすみます。

次へをクリックします。

## 手順 3/6 - ファイル金庫を作成

新しく作成するファイル金庫について情報を設定します。




ファイル金庫を作成

次の手順でファイル金庫の情報を入力します：

1. 参照をクリックしてbvdファイルの場所を選択します。

   **注意**
   ファイル金庫はコンピュータ上に作成される暗号化されたファイルでbvd拡張子をもっています。

2. 新しいファイル金庫のドライブ名をドロップダウンメニューから選択します。

   **注意**
   bvdファイルをマウントすると論理パーティション（新しいドライブ）が表示されます。

3. このファイル金庫のパスワードをフィールドに入力します。

   **注意**
   パスワードは半角で最低で８文字が必要です。

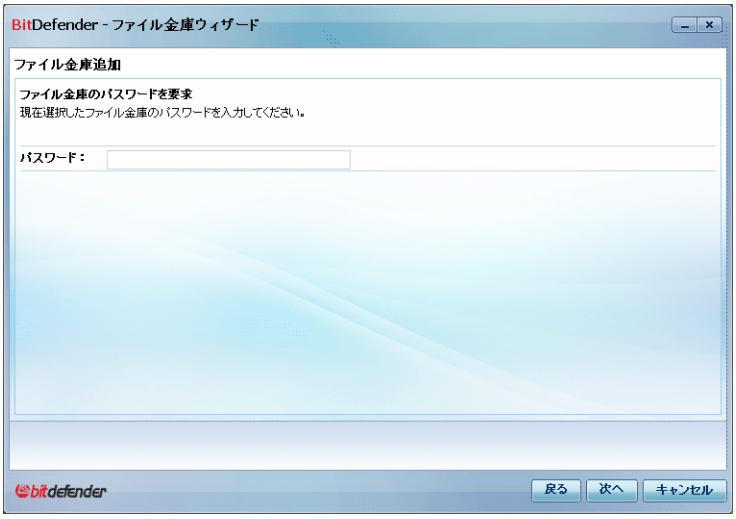
4. パスワードの再入力
5. ファイル金庫のサイズを（MBで）指定します。フィールドに数値を入力します。

次へをクリックします。

手順５に進みます。

## 手順 4/6 - パスワード

選択したファイル金庫のパスワード入力が求められます。

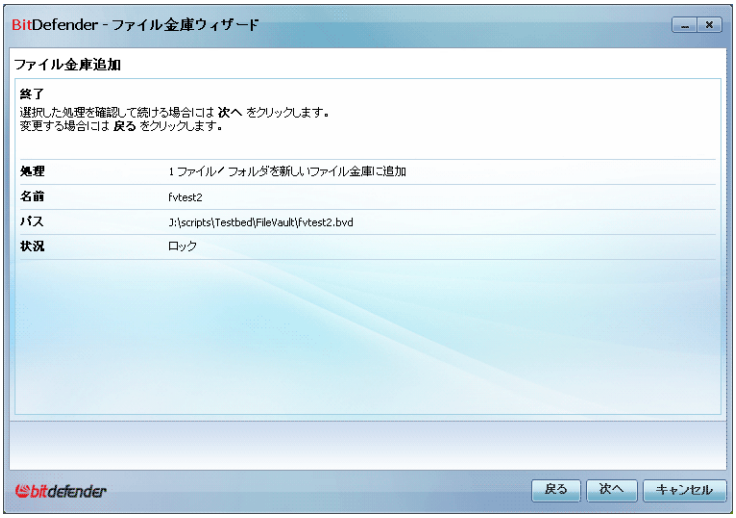



パスワードを入力

パスワードを入力して次へをクリックします。

## 手順 5/6 - まとめ

ここで選択した処理を確認できます。

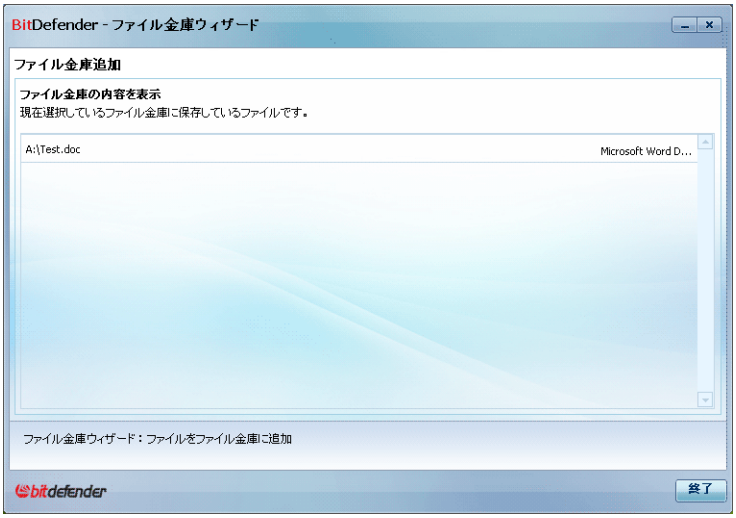



概要

次へをクリックします。

## 手順 6/6 - 結果を表示する

ファイル金庫の中をみることができます。




結果

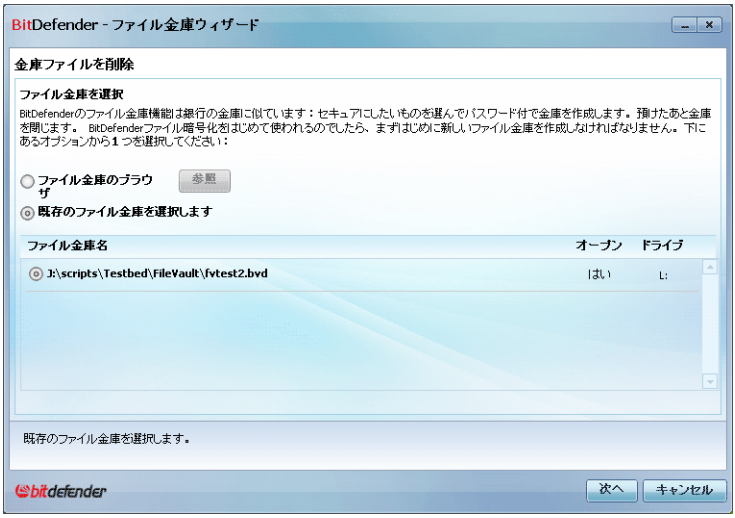
終了をクリックします。

### 11.4.2. 金庫ファイルを削除

このウィザードは、指定したファイル金庫からファイルを削除する手助けをします。

#### 手順 1/5 - 金庫を選択

ファイルを除去したい金庫を選択します。




ファイル金庫を選択

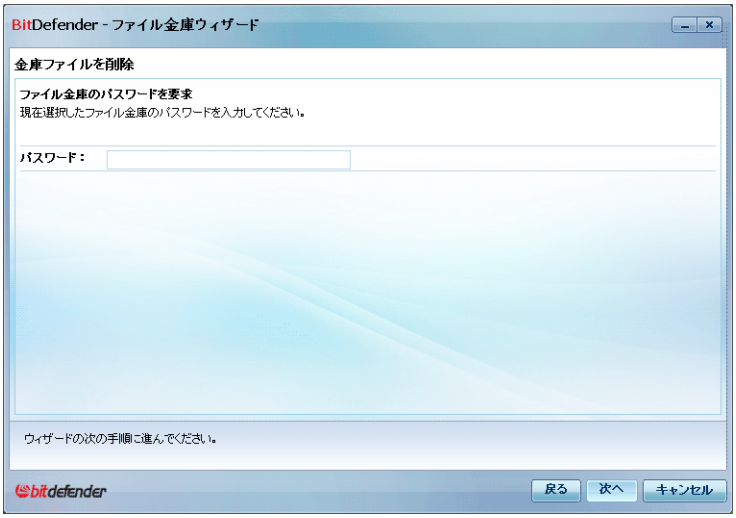
ファイル金庫を参照を選択して、参照をクリックしファイル金庫を選択します。もし選択した金庫がオープン（マウント中）であればここから手順３へ、ロック（アンマウント状態）であれば手順２に行きます。

既存のファイル金庫を選択をクリックし金庫の名前をクリックします。もし選択した金庫がオープンして（マウント）いるなら手順３へ、ロックされて（アンマウント状態）なら手順２へ進みます。

次へをクリックします。

### 手順 2/5 - パスワード

選択したファイル金庫のパスワード入力が求められます。

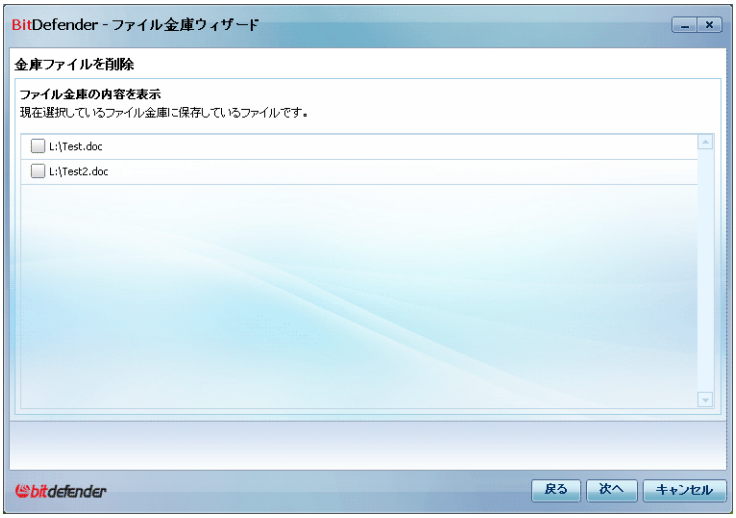



パスワードを入力

パスワードを入力して次へをクリックします。

### 手順 3/5 - ファイルを選択

さきほど選択した金庫のファイルリストが表示されます。

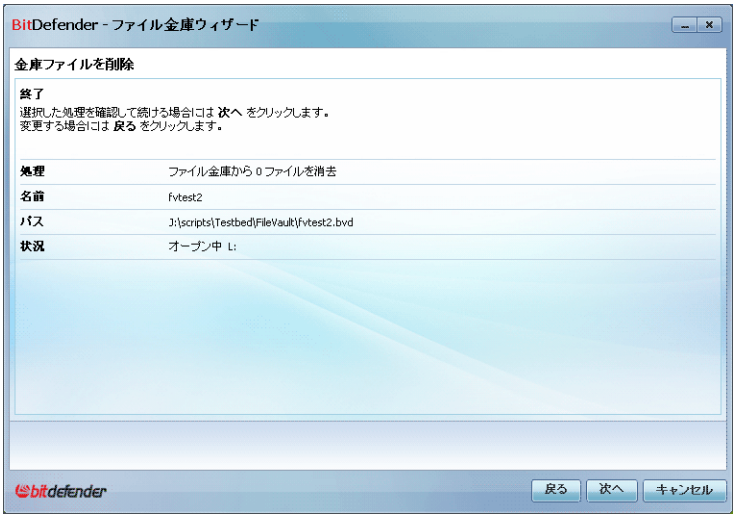



ファイルを選択

削除するファイルを選択して次へをクリックします。

### 手順 4/5 - まとめ

ここで選択した処理を確認できます。

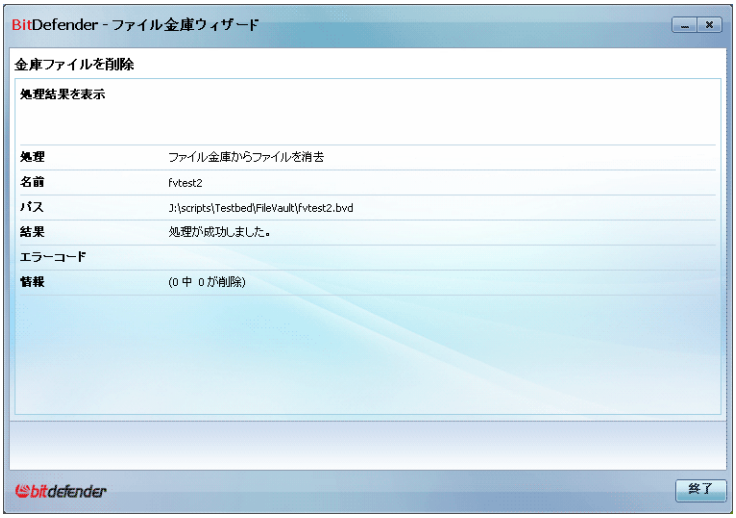



概要

次へをクリックします。

## 手順 5/5 - 結果を表示する

処理結果をみることができます。




結果

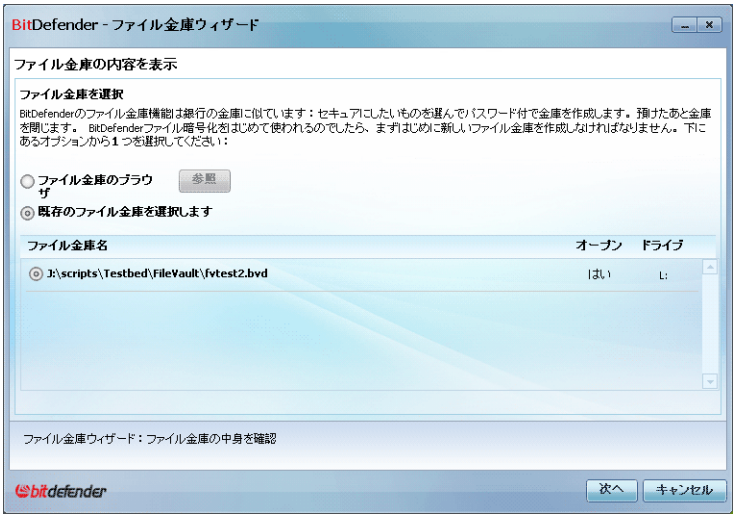
終了をクリックします。

### 11.4.3. ファイル金庫を表示

このウィザードは、指定したファイル金庫を開いて、そのファイルの内容を表示する手助けをします。

#### 手順 1/4 - ファイル金庫を選択

ファイルを確認したいファイル金庫を選択します。




ファイル金庫を選択

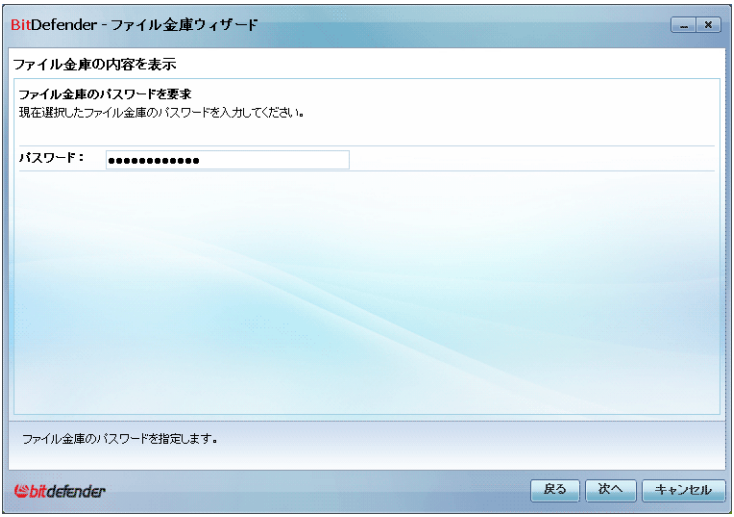
ファイル金庫を参照を選択して、参照をクリックしファイル金庫を選択します。もし選択した金庫がオープン（マウント中）であればここから手順３へ、ロック（アンマウント状態）であれば手順２に行きます。

既存のファイル金庫を選択をクリックし金庫の名前をクリックします。もし選択した金庫がオープンして（マウント）いるなら手順３へ、ロックされて（アンマウント状態）なら手順２へ進みます。

次へをクリックします。

### 手順 2/4- パスワード

選択したファイル金庫のパスワード入力が求められます。

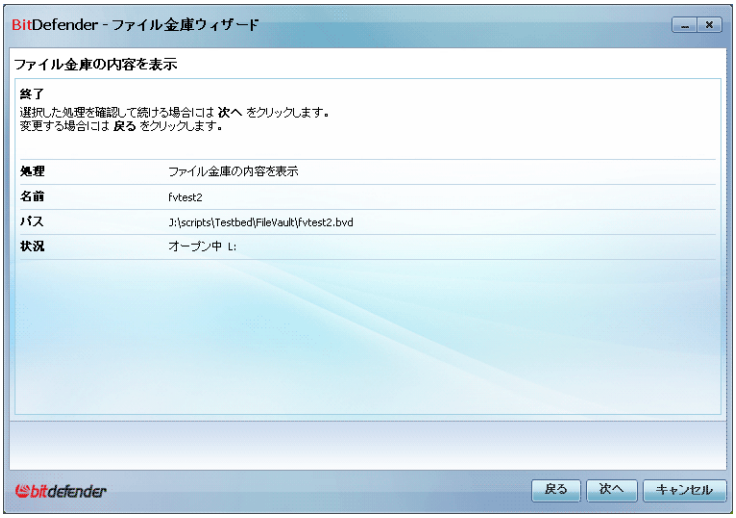



パスワードを入力

パスワードを入力して次へをクリックします。

### 手順 3/4 - まとめ

ここで選択した処理を確認できます。

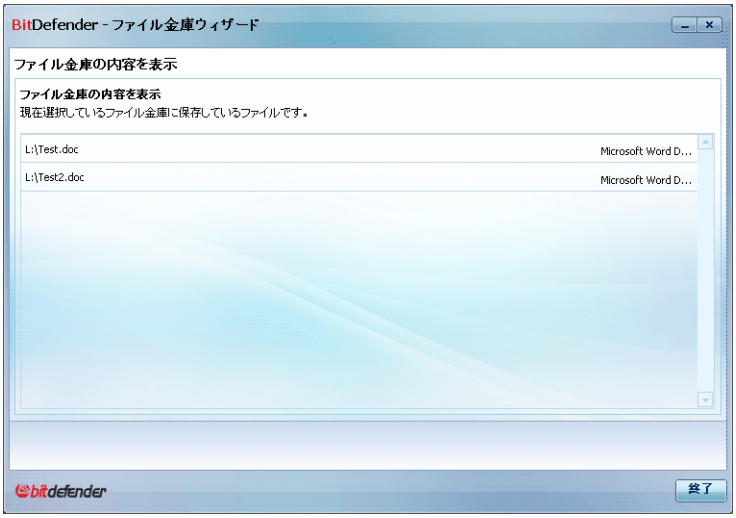



概要

次へをクリックします。

## 手順 4/4 - 結果を表示する

金庫にあるファイルをみることができます。




結果

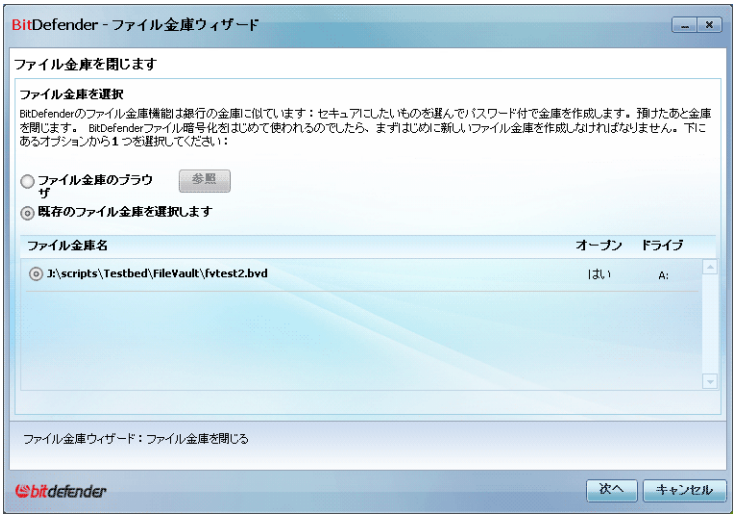
終了をクリックします。

### 11.4.4. ファイル金庫をロック

このウィザードは、指定したファイル金庫をロックして、その内容を保護する手助けをします。

#### 手順 1/3 - ファイル金庫を選択

ロックする金庫を指定します。




ファイル金庫を選択

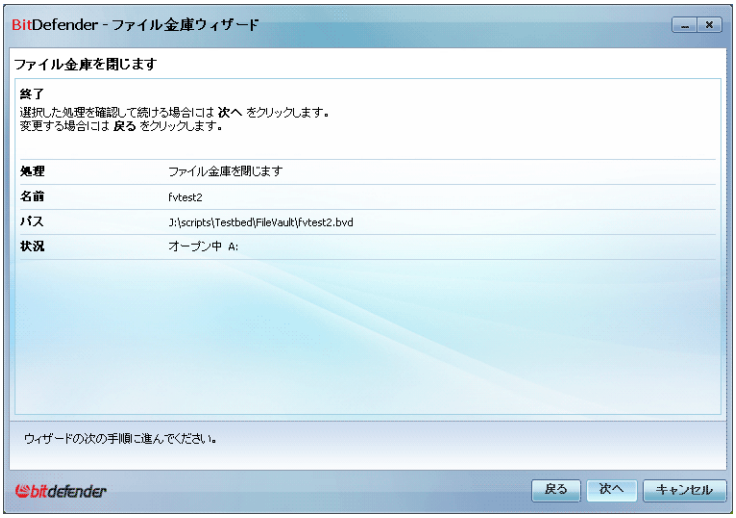
ファイル金庫を参照を選択して参照 をクリック、ファイル金庫を選択します。

既存のファイル金庫を選択をクリックして目的の金庫の名前をクリックします。

次へをクリックします。

### 手順 2/3 - まとめ

ここで選択した処理を確認できます。

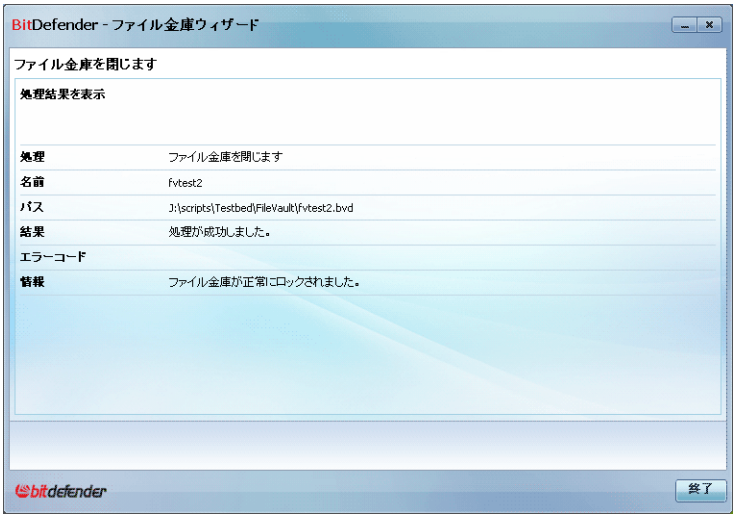



概要

次へをクリックします。

## 手順 3/3 - 結果を表示する

処理結果をみることができます。




結果

終了をクリックします。

# 中級者モード

# 12. ダッシュボード

ダッシュボードタブは、お使いのコンピュータのセキュリティステータスに関する情報を提供し、解決していない問題を修正することができます。


ダッシュボード

ダッシュボードは、次の章で構成されています：

- 全体の状態 - お使いのコンピュータに影響を与えている問題の数を表示して、その修復を手助けします。 未解決の問題がある場合は、感嘆符付きの赤い丸及び全ての問題を修復ボタンが表示されます。ボタンをクリックして、全ての問題を修復ウィザードを開始してください。
- ステータスの詳細 - 分かりやすい表現を使用して、それぞれの主なモジュールのステータスを、以下のいずれかのアイコンで示しています。

  チェックマーク付きの緑色の丸: セキュリティの状態に影響を与える問題はありません。 お使いのコンピュータ及びデータは保護されています。

  感嘆符付きの灰色の丸: モジュールのコンポーネントの処理が監視されていません。従って、セキュリティの状態に関して、有効な情報はありません。 このモジュールに関連する指定した問題があるかもしれません。

感嘆符付きの赤い丸: お使いのシステムのセキュリティに影響する問題があります。 重大な問題は直ぐにお客様の注意が必要になります。重大な問題でない場合でも、できる限り早く通知されるべきです。

この状況に関する詳細を確認するには、モジュール名をクリックして、コンポーネントの監視状況を設定します。

- 使用プロファイル – 現在選択された使用プロファイルを表示して、そのプロファイルに関連するタスクのリンクを提供します。
  - 標準プロファイルを選択すると、 今すぐスキャンボタンで、アンチウィルススキャンウィザードを使用して、システムスキャンを実行することができます。 アーカイブを除く、システム全体がスキャンされます。デフォルト設定では、ルートキット以外の全てのマルウェア形式をスキャンします。
  - ペアレントプロファイルを選択すると、ペアレンタルコントロール ボタンで、ペアレンタルコントロールを設定します。 ペアレンタルコントロールの設定方法について詳細は、「ペアレンタルコントロール」 (p. 191)を参照してください。
  - ゲーマープロファイルが選択されると、 ゲームモードをオン/オフに切り替えるボタンで ゲームモードを有効/無効に切り替えることができます。 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。
  - カスタムプロファイルが選択されると、 今すぐアップデート ボタンが、直ち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ィンドウが新たに開きます。

別のプロファイルに切り替える、または現在使用しているものを修正するには、プロファイルをクリックして、この設定ウィザードに従ってください。

# 13. セキュリティ

BitDefenderはBitDefenderを最新に保ちコンピュータをウィルスから守るためのセキュリティモジュールを備えています。 セキュリティモジュールに入るにはセキュリティタブをクリックします。


セキュリティ

セキュリティモジュールは次の２つのセクションで構成されます：

- ステータスエリア - 全ての監視されているセキュリティコンポーネントの現在の状況を表示して、どのコンポーネントを監視するかを選択することができます。
- クイックタスク - ここで最も重要なセキュリティタスクへのリンクを見つけることができます：今すぐアップデート、システムスキャン、マイドキュメントのスキャン、完全システムスキャン、カスタムスキャン、脆弱性スキャン

## 13.1. ステータスエリア

監視されたセキュリティコンポーネントの全てのリスト及び現在の状況を確認できるステータスエリアです。 それぞれのセキュリティモジュールを監視することで、BitDefenderは、お使いのコンピュータのセキュリティに影響する設定を行った時だけでなく、重要なタスクを実行し忘れた場合にもお知らせします。

コンポーネントの現在の状況は、分かりやすい表現及び以下のいずれかのアイコンを使用して表示されます：

チェックマーク付きの緑色の丸: コンポーネントに影響する問題はありません。
感嘆符付きの赤い丸: コンポーネントに影響する問題があります。

問題を表示している文章は、赤色で記載されています。 該当する表現の修正ボタンをクリックするだけで、報告された問題を修正します。 問題がその場で修正されない場合、ウィザードに沿って修正してください。

### 13.1.1. ステータスの追跡を設定

BitDefenderが監視するコンポーネントを選択するには、ステータスの追跡を設定をクリックして、追跡したい機能の警告を有効にする欄を選択してください。

**重要項目**

コンポーネントのセキュリティに影響する問題がある際に通知されたい場合は、コンポーネントの状況の追跡を有効にする必要があります。 お使いのシステムが完全に保護されるためには、全てのコンポーネントの追跡を有効にして、報告された全ての問題を修正します。

以下のセキュリティコンポーネンツのステータスは、BitDefenderによって追跡されます:

- アンチウィルス - BitDefender は、アンチウィルス機能の2つのコンポーネントの状態を監視します: リアルタイム保護とオンデマンドスキャン このコンポーネントに対して報告されている最も共通する問題が、以下の表に一覧になっています。

| 問題 | 解説 |
|---|---|
| リアルタイムプロテクションは無効です | ユーザ及びこのシステムで実行しているアプリケーションがアクセスするファイルをスキャンしません。 |
| マルウェアスキャンをこれまでに実行していません | オンデマンドシステムスキャンは、お使いのコンピュータに保管されているファイルに、マルウェアが存在していないかどうかの確認を行ったことはありません。 |
| 開始した最新のシステムスキャンは、完了前に中止されました | 完全システムスキャンが開始されましたが、完了していません。 |
| アンチウィルス機能は危険な状態です | リアルタイムプロテクションは無効で、システムスキャンの実行が延期されています。 |

- アップデート - BitDefender は、マルウェアシグネチャがアップデートされているかどうかを監視します。 このコンポーネントに対して報告されている最も共通する問題が、以下の表に一覧になっています。

| 問題 | 解説 |
|---|---|
| 自動アップデートが無効です | お使いのBitDefender製品のマルウェアシグネチャは、定期的に自動アップデートされていません。 |
| アップデートは x 日間実行されていません | お使いのBitDefender 製品のマルウェアシグネチャは期限切れです。 |

- ファイアーウォール - BitDefenderは、ファイアーウォール機能の状態を監視します。もしこれが有効でない場合は、この問題ファイアーウォールが無効ですが報告されます。
- アンチスパム - BitDefenderは、アンチスパム機能の状態を監視します。もしこれが有効でない場合は、この問題アンチスパムが無効ですが報告されます。
- アンチフィッシング - BitDefenderは、アンチフィッシング機能の状態を監視します。 サポートされている全てのアプリケーションが有効でない場合は、次の問題アンチフィッシングが無効ですが、報告されます。
- 脆弱性の確認 - BitDefenderは脆弱性チェック機能の追跡を行います。脆弱性チェックは、あらゆるWindowsのアップデート、アプリケーションのアップデートのインストールが必要な場合、又はパスワードの強化が必要な場合にお知らせします。

  このコンポーネントに対して報告されている最も共通する問題が、以下の表に一覧になっています。

| 状況 | 解説 |
|---|---|
| 脆弱性チェックが無効です | BitDefenderは、 実行されていないWindowsアップデートやアプリケーションアップデート、又は弱いパスワードに関する潜在的な脆弱性に対して、確認が行われていません。 |
| 複数の脆弱性が検出されました | BitDefenderは、実行されていないWindowsのアプリケーションのアップデート、及び弱いパスワードを検出しました。 |
| 重要なMicrosoftアップデート | 重要なMicrosoftのアップデートが有効ですが、インストールされていません。 |

| 状況 | 解説 |
| --- | --- |
| その他のMicrosoft アップデート | 重要ではないMicrosoftのアップデートが有効ですが、インストールされていません。 |
| Windows 自動アップデートが無効です | Windowsセキュリティアップデートは、それが有効になっても直ぐに自動的にインストールされません。 |
| アプリケーション（古い） | アプリケーションの新しいバージョンは有効ですが、インストールされていません。 |
| ユーザ（弱いパスワード） | ユーザパスワードは、特別なソフトウェアを持つ悪意のある人達によって、簡単に解読されてします。 |

## 13.2. クイックタスク

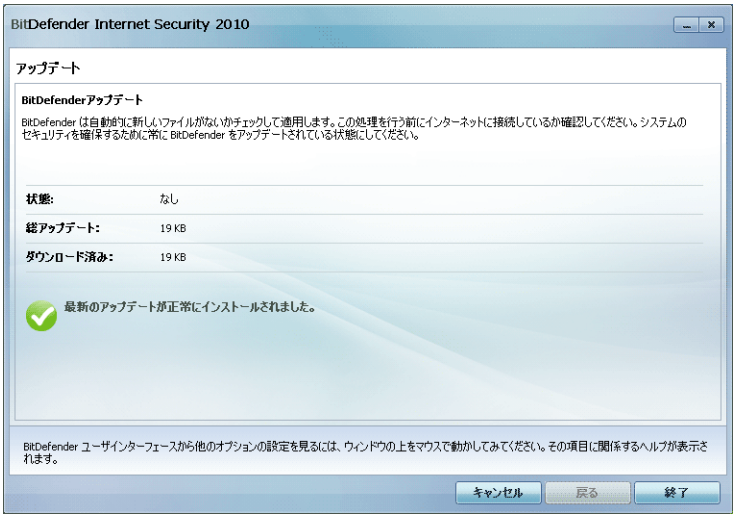
ここで最も重要なセキュリティタスクへのリンクを見つけることができます：

- アップデート - すぐにアップデートを開始します。
- システムスキャン - お使いのコンピュータの標準スキャンを開始します(アーカイブを含む)。追加のオンデマンドスキャンタスクは、この矢印の▾をクリックして、別のスキャンタスクを選択してください: "マイドキュメントをスキャン"又は"完全システムスキャン"
- カスタムスキャン - ウィザードを開始して、カスタムスキャンタスクを作成及び実行する
- 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導きます。

### 13.2.1. 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。

このウィ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。

### 13.2.2. 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、又はドロップダウンメニューから選択して、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 | 解説 |
|---|---|
| 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。 デフォルト設定では、 ルートキット以外の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 | 重要な現在の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。 |
| 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、ウィルス，スパイウェア，アドウェア，ルートキット 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。 |
| カスタムスキャン | ここでスキャンする特定のファイルあるいはフォルダを指定できます。 |

**注意**

完全システムスキャンと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。

システムスキャンを実行すると、完全システムスキャン、マイドキュメントのスキャン、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. 57）

カスタムスキャンを実行すると、カスタムスキャンウィザードが、スキャン手順を誘導します。 6つの手順に従って、特定したファイル又はフォルダのスキャンを行ってください。 このウィザードの詳細については次を参照してください。「カスタムスキャンウィザード」（p. 61）。

### 13.2.3. 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、次の6つの手順に従ってください。 詳細については、「脆弱性の解消」 (p. 247)を参照してください。

# 14. ペアレンタル

BitDefender Internet Security 2010 にはペアレンタルコントロールモジュールがあります ペアレンタルコントロールはお子様のインターネットへのアクセスや指定したアプリケーションの利用に、使用を制限することができます。 ペアレンタルコントロールの状況をチェックするには ペアレンタル タブをクリックしてください。


ペアレンタル

ペアレンタルモジュールは２つのセクションから構成されています。

- ステータスエリア - ペアレンタルコントロールが、このモジュール活動の追跡を有効/無効にしているかどうかの設定を確認することができます。
- クイックタスク - ここで最も重要なセキュリティタスクへのリンクを見つけることができます：システムスキャン、完全スキャン、いますぐアップデート

## 14.1. ステータスエリア

ペアレンタルコントロールモジュールの現在の状況は、分かりやすい表現及び以下のいずれかのアイコンを使用して表示されます：

チェックマーク付きの緑色の丸：コンポーネントに影響する問題はありません。
感嘆符付きの赤い丸：コンポーネントに影響する問題があります。

問題を表示している文章は、赤色で記載されています。 該当する表現の修正ボタンをクリックするだけで、報告された問題を修正します。 このモジュールに関して報告されている最も共通する問題は、ペアレンタルコントロールは設定されていませんです。

BitDefenderがペアレンタルコントロールモジュールを監視する場合は、追跡状況の設定をクリックして、このモジュールの警告を有効にする欄を選択してください。

## 14.2. クイックタスク

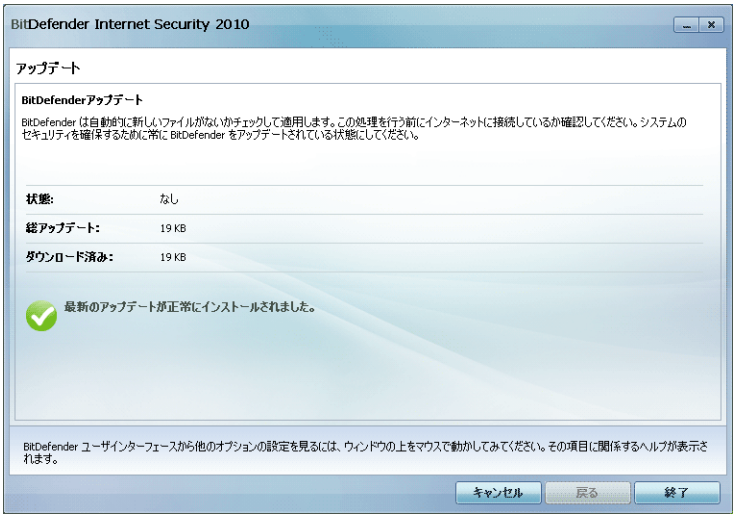
ここで最も重要なセキュリティタスクへのリンクを見つけることができます：

- アップデート - すぐにアップデートを開始します。
- 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。
- 完全システムスキャン - 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。

### 14.2.1. 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。

このウィ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。

### 14.2.2. 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 | 解説 |
|---|---|
| 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。 デフォルト設定では、 ルートキット以外の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、ウィルス，スパイウェア，アドウェア，ルートキット 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. 57)

# 15. ファイル金庫

BitDefenderはファイル金庫機能があります。これはデータを安全といったレベルにとどまらず、機密レベルで保護します。この目的を利用するためには、このファイル金庫を使用してください。

この機能で、ファイルをファイル金庫に保管して、保護することができます。

- ファイル金庫は安全な領域で個人情報や重要なファイルを保存するためのものです。
- このファイル金庫はbvd拡張子をもった暗号化されたファイルです。 いったん暗号化されると、その中にあるデータは盗難やセキュリティ違反にも強固になります。
- このbvdファイルをマウントすると、新しい論理パーティション（新しいドライブ）が表示されます。このしくみを理解するには、ISOイメージをVitualCDとしてマウントすることに近いと考えるとわかりやすくなるとおもいます。

  マイコンピュータを開くと、新しいドライブがファイル金庫として表示されています。この中でファイル操作（コピー、削除、変更など）ができます。ここにあるファイルは、このドライブの中にある限り守られています（それはマウント時にパスワードが必要だからです）。

  終了したらそのファイル金庫をロック（アンマウント）して内容の防御を開始します。

ファイル金庫モジュールにアクセスするには ファイル金庫 タブをクリックします。


ファイル金庫

ファイル金庫モジュールは２つのセクションから構成されています：

- ステータスエリア - 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。
- クイックタスク -ここで最も重要なセキュリティタスクへのリンクを見つけることができます：ファイル金庫の追加、表示、ロック、除去

## 15.1. ステータスエリア

コンポーネントの現在の状況は、分かりやすい表現及び以下のいずれかのアイコンを使用して表示されます：

チェックマーク付きの緑色の丸：コンポーネントに影響する問題はありません。
感嘆符付きの赤い丸：コンポーネントに影響する問題があります。

問題を表示している文章は、赤色で記載されています。 該当する表現の修正ボタンをクリックするだけで、報告された問題を修正します。 問題がその場で修正されない場合、ウィザードに沿って修正してください。

ファイル金庫タブ内のステータスエリアで、ファイル金庫モジュールの状態に関する情報を提供します。

BitDefenderがファイル金庫を監視する場合は、追跡状況の設定をクリックして、警告を有効にする欄を選択してください。

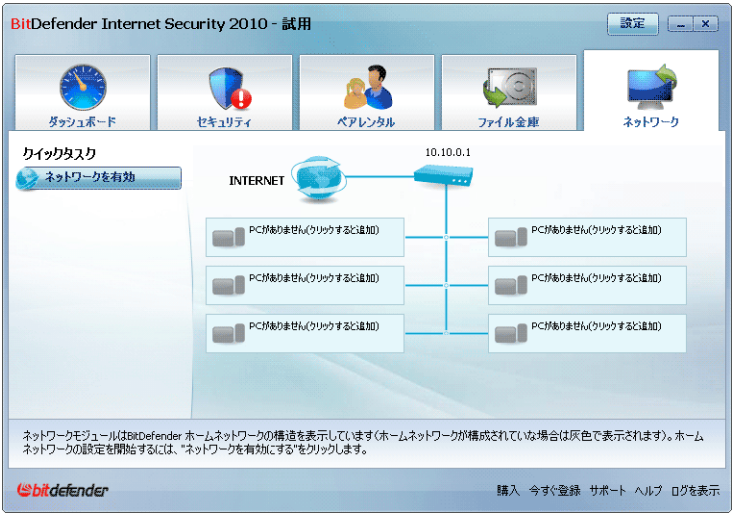
## 15.2. クイックタスク

以下のボタンを使用することができます：

- ファイル金庫に追加 - ウィザードを開始して重要なファイル、ドキュメントを暗号化された特別の金庫ドライブに格納します。 詳細については、次を参照してください。「ファイルを金庫に追加」 (p. 76).
- 金庫のファイルを除去 - ウィザードによってファイル金庫からデータを削除します。 詳細については、次を参照してください。「金庫ファイルを削除」 (p. 81).
- ファイル金庫表示 - ウィザードを開始して、ファイル金庫にある内容を表示します。 詳細については、次を参照してください。「ファイル金庫を表示」 (p. 86).
- ファイル金庫をロック -ウィザードを使用して、保管データの保護を開始するためにファイル金庫をロックします。 詳細については、次を参照してください。「ファイル金庫をロック」 (p. 90).

# 16. 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

## 16.1. クイックタスク

最初の状態では１つのボタンが使用できるだけです。

- ネットワークを有効にする - 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。

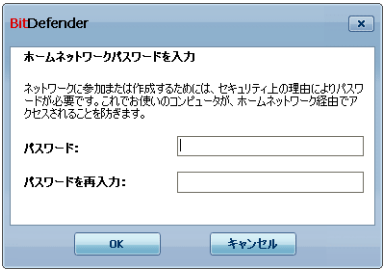
ネットワークに参加すると、さらにいくつかのボタンが表示されます。

- ネットワークを無効にする - 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。
- 全てのコンピューター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。

### 16.1.1. BitDefenderネットワークに参加する

BitDefender ホームネットワークに参加するには、以下の手順に従ってください：

1. ネットワークを有効に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。

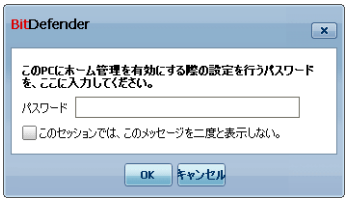
ネットワークマップ上にコンピュータ名が表示されます。

### 16.1.2. 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。

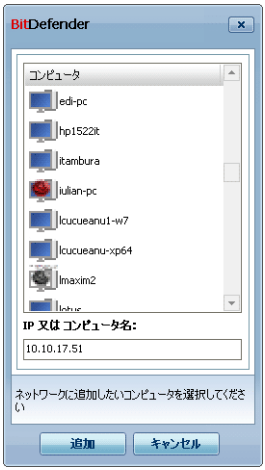
BitDefenderホームネットワークにコンピュータを追加するには、次の手順を行ってください：

1. コンピュータを追加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。



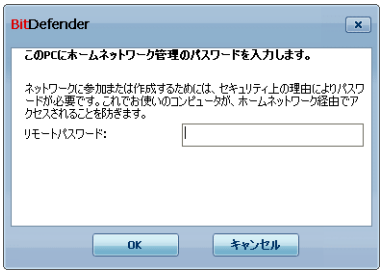

コンピュータを追加

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。

### 16.1.3. 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。

- ホームネットワークからPCを削除

  ネットワークからPCを削除できます。

- このコンピュータにBitDefenderを登録する

  ライセンスキーを入力して、このコンピュータにBitDefenderを登録することができます。

- リモートPCにパスワードを設定する

  パスワードを作成して、このPCでBitDefenderの設定に接続できないように設定します。

- オンデマンドスキャンタスクを実行

  リモートコンピュータでオンデマンドスキャンを実行することができます。以下のスキャンタスクを実行することができます：マイドキュメントのスキャン、システムスキャン、完全システムスキャン

●このPCの全ての問題点を修正

以下の全ての問題を修正ウィザードに従って、このコンピュータのセキュリティに影響を与えている問題を修正することができます。

●履歴/イベントを表示

このコンピュータにインストールされているBitDefender製品の、履歴&イベント機能にアクセスすることができます。

●今すぐアップデートする

このコンピュータにインストールされているBitDefender製品のアップデート処理を開始してください。

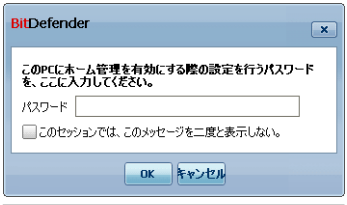
●ペアレンタルコントロールプロファイルの設定

このコンピュータのペアレンタルコントロールウェブフィルタで使用される年齢カテゴリを設定することができます：子ども、十代の若者、大人

●このネットワークをアップデートサーバに設定

このネットワーク内のコンピュータにインストールされている全てのBitDefender製品のアップデートサーバとして、このコンピュータを設定することができます。このオプションを使用するとインターネットトラフィックを削減します。なぜならば、ネットワーク内の1つのコンピュータだけがインターネットに接続して、アップデートのダウンロードを行うためです。

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。

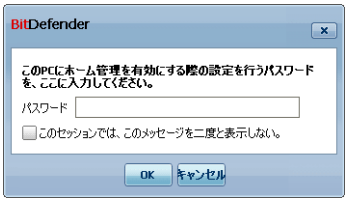
注意

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選択してください。　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。

### 16.1.4. 全てのコンピュータのスキャン

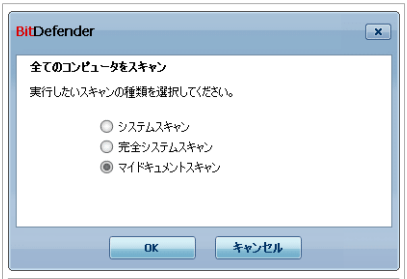
全ての管理しているコンピュータをスキャンするには、以下の手順を行います：

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
   - 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。
   - 完全システムスキャン - 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。



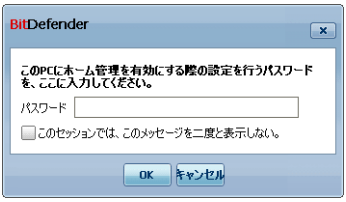

スキャンタイプを選択

3. OKをクリックします。

### 16.1.5. 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. 全てのコンピューターをアップデート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。



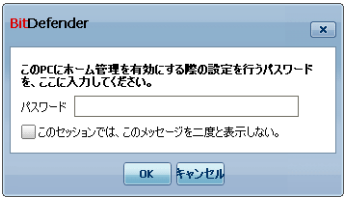

パスワードを入力

2. OKをクリックします。

### 16.1.6. 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. 同時にライセンス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。

# 上級者モード

# 17. 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。

## 17.1. ダッシュボード

お使いのコンピュータに影響を与える問題を確認する他に、製品処理の統計やお客様の登録状況を確認するには、上級者モード内の一般設定>ダッシュボードで行ってください。


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。

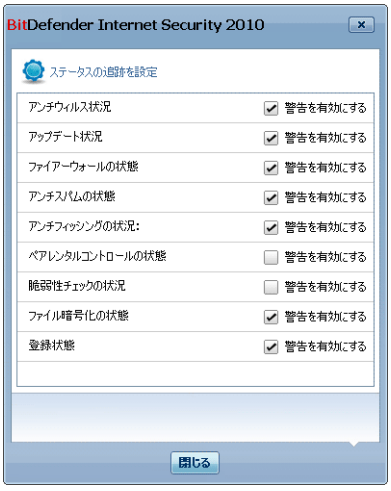
- 全体の状況 - お使いのコンピュータのセキュリティに影響を与える、あらゆる問題を通知します。
- 統計情報：BitDefenderの統計情報と重要な情報をみることができます
- 概要 - 更新状況やBitDefenderアカウント、ライセンスの状況を確認することができます。

- ファイル処理 – BitDefender アンチマルウェアによってスキャン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。
- ネットワーク処理 – BitDefenderファイアーウォールによって、フィルタされたネットワーク通信量を表示しています。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。

### 17.1.1. 全体の状態

ここで、お使いのコンピュータのセキュリティに影響を与えている問題の数を確認できます。　全ての脅威を削除するには、全ての問題を解決をクリックしてください。そうすると、全ての問題を解決ウィザードが開始します。

BitDefender Internet Security 2010で追跡するモジュールを設定するには、ステータスの追跡を設定をクリックします。 新しいウィンドウが表示されます：




ステータスの追跡を設定

BitDefenderにコンポーネントを監視させたい場合は、コンポーネントの 警告を有効にする欄を選択します。　以下のセキュリティコンポーネンツのステータスは、BitDefenderによって追跡されます：

- アンチウィルス – BitDefender は、アンチウィルス機能の2つのコンポーネントの状態を監視します：リアルタイム保護とオンデマンドスキャン このコンポーネントに対して報告されている最も共通する問題が、以下の表に一覧になっています。

| 問題 | 解説 |
| --- | --- |
| リアルタイムプロテクションは無効です | ユーザ及びこのシステムで実行しているアプリケーションがアクセスするファイルをスキャンしません。 |
| マルウェアスキャンをこれまでに実行していません | オンデマンドシステムスキャンは、お使いのコンピュータに保管されているファイルに、マルウェアが存在していないかどうかの確認を行ったことはありません。 |
| 開始した最新のシステムスキャンは、完了前に中止されました | 完全システムスキャンが開始されましたが、完了していません。 |
| アンチウィルス機能は危険な状態です | リアルタイムプロテクションは無効で、システムスキャンの実行が延期されています。 |

- アップデート - BitDefender は、マルウェアシグネチャがアップデートされているかどうかを監視します。 このコンポーネントに対して報告されている最も共通する問題が、以下の表に一覧になっています。

| 問題 | 解説 |
| --- | --- |
| 自動アップデートが無効です | お使いのBitDefender製品のマルウェアシグネチャは、定期的に自動アップデートされていません。 |
| アップデートは x 日間実行されていません | お使いのBitDefender 製品のマルウェアシグネチャは期限切れです。 |

- ファイアーウォール - BitDefenderは、ファイアーウォール機能の状態を監視します。もしこれが有効でない場合は、この問題ファイアーウォールが無効ですが報告されます。
- アンチスパム - BitDefenderは、アンチスパム機能の状態を監視します。もしこれが有効でない場合は、この問題アンチスパムが無効ですが報告されます。
- アンチフィッシング - BitDefenderは、アンチフィッシング機能の状態を監視します。 サポートされている全てのアプリケーションが有効でない場合は、次の問題アンチフィッシングが無効ですが、報告されます。
- ペアレンタルコントロール - BitDefenderはペアレンタルコントロール機能の状態を監視します。もしこれが有効でない場合は、この問題ペアレンタルコントロールが設定されていませんが報告されます。
- 脆弱性の確認 - BitDefenderは脆弱性チェック機能の追跡を行います。脆弱性チェックは、あらゆるWindowsのアップデート、アプリケーションのアップデート

のインストールが必要な場合、又はパスワードの強化が必要な場合にお知らせします。

このコンポーネントに対して報告されている最も共通する問題が、以下の表に一覧になっています。

| 状況 | 解説 |
| --- | --- |
| 脆弱性チェックが無効です | BitDefenderは、　実行されていないWindowsアップデートやアプリケーションアップデート、又は弱いパスワードに関する潜在的な脆弱性に対して、確認が行われていません。 |
| 複数の脆弱性が検出されました | BitDefenderは、実行されていないWindowsのアプリケーションのアップデート、及び弱いパスワードを検出しました。 |
| 重要なMicrosoftアップデート | 重要なMicrosoftのアップデートが有効ですが、インストールされていません。 |
| その他のMicrosoft アップデート | 重要ではないMicrosoftのアップデートが有効ですが、インストールされていません。 |
| Windows 自動アップデートが無効です | Windowsセキュリティアップデートは、それが有効になっても直ぐに自動的にインストールされません。 |
| アプリケーション（古い） | アプリケーションの新しいバージョンは有効ですが、インストールされていません。 |
| ユーザ（弱いパスワード） | ユーザパスワードは、特別なソフトウェアを持つ悪意のある人達によって、簡単に解読されてします。 |

- ファイル暗号化がファイル金庫の状態を監視します。もしこれが有効でない場合は、この問題 ファイル暗号化が無効ですが報告されます。

**重要項目**
お使いのシステムが完全に保護されるためには、全てのコンポーネントの追跡を有効にして、報告された全ての問題を修正します。

### 17.1.2. 統計データ

BitDefenderの動作状況を確認するときには、この統計情報を確認することをお勧めします。 次の内容が確認できます：

| 項目 | 解説 |
| --- | --- |
| 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 |
| 感染しているファイルを検出 | 前回のスキャンでシステムで検出されたウィルスに感染したファイルの数 |
| 最新のシステムスキャン | 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。 |

### 17.1.3. 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。

| 項目 | 解説 |
| --- | --- |
| 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かを表示します。 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。 |
| BitDefender account | 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。「登録とマイアカウント」 (p. 52). |
| 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 |

| 項目 | 解説 |
| --- | --- |
| | 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。 |

## 17.2. 設定

BitDefenderの一般設定、及びその管理は、上級者モードの一般設定>設定で行います。


全体設定

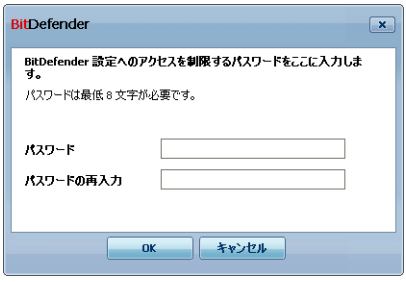
BitDefenderの全体的な動作をここで設定できます。デフォルトでは、BitDefenderはWindowsの起動時に読み込まれ、タスクバーに最小化された状態で実行されます。

### 17.2.1. 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。

ペアレンタルコントロールを設定するときだけパスワードを要求するには、ペアレンタルコントロールだけにパスワードを要求、適用を選択する必要があります。パスワードが元々ペアレンタルコントロールだけに設定されている場合は、このオプションのチェックを外すとBitDefenderの設定を変更する際そのパスワード入力が求められるようになります。

**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。

- ペアレンタルコントロールを有効にしているときにパスワードを設定するか確認する - ペアレンタルコントロールを構成するとき、またパスワードが設定されていなければパスワードを設定するかどうかを確認します。 パスワード設定することで、特定のユーザのために設定したペアレンタルコントロール設定を、管理者権限を持つ他のユーザが変更することができなくなります。
- BitDefender News（セキュリティ関連の通知）を表示 - BitDefenderサーバが送信するウィ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。 インターフェースが初級者モード、中級者モード、上級者モードに設定されていると、BitDefenderをポップアップ表示に設定できます。

- 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） - Windowsにログオンするたびに、スキャンアクティビティバーを表示します。 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、インターフェースが上級者モードの時だけに利用できます。

### 17.2.2. ウィルスレポート設定

- ウィルスレポートを送信 - コンピュータで見つかったウィルスに関するレポートを、BitDefender研究所へ送ります。ウィ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ィ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 - 可能性のあるウィ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ィルスと疑われるファイルだけが含まれ、新しいウィルスの特定にのみ使用されます。

## 17.3. 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、上級者モードの 一般情報>システム情報で行います。


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。 ファイルの関連付け設定のみ有効です！
- 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。

# 18. アンチウィルス

BitDefenderはあらゆる種類のマルウェア（ウィルス，トロイの木馬，スパイウェア，ルートキット等）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駆除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。

## 18.1. 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とBitDefenderアンチフィッシングを設定するには、上級者モードの アンチウィルス>シールドで行います。


シールド

リアルタイムプロテクションが有効/無効かを確認することができます。 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**
コンピュータをウィ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。

システムスキャンを開始するには、 今すぐスキャンをクリックしてください。

### 18.1.1. 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：

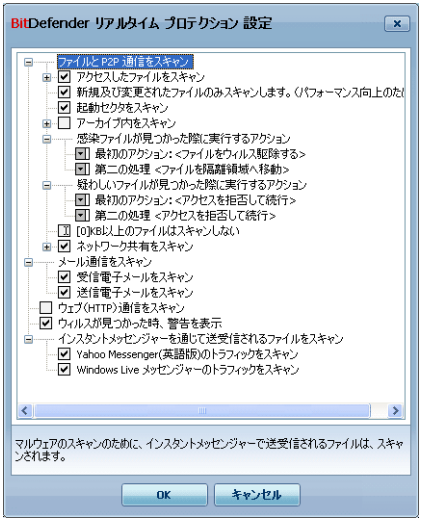
| 保護レベル | 解説 |
| --- | --- |
| 弱 | 基本的に必要なセキュリティはカバーします。リソース消費レベルはとても低いです。<br>ウィルスを対象に、プログラムおよび受信メールメッセージだけをスキャンします。従来のシグネチャ方式のスキャンに加え、ヒューリスティック分析も使用されます。感染ファイルに対するアクションは次の通りです： ファイルを感染除去/ファイルを隔離領域へ移動 |
| デフォルト | 標準的なセキュリティを提供します。リソース消費レベルは低いです。<br>すべてのファイルと受信&送信メールメッセージが、ウィルスおよびスパイウェアを対象にスキャンされます。従来のシグネチャ方式のスキャンに加え、ヒューリスティック分析も使用されます。感染ファイルに対するアクションは次の通りです：ファイルを感染除去/ファイルを隔離領域へ移動 |
| 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。<br>すべてのファイルと受信&送信メールメッセージ、ウェブ通信が、ウィルスおよびスパイウェアを対象にスキャンされます。従来のシグネチャ方式のスキャンに加え、ヒューリスティック分析も使用されます。感染ファイルに対する処理は次の通りです：ファイルを感染除去/ファイルを隔離領域へ移動 |

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。

### 18.1.2. 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。

- アクセスされるファイルとP2P通信のスキャンオプション - アクセスされる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 | | 解説 |
|---|---|---|
| アクセスされるファイルをスキャン | すべてのファイルをスキャン | ファイル形式に関わらず、アクセスされる全てのファイルがスキャンされます。 |
| | アプリケーションを対象にスキャン | 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; |

| オプション | | 解説 |
| --- | --- | --- |
| | | .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。<br>これらの種類のファイルのスキャンを行わない場合は、ダイアラとアプリケーションのスキャンをスキップ 及び/あるいは、 キーロガーのスキャンをスキップを選択します。 |
| 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。 |
| 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。<br>スキャンするアーカイブの最大サイズ、（キロバイトで、全てのアーカイブをスキャンしたい場合は0を入力してください）及びスキャンする最大アーカイブ多重度を設定することができます。 |

| オプション | | 解説 |
|---|---|---|
| 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、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。 |
| ネットワーク共有をスキャンしない | すべてのファイルをスキャン | ファイル形式に関わらず、ネットワークからアクセスする全てのファイルがスキャンされます。 |
| | アプリケーションを対象にスキャン | 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; |

| オプション | | 解説 |
| --- | --- | --- |
| | | .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。 |

- 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 | 解説 |
| --- | --- |
| 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。 |

- ウェブ(HTTP)通信をスキャン - http 通信をスキャンします。
- ウィ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ィ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ィルス名、そのパス、BitDefenderが実行したアクション、ウィ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。

### 18.1.3. アクティブウィルスコントロールを設定

BitDefenderアクティブウィルスコントロール(AVC) は、新しい脅威に対する防御壁で、またウィルス定義が提供さ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。

アプリケーションが悪意の可能性があるアクションを実行しようとすると、AVCが警告を行い、処理を実行する設定ができます。


BitDefender の AVC 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。

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。

このアプリケーションの処理を保存欄を選択すると、ユーザが選択をする前に、今後BitDefenderが選択されたアプリケーションに対して同じ処理を行います。 このように作成されたルールは、 除外の下にある表で一覧になっています。

アクティブウィルスコントロールの設定を行うには、BD AVC設定をクリックします。


BitDefender AVC の設定

該当するチェック欄を選択して、アクティブウィルスコントロールを有効にします。

**重要項目**
アクティブウィルスコントロールを有効にして、未知のウィルスを防いでください。

悪意の可能性がある処理を行ったアプリケーションがあれば、アクティブウィルスコントロールが警告を発し、処理を実行する場合は、処理を実行する前に確認する欄を選択してください。

## 保護レベルの設定

AVC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、AVC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、BitDefenderアクティブウィルスコントロールは、自動的に無効となる設定に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 | 解説 |
|---|---|
| 致命的 | 悪意のある処理に対して、全てのアプリケーションを厳しく監視します。 |
| デフォルト | ウィルス検出率が高く、偽陽性が疑われます。 |
| 中 | アプリケーションの監視は中位です。いくつか偽陽性が存在する可能性があります。 |
| 弱 | 検出率は低く、偽陽性はありません。 |

### 信頼できる/信頼できないアプリケーションのリストを管理

既知のアプリケーションを追加でき、信頼できるアプリケーションの一覧を信頼できます。これらのアプリケーションは、BitDefenderアクティブウィルスコントロールが、もはや確認を行わず、自動的にアクセスが許可されます。 同様に、常にアクセスを拒否したいアプリケーションは、信頼できないアプリケーションの一覧に追加でき、 BitDefenderアクティブウィルスコントロールは自動的にそれらをブロックします。

ルールを作成したアプリケーションは、 除外の下にある表で一覧になっています。アプリケーションのパス及び、それを設定した処理（許可又はブロック）は、各ルールに表示されます。

リストを管理するには、上の表にあるボタンを使用してください：

- 追加 - 新しいアプリケーションをリストに追加
- 削除 - リストからアプリケーションを削除
- 編集 - アプリケーションルールを編集

## 18.1.4. 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。

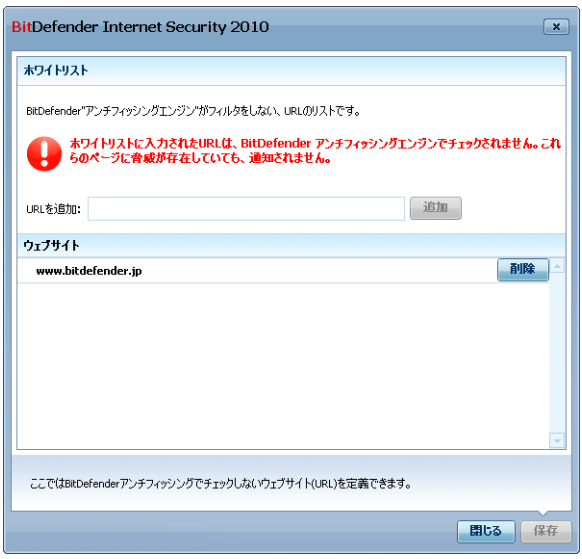
### 18.1.5. アンチフィッシング防御の設定

BitDefenderは、リアルタイム アンチフィッシング プロテクションを次の内容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 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、お客様が完全に信頼しているウェブサイトだけ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. 293)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。

保存 をクリックすると、変更を保存してウィンドウを閉じます。

## 18.2. ウィルススキャン

BitDefenderの主な目的はコンピュータをウィ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ィルスの侵入を防ぎ、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ィ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ィ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。またウィ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は、上級者モードのアンチウィルス>ウィルススキャンで行います。


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。

### 18.2.1. 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. 144)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 | 解説 |
| --- | --- |
| 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、ウィルス，スパイウェア，アドウェア，ルートキット 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。 |
| 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。デフォルト設定では、 ルートキット以外の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。 |
| 自動ログオンのスキャン | 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。<br>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。 現在の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今すぐ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。

### 18.2.2. 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直ち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、スキャン対象を確認することしかできませんので、このオプションはスキャン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。
- ログの表示 – 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。

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

注意
その他のタスクカテゴリの特殊性により、ここでは、ログの表示およびプロパティオプションのみが使用できます。

### 18.2.3. 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。

### 18.2.4. 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、タスクの左に表示されるProperties ボタンをクリックしてください(あるいはタスクの右をクリックし、 プロパティ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. 164)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 | 解説 |
|---|---|
| 弱 | 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。<br>プログラムは、ウィルスだけを対象にスキャンされます。従来のシグネチャ方式のスキャンに加え、ヒューリスティック分析も併用されます。 |
| デフォルト | 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。<br>すべてのファイルがウィ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。 |

| 保護レベル | 解説 |
| --- | --- |
| | すべてのファイルとアーカイブがウィ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：

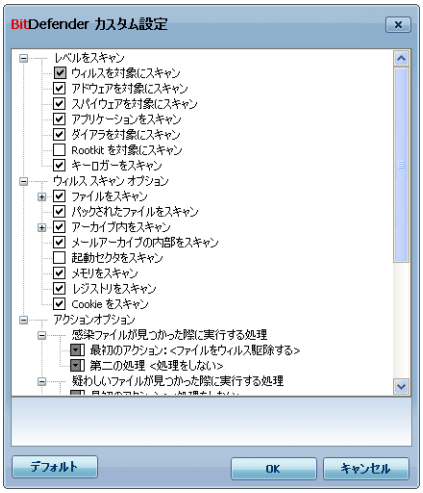
- タスクを低優先度で実行. スキャン処理の優先順位を下げます。他のプログラムはより高速で実行されますがスキャン処理終了までの時間が長くなります。
- スキャンウィザードを最小化してトレイに格納. スキャンウィンドウをシステムトレイにしまいます。BitDefenderアイコンをダブルクリックすると開きます。
- スキャンが完了し、なにも脅威が発見されない場合にはコンピュータをシャットダウンします。

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 | 解説 |
|---|---|
| ウィルスを対象にスキャン | 既知のウィルスを対象にスキャンします。<br>BitDefenderは不完全なウィ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。 |

| オプション | 解説 |
| --- | --- |
| 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。 |

- ウィルス 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 | | 解説 |
| --- | --- | --- |
| 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; 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。 |
| 圧縮ファイルをスキャン | | 圧縮されたファイルをスキャンします。 |
| アーカイブ内部をスキャン | | 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。 これらのファ |

| オプション | 解説 |
| --- | --- |
| | イル形式をスキャンしたい場合は、インストーラ及びchmアーカイブをスキャン欄を選択してください。<br>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。　スキャンするアーカイブの最大サイズを、次の欄にキロバイト(KB)のサイズを入力して設定できます。スキャンするアーカイブのサイズの制限. |
| 電子メールアーカイブ内部をスキャン | 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 | ウィ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.　このカテゴリのオプションを使用して、それぞれのカテゴリの検出ファイルで行われるアクションを指定します。

  **注意**

  新しいアクションを設定するには、この最初のアクションをクリックして、メニューから対象のオプションを選択してください。　二番目の処理を指定すると、最初の処理が失敗したときに実行されます。

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

    | アクション | 解説 |
    | --- | --- |
    | 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。 |
    | ファイルからウィルスを駆除 | 検出された感染ファイルからマルウェアコードを除去します。 |
    | ファイルを削除 | 警告なしで感染ファイルを即時に削除します。 |

| アクション | 解説 |
| --- | --- |
| 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 | 解説 |
| --- | --- |
| 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 | 解説 |
| --- | --- |
| 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 |

| アクション | 解説 |
| --- | --- |
| | 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な内容になるでしょう。 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。 パスワードで保護されたアーカイブは、お客様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 | 解説 |
| --- | --- |
| アクションなし | 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。 |
| ファイルからウィルスを駆除 | 検出された感染ファイルからマルウェアコードを除去します。 ウィルス感染駆除はいくつかのケースで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 |

| アクション | 解説 |
| --- | --- |
| | 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 | 解説 |
| --- | --- |
| アクションなし | 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 | 解説 |
| --- | --- |
| ログ専用 | 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。あるいは、既にタスクのプロパティ画面を開いている場合は、パス タブを選択してください。 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：

- フォルダを追加 - 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 - スキャンされるオブジェクトの一覧から、以前選択したファイル／フォルダを除去します。

  **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。 例えばシステムスキャンでは、次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

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、又は編集を行うには、タスクを右クリックして、スケジュールを選択してください。 既にタスクのプロパティ画面を開いている場合は、スケジューラタブを選択してください。 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（分，時間，日，週，月）で定期的にスキャンを起動します。

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

- 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。

### 18.2.5. 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、

自動ログオンスキャン 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：

- 今すぐスキャン - 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 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アクティビティバーへドラッグ&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。

### 今すぐスキャン

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「今すぐスキャン」と呼びます。

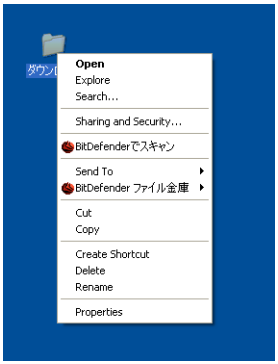
スキャンタスクを実行するには、以下の方法のいずれかを使用します：

- 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アクティビティバーへドラッグ&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 2010 → 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

フォルダを追加をクリックして、スキャンしたい場所を選択して、 OKをクリックします。 複数のフォルダをスキャンしたい場合は、それぞれ追加した場所に、この処理を繰り返してください。

選択した場所のパスが、スキャン対象に表示されます。 スキャンの対象を変更する場合には、削除ボタンをクリックします。 全てのパスを削除ボタンをクリックすると、リストに追加された全ての保存場所を削除します。

保存場所を選択すると、継続をクリックします。 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。 パスワードで保護されたアーカイブは、お客様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：

- パスワード.　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。
- パスワードを求めず、このオブジェクトのスキャンをスキップします。. 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。
- スキャンを行わないで、パスワード保護されている全ての項目をスキップします。.　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。

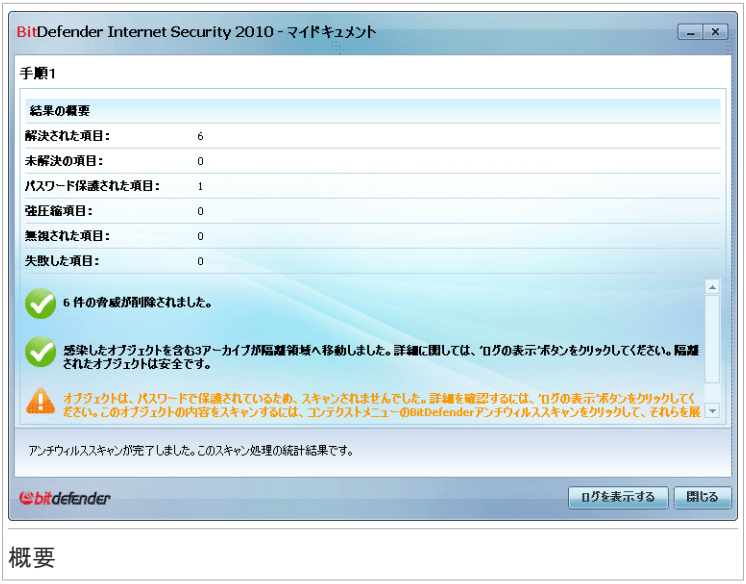
１つまたは複数のオプションがメニューで表示されます：

| アクション | 解説 |
|---|---|
| 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。 |
| ウィルスを駆除 | 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。<br>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。 スキャン処理に関して全ての情報をご覧になりたい場合には 、ログを表示 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駆除、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。

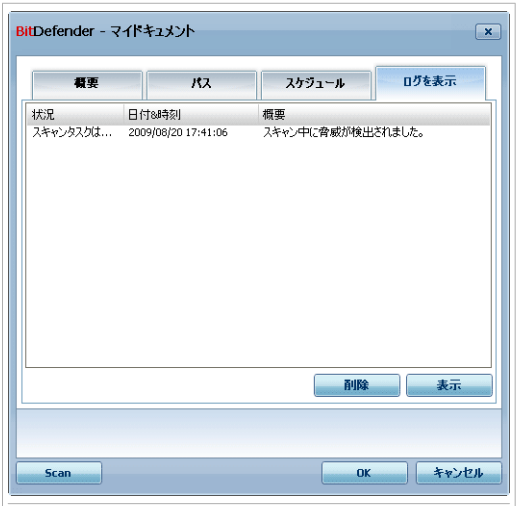
### BitDefenderは疑わしいファイルを検出しました

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。

### 18.2.6. 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：

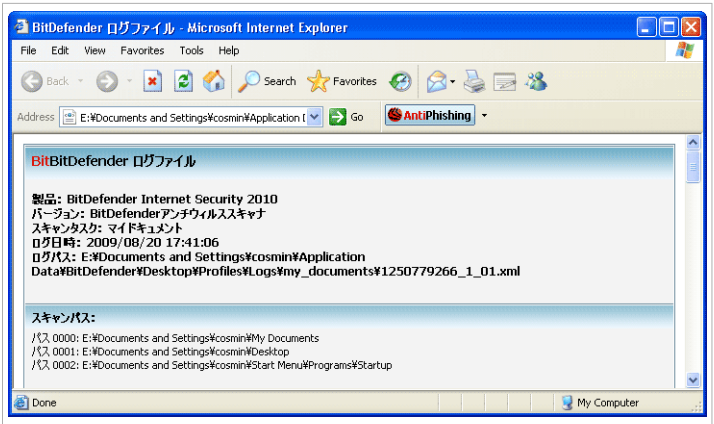
- 削除 – 選択したスキャンログを削除します。
- 表示 – 選択したスキャンログを表示します。 スキャンログがデフォルトのウェブブラウザで開きます。

**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。

## 18.3. 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。

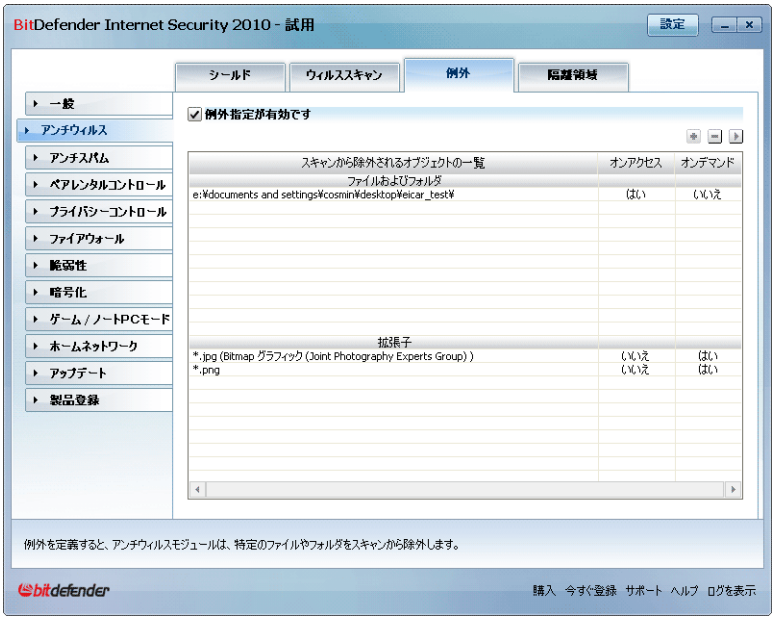
BitDefenderでは、オンアクセススキャンやオンデマンドスキャン、またはその両方でオブジェクトを例外とすることができます。この機能にはスキャンの時間を削減し、他の作業への影響を回避する狙いがあります。

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、上級者モードでアンチウィルス>例外で行います。




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

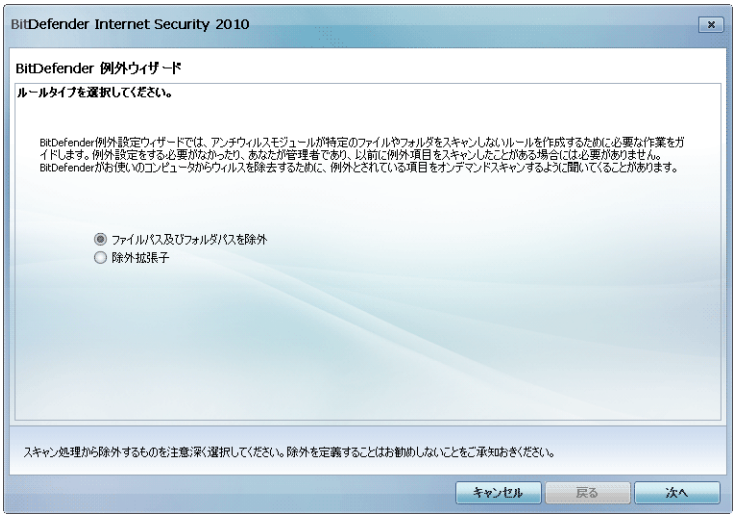
オブジェクトを右クリックし、ショートカットメニューのオプションを使用して編集や削除を行うこともできます。

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。

### 18.3.1. 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

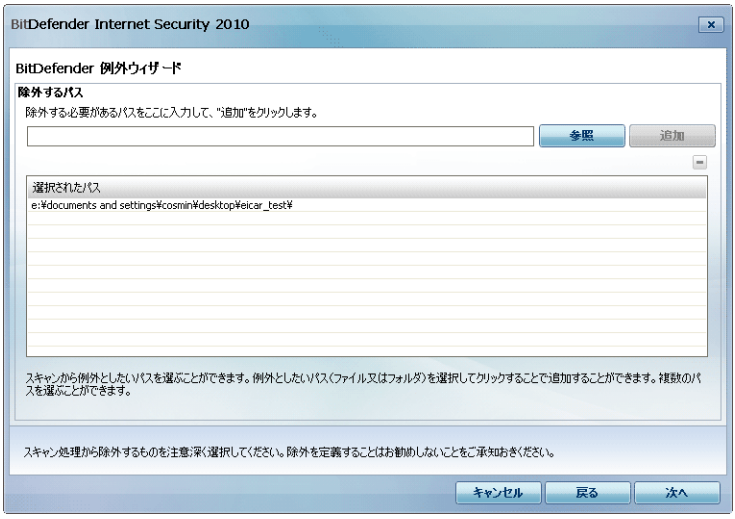



オブジェクト形式

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

スキャンを除外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、スキャンを除外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。
- スキャンから除外したいパスを編集欄に入力して、追加をクリックします。

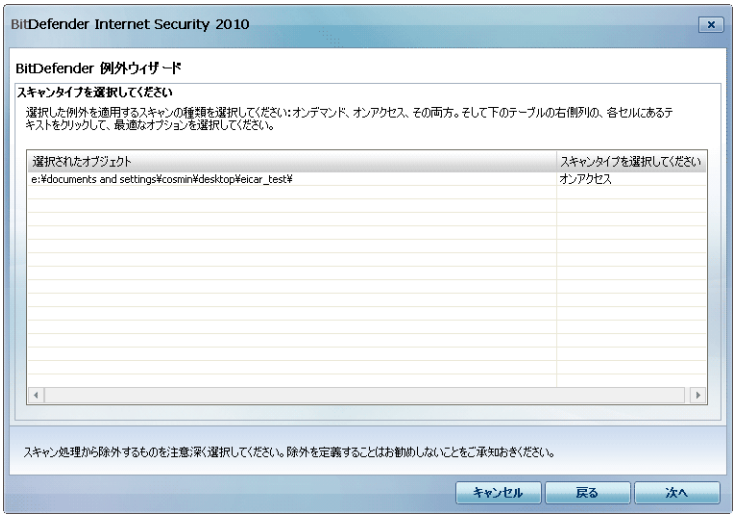
**注意**
指定したパスが存在しない場合はエラーメッセージが表示されます。OKをクリックしてパスが正しいか確認してください。

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



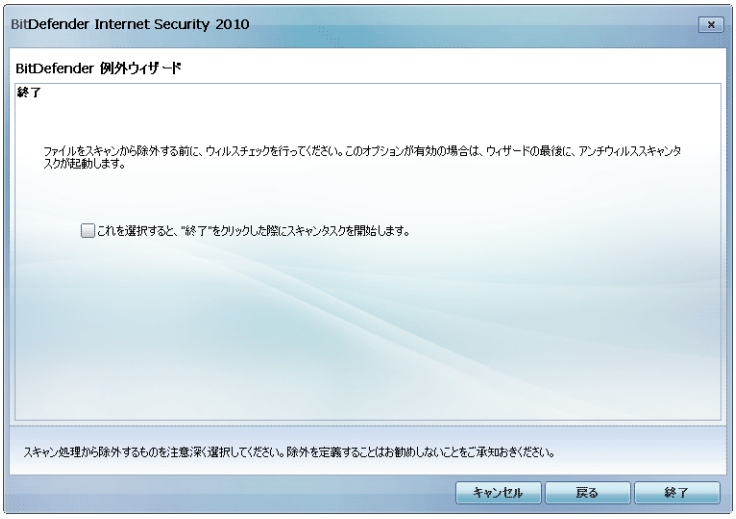

スキャン方式

スキャンを除外するパスと、除外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除外されます。除外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 - 除外したファイルをスキャン




除外したファイルをスキャン

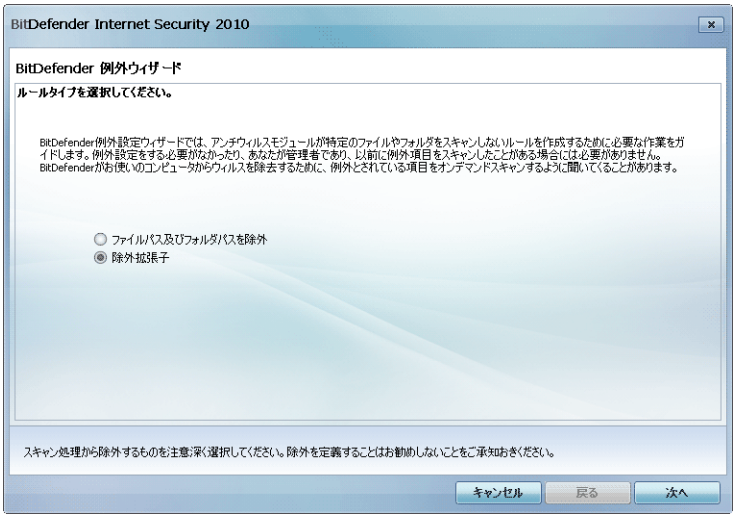
指定したパスにあるファイルをスキャンして感染していないことを確認することを強くお勧めいたします。 チェックボックスを選択してスキャン対象から例外にする前にスキャンします。

終了をクリックします。

## 18.3.2. スキャンから拡張子を除外

スキャンから拡張子を除外するには、 追加ボタンをクリックしてください。 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除外できます。

## 手順 1/4 - オブジェクト形式を選択

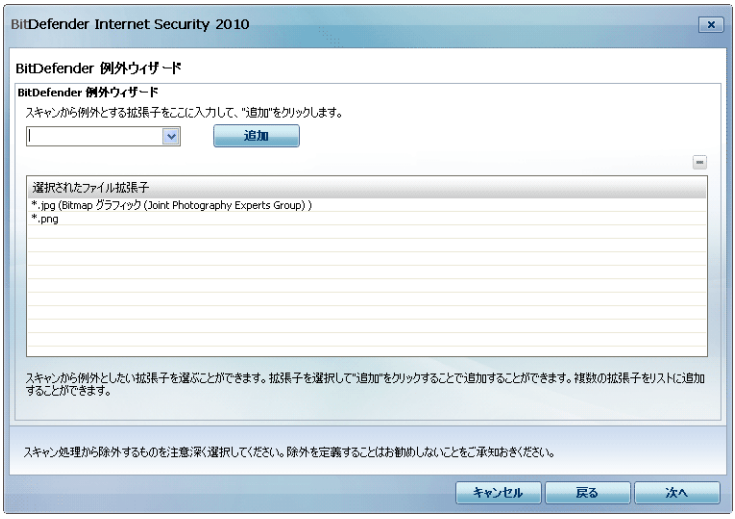



オブジェクト形式

スキャンから拡張子を除外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 - 除外する拡張子を指定




例外にする拡張子

スキャンから除外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。

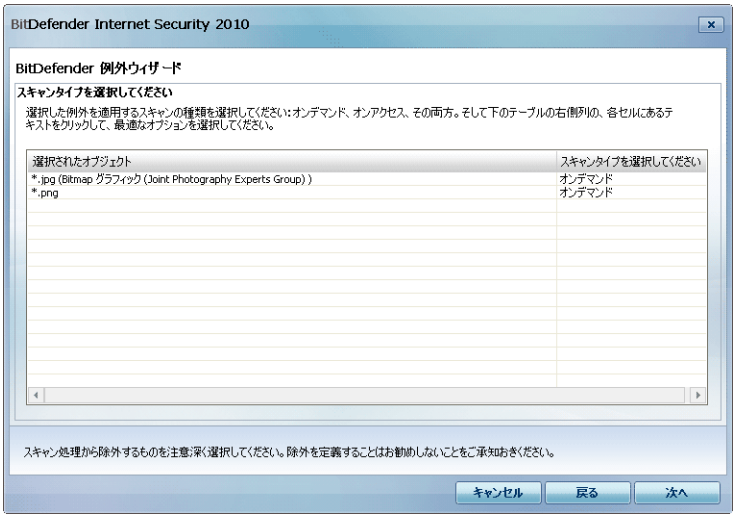
●スキャンから例外にしたい拡張子を編集欄に入力して追加をクリックします。

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



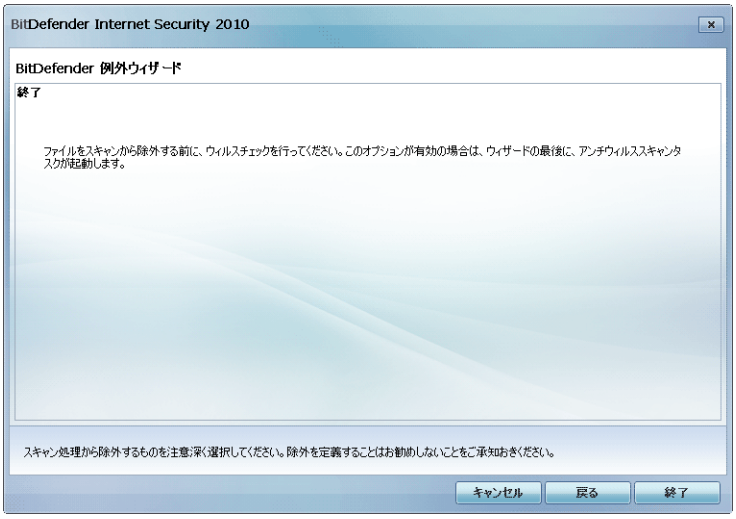

スキャン方式

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。

## 18.4. 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、上級者モードのアンチウィルス>隔離領域で行います。


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，検出されたウィルス名，元の場所へのパス，検出日が表示されます。

**注意**
隔離領域にあるウィ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、ウィルスが被害を及ぼすことはありません。

### 18.4.1. 隔離されたファイルを管理

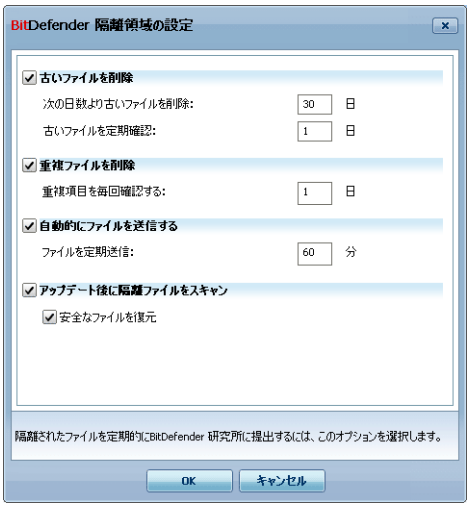
送信をクリックして隔離領域で選択したファイルをBitDefender研究所へ送ることができます。 デフォルトではBitDefenderは隔離ファイルを60分毎に自動的に送信します。

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

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。

### 18.4.2. 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。

# 19. アンチスパム

BitDefender アンチスパムは、非常に優れた革新的技術と業界標準のアンチスパムフィルタを採用しており、受信ボックスに到達する前に迷惑メールを除去します。

## 19.1. アンチスパムの知識

迷惑メール（スパム）は、個人と組織の両方にとって、日々増大する頭痛の種です。決して子どもに見せたいと思うような品のいい内容ではなく、さらに時間が無駄になり、職場のメール内にポルノを受信したことを理由に首になるかもしれません。しかも、送信する相手を止める手段はないのです。次善の策は、当然ですが、受け取らないことです。残念ながら、迷惑メールは色々な形式とサイズで届き、その種類は多岐に渡ります。

### 19.1.1. アンチスパムフィルタ

BitDefender アンチスパムエンジンは、受信ボックスから迷惑メールを一掃するためにいくつかの異なるフィルタを搭載しています： 友達一覧, スパマーリスト, Charset フィルタ, イメージフィルタ, URL フィルタ, NeuNet（ヒューリスティック）フィルタ, ベイジアンフィルタ

注意
アンチスパムモジュールの設定の項で、これらのフィルタを個別に有効/無効にできます。

#### 友人リスト（ホワイトリスト）/迷惑メール送信者一覧（ブラックリスト）

ほとんどの人は、ある種のグループの人たちと定期的に通信を行い、同じドメイン内の企業や組織からもメッセージを受け取ります。友人あるいはスパマーリストを使用することで、その内容に関わらず、メールを受け取る人（友人）と、二度と受け取らない人（迷惑メール送信者）とを簡単に区別することができます。

友人 / 迷惑メール送信者一覧は、上級者モードインターフェース、あるいはよく使われているメールクライアントに統合されたアンチスパムツールバーからから管理できます。

注意
友人の名前およびメールアドレスを友人リストに追加することをお勧めします。BitDefenderはそのリストに記載された送信者からのメッセージはブロックしません；従って、友人を追加すると信頼できるメッセージの届く精度が向上します。

### 文字コードフィルタ

多くの迷惑メールメッセージは、Cyrillic（キリル）およびAsian（アジア）キャラクタセット（文字セット）で書かれています。文字コードフィルタは、こうしたメッセージを検出し、迷惑メールと判断します。

### イメージフィルタ

ヒューリスティックフィルタの検出をすり抜けるのが困難なため、最近では不要な内容の画像だけしか持たないメッセージが受信ボックスに多く届くようになっています。これに対処するためBitDefenderはメール画像のシグネチャをBitDefenderのデータベースと比較するイメージフィルタを導入しました。合致した場合はSPAMタグを付加します。

### URLフィルタ

ほとんどの迷惑メールメッセージは、様々な場所へのリンクを含んでいます。リンク先の多くは、さらなる広告や商品を売りつけるページで、場合によってはフィッシングにも利用されます。

BitDefenderはこうしたリンクのデータベースを管理しています。 URLフィルタは、メッセージ内のすべてのURLリンクをそのデータベースと比較します。合致する場合、メッセージにSPAMタグを付加します。

### NeuNet（ヒューリスティック）フィルタ

NeuNet（ヒューリスティック）フィルタは、すべてのメッセージコンポーネント（ヘッダだけでなくHTMLあるいはテキスト形式の本文も）に一連のテストを行い、単語、文章、リンクなどの迷惑メールの特徴を探します。　分析結果を基に、メッセージにSPAMスコアを付加します。

フィルタは、件名にSEXUALLY-EXPLICIT:と記されたメッセージを検出しSPAMタグを付加します。

**注意**

2004年５月19日から、性的な内容の迷惑メールには、件名にSEXUALLY-EXPLICIT:と記載しなければならず、記載していない場合は連邦法違反となり、罰金が科せられることになりました。

### ベイジアンフィルタ

ベイジアンフィルタモジュールは、（ユーザまたはヒューリスティックフィルタにより）迷惑メールでないと判断されたメッセージと比較して、迷惑メールと分類されたメッセージに含まれる特定の単語をレーティングした統計情報を基にメッセージを分類します。

例えば迷惑メールに特定の４文字の単語が多く現れる傾向にあれば、その単語を含む次の受信メールが迷惑メールである可能性が高まることになります。メッセージのすべての関連する単語が対象になります。統計情報を総合することでメッセージ全体が迷惑メールである可能性がはじき出されます。

このモジュールには、もう１つ興味深い特徴があります：　学習可能であることです。特定のユーザが受信したメッセージの形式に素早く適応し、すべての情報を保存します。効率よく動作させるには、フィルタを訓練しなければなりません。つまり、警察犬ににおいを追わせるように、迷惑メールと通常メールのサンプルを教えるのです。場合によっては、フィルタには修正も必要です－間違った判定を行ったら調整を加えるのです。

**重要項目**

ベイジアンフィルタを修正するには、迷惑メール 及び 非迷惑メールボタンをクリックします。それは、このアンチスパムツールバーにあります。

## 19.1.2. アンチスパム操作

BitDefenderアンチスパムエンジンは、各種アンチスパムフィルタを全て使用して、メールが受信箱に入ってよいかそうでないかを判定します。

**重要項目**

BitDefenderにスパムメッセージを検知すると件名の先頭に[SPAM]　を付けます。BitDefenderは自動的にスパムメッセージを特定のフォルダに移動します：

- Microsoft Outlookではスパムメッセージは 迷惑メール フォルダに移動します。そのフォルダは 削除済み項目 フォルダにあります。 The スパム フォルダはBitDefenderのインストール時に作成されます。
- Outlook Express と Windows Mailではスパムメッセージは直接削除済み項目に移動されます。
- Thunderbirdではスパムメッセージは スパム フォルダに移動されます。そのフォルダは ごみ箱 フォルダにあります。 The スパム フォルダはBitDefenderのインストール時に作成されます。

他のメールクライアントを使用している場合には、ルールを作成してメールメッセージにBitDefenderが[SPAM] とつけられたものを適当な隔離フォルダに移動するようにしなければなりません。

インターネットから届くメールは、まずホワイトリスト/ブラックリストフィルタでチェックされます。その送信元のアドレスがホワイトリストにある場合、メールは受信ボックスへそのまま移動されます。

それ以外の場合は、ブラックリストフィルタがメールを引き継ぎ、送信元のアドレスがその一覧にあるか確認します。合致すると、メールにSPAMタグが付加され、（Microsoft Outlook内の）迷惑メールフォルダに移動されます。

それ以外の場合、文字コードフィルタがメールがCyrillic（キリル）あるいはAsian（アジア）言語で書かれていないか確認します。該当すれば、メールに”迷惑メール”タグが付加され、迷惑メールフォルダへ移動されます。

メールがAsianあるいはCyrillicで書かれていなければ、イメージフィルタへ渡されます。イメージフィルタは、迷惑メールに該当するイメージが添付されたすべてのメールメッセージを検出します。

URLフィルタは、リンクを探し、見つかったリンクをBitDefenderのデータベースと比較します。合致するとメールにSPAMスコアを追加します。

NeuNet（ヒューリスティック）フィルタがメールを引き継ぎ、すべてのメッセージ内容に対し一連のテストを行って、単語、文章、リンクその他の迷惑メールの特徴を探します。結果に応じて、メールに迷惑メールのスコアを追加します。

注意
メールの件名にアダルトコンテンツと記されていると、BitDefenderは迷惑メールと判断します。

ベイジアンフィルタモジュールは、（ユーザまたはヒューリスッティックフィルタにより）迷惑メールでないと判定されたメッセージと迷惑メールに分類されたメッセージとを比較して、含まれる特定の単語のレートに関する統計情報でさらにメッセージを分析します。メールには、迷惑メールスコアが追加されます。

集計されたスコア（URLスコア + ヒューリスティックスコア + ベイジアンスコア）が（状態の項でしきい値レベルとしてユーザが指定した）メッセージの迷惑メールスコアを超えた場合、メッセージは迷惑メールと判定されます。

### 19.1.3. アンチスパムアップデート

アップデートを実行すると：

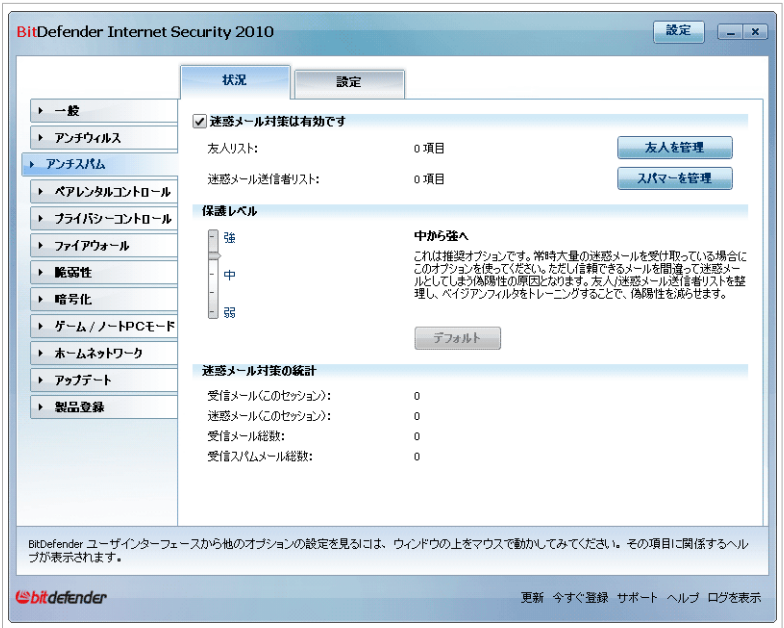
- 新しいイメージシグネチャがイメージフィルタに追加されます。
- 新しいリンクがURLフィルタに追加されます。
- 新しいルールがNeuNet（ヒューリスティック）フィルタに追加されます。

これによりアンチスパムエンジンの精度が向上します。

スパマーからユーザを守るためにBitDefenderは自動的にアップデートを実行することができます。自動アップデートオプションを有効にしておいてください。

## 19.2. 状況

アンチスパム保護を設定するには、上級者モードのアンチスパム>ステータスで行います。




迷惑メール対策の状態

アンチスパムが有効か無効かを見ることとができます。 アンチスパムのステータスを変更する場合には、該当するチェックボックスをクリアまたは選択します。

**重要項目**
迷惑メールが受信ボックスに届かないよう、アンチスパムフィルタを有効にしておいてください。

統計画面では、アンチスパム処理の結果を（コンピュータが起動してからの）セッション毎に、あるいはまとめて（BitDefender をインストールしてからの総計を）確認できます。

### 19.2.1. プロテクションレベルの設定

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。

５つの保護レベルがあります：

| 保護レベル | 解説 |
| --- | --- |
| 弱 | 出所が確かな商用メールを多く受け取るアカウントを保護します。 フィルタは多くのメールを通過させますが、迷惑メールを通常メールと判定する可能性があります。 |
| 弱から中 | 出所が確かな商用メールを受け取るアカウントを保護します。 フィルタは多くのメールを通過させますが、迷惑メールを通常メールと判定する可能性があります。 |
| 中 | 一般的なアカウントを保護します。 フィルタは、疑わしいもの避けながら、ほとんどの迷惑メールをブロックします。 |
| 中から強 | 大量の迷惑メールを日常的に受け取るアカウントを保護します。 フィルタは迷惑メールをほとんど通過させませんが、通常のメールを間違って迷惑メールと判定する可能性があります。<br>誤って迷惑メールとしてしまう数を減らすには、友人/スパマーリストを作成して学習エンジン（ベイジアン）を学習させます。 |
| 強 | 非常に多くの迷惑メールを日常的に受け取るアカウントを保護します。 フィルタは迷惑メールをほとんど通過させませんが、通常のメールを間違って迷惑メールと判定する可能性があります。<br>誤って迷惑メールとしてしまう数を減らすためには、アドレス帳を友人リストに追加してください。 |

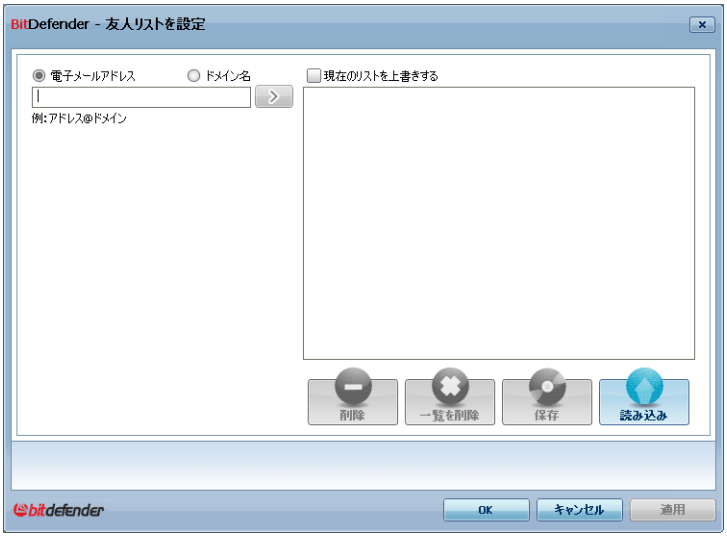
保護レベルをデフォルトの（中から強）に設定するには、デフォルトレベルをクリックします。

### 19.2.2. 友人リストを設定

友人リストは、その内容に関わらず、常にメッセージを受け取りたいすべてのメールアドレスの一覧です。友人からのメッセージは、内容が迷惑メールのように見えても迷惑メールと判定されません。

**注意**
友人リストのアドレスから届いたメールはすべて、それ以上の処理は行われずに自動的に受信ボックスへ届きます。

友人リストを設定するには、友人の管理をクリックします。または 友人ボタン（ アンチスパムツールバー内）をクリックします。




友人リスト

友人リストの項目追加または削除をここで行うことができます。

電子メールアドレスを追加するには、電子メールアドレスオプションにチェックし、アドレスを入力して、をクリックします。アドレスは友人リストに表示されます。

**重要項目**
構文：name@domain.com

ドメインを追加するには、ドメイン名オプションにチェックし、ドメインを入力して、をクリックします。ドメインが友人リストに表示されます。

**重要項目**
構文：

- @domain.com, *domain.com, domain.com - domain.comから受信したメールメッセージはすべて、その内容に関わらず受信ボックスに届きます；
- *domain* - domainから受信したメールメッセージはすべて（その末尾が何であれ）その内容に関わらず受信ボックスに届きます；
- *com - comで終わるドメインを持つ受信メールメッセージはすべて、その内容に関わらず受信ボックスに届きます；

一覧から項目を削除するには、それを選択して、削除ボタンをクリックします。 一覧から全ての項目を削除するには、一覧を削除するボタンをクリックして、はいを選択します。

友人リストをファイルに保存することができるので、それを別のコンピュータや製品の再インストール後に使用することができます。 友人リストを保存するには、保存ボタンをクリックして、お好きな場所に保存します。 このファイルは.dat拡張子が付いています。

以前保存した友人リストを読み込むには、読み込むボタンをクリックして、.bwlファイルを開きます。 以前保存した一覧を読み込んだ際に、現在の一覧の内容をリセットするには、現在の一覧を上書きするを選択してください。

**注意**
友人の名前およびメールアドレスを友人リストに追加することをお勧めします。BitDefenderはそのリストに記載された送信者からのメッセージはブロックしません；従って、友人を追加すると信頼できるメッセージの届く精度が向上します。

適用およびOKをクリックして友人リストを保存して閉じます。

### 19.2.3. スパマーリストを設定

スパマーリストは、内容に関わらず、メッセージを一切受け取りたくないメールアドレスの一覧です。

**注意**
迷惑メール送信者リストのアドレスから受け取ったメールはすべて、それ以降の処理なしに自動的にSPAMとマークされます。

迷惑メール送信者を管理するには、迷惑メール送信者の管理 または  迷惑メール送信者 ボタン（ アンチスパムツールバー内）をクリックします。


スパマーリスト

スパマーリストの項目追加や削除を、ここで行うことができます。

メールアドレスを追加するには、メールアドレスオプションにチェックし、アドレスを入力して、をクリックします。アドレスはスパマーリストに表示されます。

**重要項目**
構文：name@domain.com

ドメインを追加するには、ドメイン名オプションにチェックし、ドメインを入力して、をクリックします。ドメインはスパマーリストに表示されます。

**重要項目**
構文：

- @domain.com, *domain.com, domain.com - domain.comから届いたすべての受信メールメッセージに、SPAMタグが付加されます；
- *domain* - domainから届いたすべての受信メールメッセージ（ドメイン末尾に関わらず）に、SPAMタグが付加されます；
- *com - ドメイン末尾がcomのすべての受信メールメッセージにSPAMタグが付加されます；

**警告**

正当なウェブベースの電子メールサービスのドメインを迷惑メール送信者一覧に追加しないでください。（Yahoo、Gmail、Hotmail等） さもなければ、このようなサービスに登録しているユーザから受信した電子メールメッセージは、迷惑メール送信者として検出されてしまいます。 例えば、yahoo.comを迷惑メール送信者一覧に追加すると、 yahoo.com から送信された全ての電子メールメッセージが[spam]として区別されてしまいます。

一覧から項目を削除するには、それを選択して、削除ボタンをクリックします。 一覧から全ての項目を削除するには、一覧を削除するボタンをクリックして、はいを選択します。

迷惑メール送信者リストをファイルに保存することができるので、それを別のコンピュータや製品の再インストール後に使用することができます。 迷惑メール送信者リストを保存するには、保存ボタンをクリックして、お好きな場所に保存します。このファイルは.dat拡張子が付いています。

以前保存した迷惑メール送信者リストを読み込むには、読み込むボタンをクリックして、.bwl ファイルを開きます。 以前保存した一覧を読み込んだ際に、現在の一覧の内容をリセットするには、現在の一覧を上書きするを選択してください。

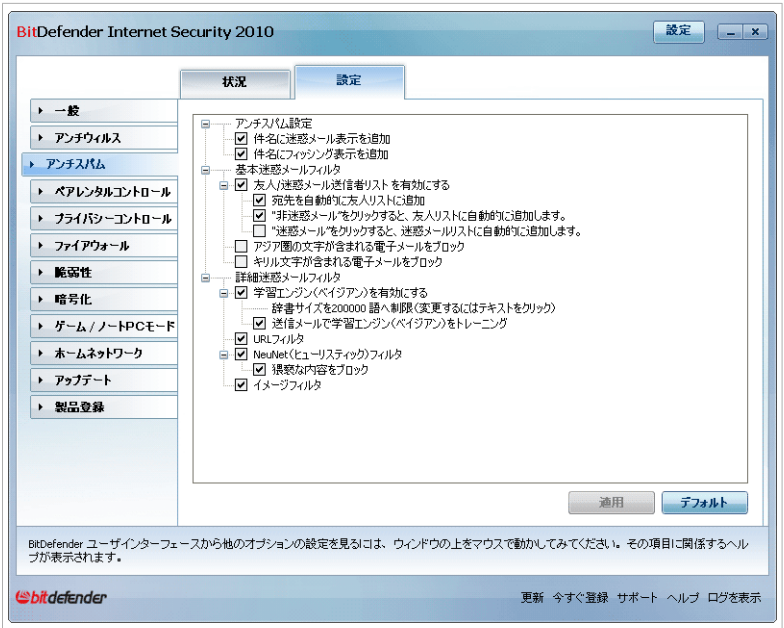
適用およびOKをクリックしてスパマーリストを保存して閉じます。

**重要項目**

BitDefenderを再インストールする場合にはその前に友人/スパマーリストを保存しておき、再インストール処理が終わってから読み込むとよいでしょう。

## 19.3. 設定

アンチスパムの設定は、上級者モードのアンチスパム>設定で行います。




アンチスパム設定

Windows で使用されているような拡張メニューに（迷惑メール対策設定、基本迷惑メールフィルタ、詳細な迷惑メールフィルタ）の３種類のオプションのカテゴリが用意されています。

**注意**
"+"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。

オプションを有効/無効にするには対応するチェックボックスをチェック/チェック解除してください。

デフォルトの設定を適用するには、デフォルトに戻すをクリックします。

適用をクリックして変更を保存します。

### 19.3.1. アンチスパム設定

- 件名に迷惑メール表示を追加 - 迷惑メールと判断されたすべてのメールメッセージは、件名にSPAMタグが付加されます。

- 件名にフィッシング表示を追加 - フィッシングメッセージと判断されたすべてのメールメッセージは、件名にSPAMタグが付加されます。

### 19.3.2. 基本迷惑メールフィルタ

- 友人／迷惑メール送信者リストを有効にする - 友人／迷惑メール送信者リスト使って、電子メールメッセージをフィルタリングします。
  - 宛先を自動的に友人リストに追加 - 送信メールの受信者を自動的に友人リストに追加します。
  - 自動的に友人リストに追加 - 非迷惑メールボタン（アンチスパムツールバー内）をクリックすると、送信者は自動的に友人リストに追加されます。
  - 自動的に迷惑メール送信者一覧に追加 - 迷惑メールボタン （アンチスパムツールバー内）をクリックすると、送信者は自動的に迷惑メール送信者一覧に追加されます。

  **注意**
  非迷惑メールおよび迷惑メールボタンは、ベイジアンフィルタを学習させるために使われます。

- アジア圏の文字が含まれる電子メールをブロック - アジア文字コードで書かれたメッセージはブロックします。
- キリル文字が含まれる電子メールをブロック - Cyrillic（キリル）文字コードで書かれたメッセージはブロックします。

### 19.3.3. 詳細迷惑メールフィルタ

- 学習エンジン（ベイジアン）を有効にする - 学習エンジン（ベイジアン）を有効/無効にします。
  - 辞書サイズを200000語に制限 - ベイジアン辞書のサイズを設定します - 小さいほど速いですが、大きいほど正確です。

    **注意**
    推奨サイズ：200,000 語

  - 送信メールで学習エンジン（ベイジアン）をトレーニング - 学習エンジン（ベイジアン）を送信メールでも学習させます。
- URL フィルタ - URL フィルタを有効/無効にします。
- NeuNet（ヒューリスティック）フィルタ - NeuNet（ヒューリスティック）フィルタを有効/無効にします。
  - 猥褻な内容をブロック - 件名に アダルトコンテンツ と書かれたメッセージの検出を有効/無効にします。

●イメージフィルタ - イメージフィルタを有効/無効にします。

# 20. ペアレンタルコントロール

BitDefenderペアレンタルコントロールは、お使いのシステムのアカウントごとにアクセスできるサイト、アプリケーションをコントロールすることができます。

ペアレンタルコントロールで遮断する設定ができます

- 不適切なウェブページ
- 特定の時間帯（例えば勉強の時間）のインターネット
- 特定のキーワードを含むウェブページ、メールやインスタントメッセージ
- ゲーム、チャット、ファイル共有プログラムなどのアプリケーション。
- それら以外の接触が許可されているIMによって送られたインスタントメッセージ。

**重要項目**

管理者権限をもったユーザのみ（システム管理者）がペアレンタルコントロールを構成することができます。 他のユーザがペアレンタルコントロールの設定を変更できないようにするために、パスワードを設定して保護することができます。 ユーザを指定してペアレンタルコントロールを有効にするとパスワードの設定が求められます。

ペアレンタルコントロールを使ってお子様をコンピュータやオンラインから制限するには、次にある主要なタスクを行う必要があります：

1. お子様が利用する際に使う、制限された（標準の）Windowsユーザアカウントを作成します。

**注意**

Windowsユーザアカウントを作成するには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）で行います。

2. ペアレンタルコントロールをお子様が使用するWindowsアカウントに設定する

ペアレンタルコントロールを設定するには、上級者モードのペアレンタルコントロールで行います。


ペアレンタルコントロール

それぞれのWindowsユーザアカウントのペアレンタルコントロールの状態に関する情報を、確認することができます。　ペアレンタルコントロールが有効の場合は、各ユーザ名の下に年齢カテゴリが記載されています。 ペアレンタルコントロールが無効な場合、ステータスは未設定です。

さらに、各ユーザごとに、ペアレンタルコントロール機能の状態を確認することができます：

- チェックマーク付きの緑色の丸：機能は有効です。
- 感嘆符付きの赤い丸：その機能は無効です。

ユーザ名の隣にある変更 ボタンをクリックして、それぞれのユーザアカウントのペアレンタルコントロールを設定することができるウィンドウを開きます。

この章では次のセクションでペアレンタルコントロールの機能の詳細と、その設定方法についてで説明しています。

## 20.1. 指定したユーザにペアレンタルコントロールを設定する

指定したユーザアカウントのペアレンタルコントロールを設定するには、該当するユーザアカウントの修正ボタンをクリックして、ステータスタブをクリックします。


ペアレンタルコントロールの状態

このユーザアカウントに対してペアレンタルコントロールを設定するには次の手順を行ってください：

1. このユーザアカウントに対してペアレンタルコントロールを有効にするには、ペアレンタルコントロール欄を選択します。

   **重要項目**
   独自に設定したコンピュータの利用ルールで、不適切なコンテンツからお子様を守るために、ペアレンタルコントロールを有効にしておいてください。

2. ペアレンタルコントロールの設定を保護するためにパスワードを設定する　詳細については、「ペアレンタルコントロール設定の保護」（p. 194）を参照してください。
3. お子様の年齢に相応しいウェブサイトのみをアクセスできるように、年齢カテゴリを設定します。 詳細については、「年齢カテゴリの設定」（p. 195）を参照してください。
4. 必要に応じて、このユーザのオプションを監視する設定をします：
   - 電子メールで活動報告を受信.　電子メール通知は、BitDefenderペアレンタルコントロールが、このユーザの活動をブロックする度に送信されます。

- インターネットトラフィック記録を保存. ユーザがアクセスしたウェブサイトを記録します。

詳細については次を参照してください。 「お子様のインターネット活動を監視」(p. 198).

5. 該当するペアレンタルコントロール機能を設定するアイコン又はタブをクリックします：
   - ウェブ - ウェブの項で設定したルールに従って、ウェブ閲覧をフィルタリングするには、ウェブを有効にします。
   - アプリケーション - アプリケーションの項で設定したアプリケーションへのアクセスをブロックします。
   - キーワード - キーワードの項で設定したルールに従って、ウェブ、メール、インスタントメッセージをフィルタリングするには、キーワードを有効にします。
   - インスタントメッセージ - IM トラフィックの項で設定したルールに基づいてコンタクト先とのチャットを許可、又はブロックするには、インスタントメッセージを有効にします。
   - 時間制限 - 時間制限の項で設定した時間表に従ってウェブ閲覧を許可するには、時間制限を有効にします。

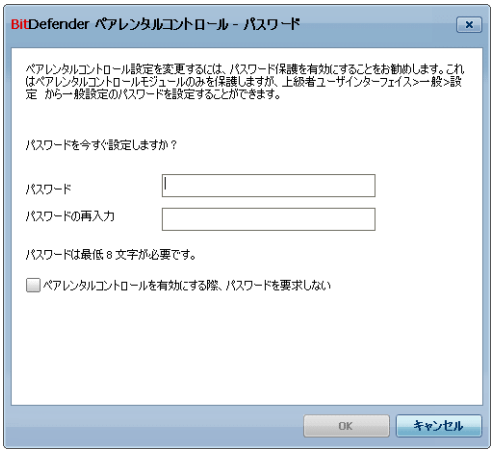
   **注意**
   設定方法については、この章の以下の項目を参照してください。

インターネットへのアクセスを完全にブロックするには、 インターネットをブロックボタンをクリックしてください。

### 20.1.1. ペアレンタルコントロール設定の保護

お客様以外でも、このコンピュータを使用する管理者権限を持っている場合は、ペアレンタルコントロール設定をパスワードで保護することをお勧めします。 パスワード設定することで、特定のユーザのために設定したペアレンタルコントロール設定を、管理者権限を持つ他のユーザが変更することができなくなります。

デフォルトではペアレンタルコントロールを有効にすると、パスワードを設定するか BitDefenderが確認します。




パスワード保護を設定

パスワード保護を設定するには、以下の項目を実行してください：

1. パスワード欄にパスワードを入力します。
2. 同じパスワードをパスワードを再入力欄に入力して確認します。
3. OKをクリックしてパスワードを保存し、ウィンドウを閉じます。

パスワードが設定されると、ペアレンタルコントロール設定を変更しようとする度に、パスワードの入力を求められます。 他のシステム管理者（もしいれば）もペアレンタルコントロール設定を変更する際には、パスワードの入力を求められます。

**注意**
このパスワードは他のBitDefender設定は保護しません。

パスワードを設定せず、このウィンドウが表示されないようにするには、ペアレンタルコントロールを有効にする際、パスワードを要求しないにチェックしてください。

### 20.1.2. 年齢カテゴリの設定

ヒューリィスティック・ウェブフィルタは、ウェブページを分析して、不適切な可能性のあるコンテンツの傾向に合致したものをブロックします。

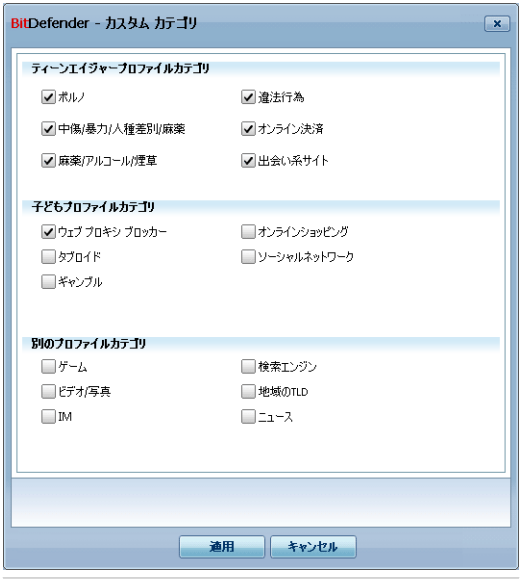
年齢に基づいて定義されたルールセットでウェブアクセスをフィルタリングするには、特定の許容レベルを設定する必要があります。　目盛りに沿ってスライダをドラッグして、選択したユーザに適当と思われる許容レベルを設定できます。

３種類の許容レベルがあります：

| しきい値レベル | 解説 |
|---|---|
| 子ども | 14歳未満のユーザに推奨される設定に従ってウェブの利用を制限できます。 ポルノ，性的，麻薬，ハッキングなど子どもに害を与える可能性のあるコンテンツのウェブページがブロックされます。 |
| １０代 | 14から18歳のユーザに推奨される設定に従って、ウェブの利用を制限できます。　性的，ポルノ，成年向けコンテンツのウェブページがブロックされます。 |
| 成人 | コンテンツに関わらず、すべてのウェブページの利用を無制限に許可します。 |

スライダをデフォルトレベルに設定するには、デフォルトレベルをクリックします。

ユーザがインターネットで見ることができるコンテンツの種類を、細かくコントロールしたい場合は、ウェブコンテンツのカテゴリを定義して、ウェブフィルタでブロックさせることができます。 ブロックするウェブコンテンツの形式を選択するには、カスタムカテゴリをクリックします。 新しいウィンドウが表示されます：




ウェブフィルタカテゴリ

ブロックしたいカテゴリ欄を選択すると、ユーザは一致するカテゴリのウェブサイトに、もはやアクセスすることはできません。 より簡単に選択するために、ウェブコンテンツのカテゴリは、適切であるとみなされる年齢層に応じて、一覧になっています：

- 子ども用プロファイルカテゴリ は、14歳以下の子どもがアクセスできるコンテンツを持っています。

| カテゴリ | 解説 |
|---|---|
| ゲーム | ゲーム、ゲームのフォーラム、ゲームのダウンロード、ダウト（トランプゲーム）、ゲーム攻略の手引き等、を提供するウェブサイト |
| ビデオ/写真 | ビデオやフォトギャラリを対応するウェブサイトです。 |
| IM | インスタントメッセージアプリケーション |
| 検索エンジン | 検索エンジンと検索ポータル |
| TLDの領域 | お客様の領域外のドメイン名を持つウェブサイトです。 |
| News | オンライン新聞 |

- ティーンエイジャー向けプロファイルカテゴリ は、14歳から18歳の子ども向けに安全とみなされたコンテンツです。

| カテゴリ | 解説 |
|---|---|
| ウェブプロキシブロッカー | 要求されたウェブサイトのURLを隠すためのウェブサイト |
| タブロイド | オンラインマガジン |
| 賭博 | オンラインカジノ、賭けをするウェブサイト、賭けのヒントを提供するウェブサイト、賭けのフォーラム 等。 |
| オンラインショッピング | オンラインショップや店舗 |
| ソーシャルネットワーキング | ソーシャルネットワーキングウェブサイト |

- 大人向けプロファイルカテゴリ 子どもやティーンエイジャーには不適切なコンテンツです。

| カテゴリ | 解説 |
| --- | --- |
| ポルノ | ポルノのコンテンツを運営するウェブサイト。 |
| 嫌がらせ / 暴力/ 人種差別 / 麻薬 | 暴力や人種差別、テロリズムや麻薬の使用を促進しているコンテンツを運営するウェブサイトです。 |
| 麻薬 / アルコール/ 煙草 | 麻薬、アルコール、煙草製品を販売、又は広告しているウェブサイト |
| 違法な活動 | 著作権侵害や海賊版コンテンツを運営するウェブサイトです。 |
| オンライン決済 | オンライン店舗のオンライン決済や精算のウェブフォームです。 ユーザはオンライン店舗を閲覧できますが、購入はブロックされます。 |
| オンラインデート | チャット、ビデオや写真共有によるアダルトデートウェブサイトです。 |

適用をクリックして、ユーザによってブロックされたウェブコンテンツのカテゴリを保存します。

## 20.2. お子様のインターネット活動を監視

BitDefenderは、お客様が不在のときでも、お子様がコンピュータで何をしていたかを追跡する手助けをします。 警告は、ペアレンタルコントロールモジュールが活動をブロックする度に、電子メールで送信されます。アクセスしたウェブサイトの履歴に関する記録も、保存することができます。

有効にしたいオプションを選択：

- 電子メールで活動報告を受信. 電子メール通知は、BitDefenderペアレンタルコントロールが活動をブロックする度に送信されます。
- インターネットトラフィック記録を保存. ペアレンタルコントロールが有効なユーザがアクセスしたウェブサイトを記録する。

### 20.2.1. アクセスしたウェブサイトを確認する

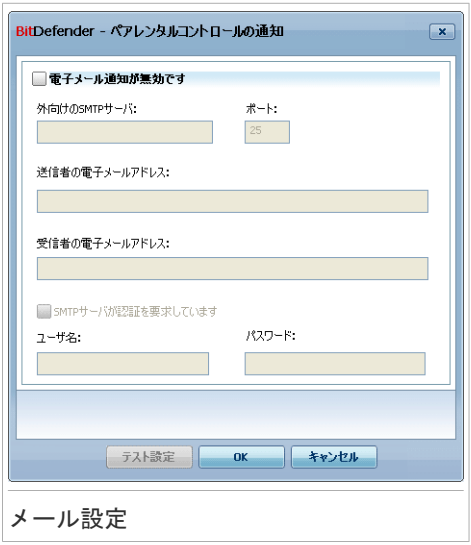
BitDefenderは、お子様がアクセスしたウェブサイトをデフォルトで記録します。

ログを表示するには、ログを表示するをクリックして、履歴&イベントを開き、インターネットログを選択します。

### 20.2.2. 電子メール通知を設定する

ペアレンタルコントロールがアクティビティをブロックすると、電子メールを受信する設定をするためには、ペアレンタルコントロールの標準設定画面の電子メールで活動報告を受信を選択してください。 電子メールアカウントの設定が求められます。はいをクリックして、設定ウィンドウを開くきます。

注意
通知設定をクリックして、後で設定画面を開くことができます。




メール設定

次に従って電子メールアカウントの設定を行ってください：

- 送信SMTPサーバ - 電子メールメッセージが送信されるメールサーバのアドレスを入力します。
- サーバーをデフォルトの25番ポート以外でお使いの場合、入力欄にポート番号を入力してください。
- 送信者電子メールアドレス - 電子メールの送信者欄に表示したいアドレスを入力します。
- 受信者の電子メールアドレス - レポートを受信したいアドレスを入力します。
- 認証が必要なサーバの場合は、SMTPサーバは認証が必要欄を選択して、該当欄にユーザ名とパスワードを入力してください。

**注意**
設定内容がお分かりにならない場合は、メールクライアントを開いて、電子メールアカウント設定をご確認ください。

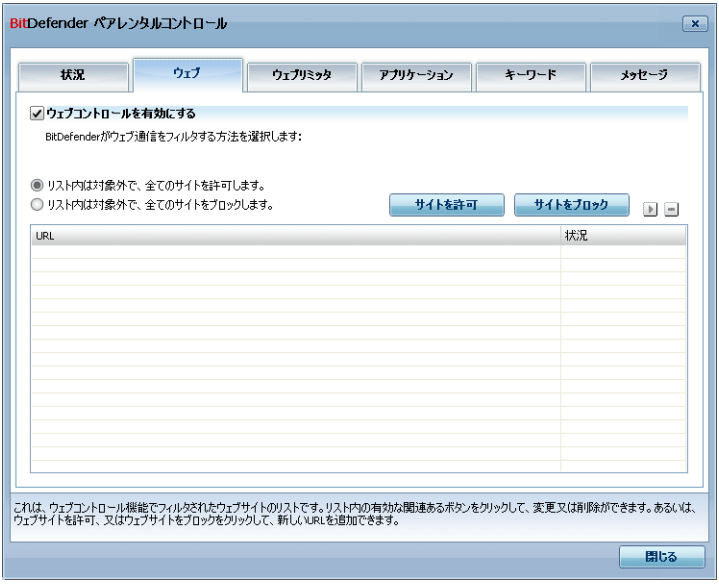
設定を検証するには、テスト設定ボタンをクリックしてください。検証中に問題が発見された場合は、BitDefenderはどの領域に注意をすればよいか通知します。

OKをクリックして変更を保存しウィンドウを閉じます。

## 20.3. ウェブコントロール

ウェブコントロールは、不適切なコンテンツのウェブサイト利用をブロックするのに役立ちます。BitDefenderはブロックするサイトやその部分の候補一覧を表示して通常のアップデート処理の一環としてアップデートします。

指定したユーザアカウントのウェブコントロールを設定するには、該当するユーザアカウントの修正 ボタンをクリックして、ウェブタブをクリックします。



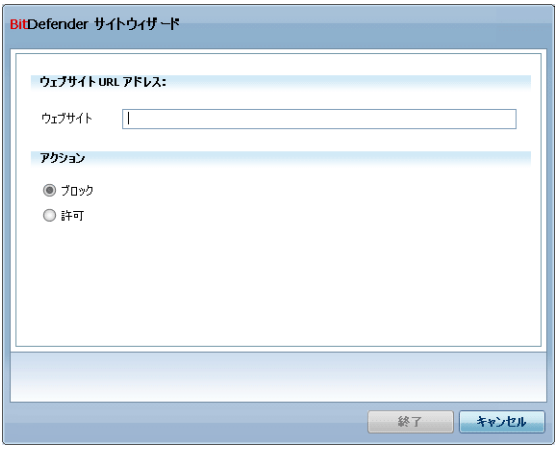

ウェブコントロール

この保護を有効にするには、ウェブコントロールを有効にするチェックボックスを選択してください。

### 20.3.1. ウェブコントロールルールを作成

ウェブサイトにアクセスを許可/ブロックする設定は、次の手順に従ってください：

1. サイトを許可 又は サイトをブロックをクリックしてください。新しいウィンドウが表示されます：




ウェブサイトを指定

2. ウェブサイト欄に、ウェブサイトアドレスを入力してください。
3. このルールから希望するアクションを選択します- 許可 又は ブロック
4. 完了 をクリックして、ルールを追加します。

### 20.3.2. ウェブコントロールルールを管理

設定されたウェブサイトコントロールルールは、画面の下側にあるテーブル内に一覧になっています。ウェブサイトアドレス、現在のステータスがウェブコントロールルールごとに一覧になっています。

ルールを編集するには、それを選択し、 編集ボタンをクリックするか、設定画面で必要な変更を行ってください。 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。

ウェブコントロールルールが無いウェブサイトに、BitDefenderペアレンタルコントロールが、どんなアクションを実行するかも、選択しなければなりません：

- リスト内のものを除き、全てのサイトを許可のオプションを選択して、設定したブロックアクション以外の全てのウェブサイトへのアクセスを許可します。

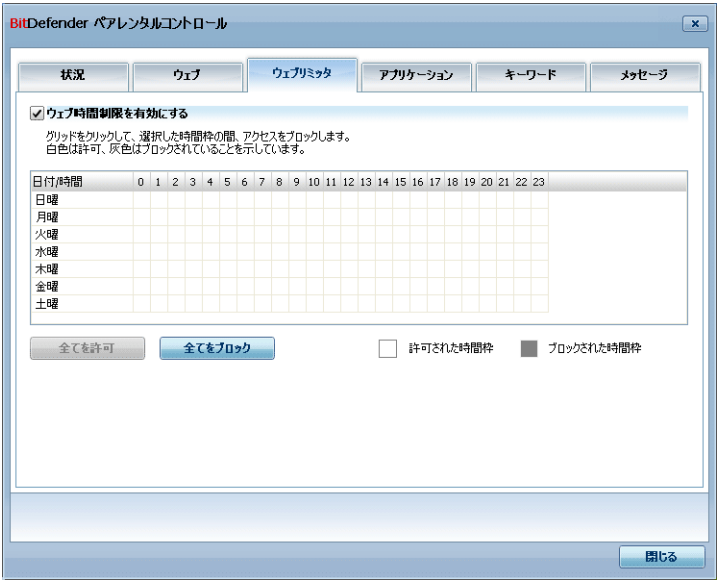
- リスト内のものを除き、全てのサイトをブロックのオプションを選択して、設定した許可アクション以外の全てのウェブサイトへのアクセスをブロックします。

## 20.4. ウェブ時間制限

ウェブ時間制限は、指定した時間、ユーザやアプリケーションによるウェブの利用を、許可またはブロックするようにします。

**注意**
BitDefenderはウェブ時間制限の設定に関わらず、１時間毎にアップデート処理を行います。

指定したユーザのウェブ時間制限を設定するには、該当するユーザアカウントの変更 ボタンをクリックして、ウェブ制限タブをクリックします。




ウェブ時間制限

この保護を有効にするには、ウェブ時間制限を有効にするチェックボックスを選択します。

全てのインターネットの接続がブロックされる、時間枠を選択してください。 各セルをクリックするか、クリックとドラッグで長い期間選択できます。全てをブロックをクリックして、全てのセルを選択して、全てのウェブアクセスをブロックする

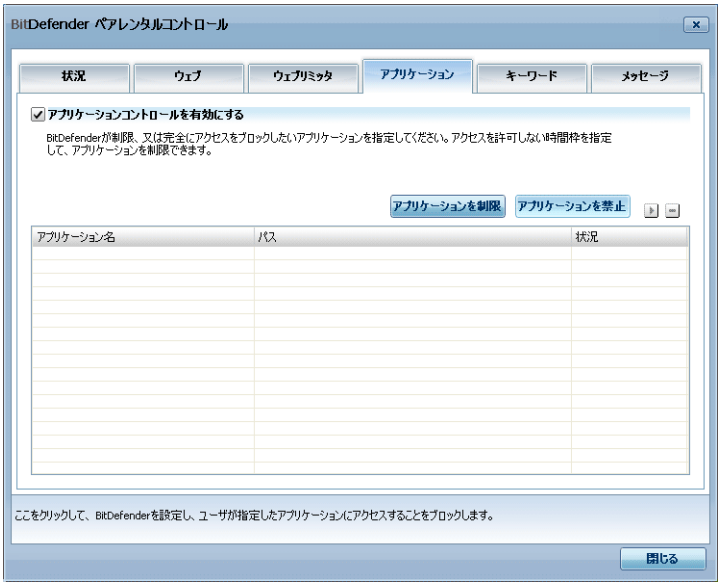
ことができます。全てを許可をクリックすると、インターネットへのアクセスは常時許可されます。

**重要項目**
灰色のボックスは、すべてのインターネット接続がブロックされる時間を表します。

## 20.5. アプリケーションコントロール

アプリケーションコントロールは、特定のアプリケーションの実行をブロックする手助けをします。ゲーム、メディア、およびメッセンジャソフトウェアやその他のカテゴリのソフトウェアおよびマルウェアは、この方法でブロックできます。この方法でブロックされたアプリケーションは、変更からも保護され、複製も移動もできません。 アプリケーションを完全にブロックする、又はお子様が宿題をしている間だけ等、決まった間だけブロックすることができます。

指定したユーザアカウントのアプリケーションコントロールを設定するには、該当するユーザアカウントの修正ボタンをクリックして、アプリケーションタブをクリックします。



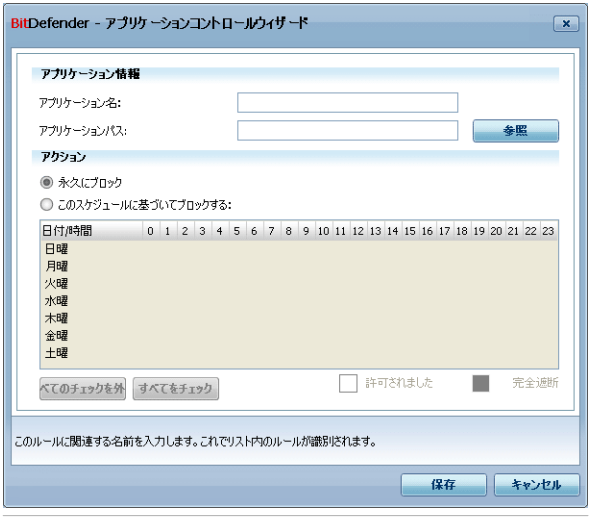

アプリケーションコントロール

この保護を有効にするには、アプリケーションコントロールを有効にするチェックボックスを選択してください。

### 20.5.1. アプリケーションコントロールルールを作成する

アプリケーションへのアクセスをブロック/制限する設定を行うには、次の手順に従ってください：

1. アプリケーションをブロック 又は アプリケーションを規制をクリックしてください。新しいウィンドウが表示されます：




アプリケーションを指定する

2. 閲覧　をクリックして、アクセスをブロック又は制限したいアプリケーションを決めてください。
3. ルールのアクションを選択：
   - 完全にブロック アプリケーションへのアクセスを完全にブロックします。
   - このスケジュールに基づいてブロック　決まった時間枠でアクセスを制限します。

   アプリケーションを完全にブロックするよりもむしろ、アクセスを制限したい場合は、アクセスをブロックする日数や時間枠も、グリッドから選択しなければなりません。　各セルをクリックするか、クリックとドラッグで長期間選択できます。全てをチェックをクリックして、全てのセルを選択して、全てのアプリケー

ションをブロックすることができます。全てのチェックを外すをクリックすると、アプリケーションへのアクセスは常時許可されます。

4. 完了 をクリックして、ルールを追加します。

### 20.5.2. アプリケーションコントロールルールを管理する

設定されたアプリケーションコントロールルールは、ウィンドウの下側にあるテーブル内に一覧になっています。アプリケーション名、パス、現在のステータスが、アプリケーションコントロールルールごとに表示されています。

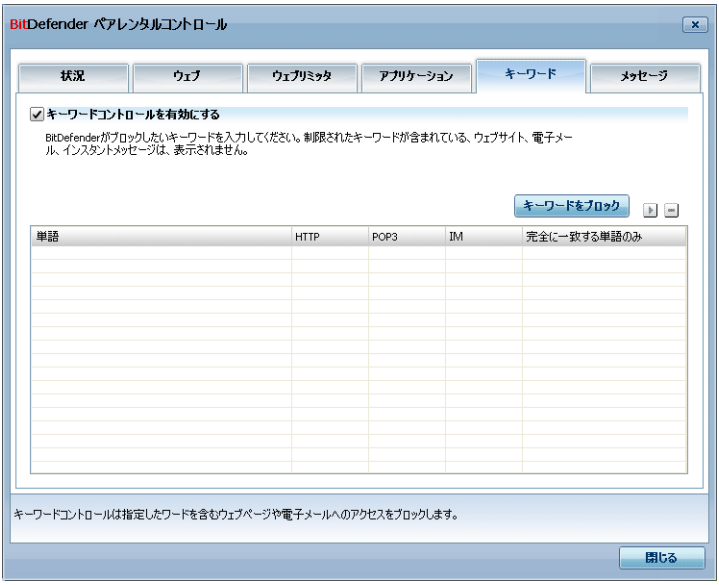
ルールを編集するには、それを選択し、 編集ボタンをクリックするか、設定画面で必要な変更を行ってください。 あるルールを削除するには、それを選択して 削除 ボタンをクリックします。

## 20.6. キーワードコントロール

キーワードコントロールは、特定の単語を含んだ電子メールメッセージ、ウェブページ、インスタントメッセージのアクセスをブロックします。 キーワードコントロールを使用することで、オンライン時にお子様が、不適切な言葉やフレーズを見ないようにすることができます。

**注意**
インスタントメッセンジャーのキーワードコントロールは、Yahooメッセンジャーと Windows Live(MSN)メッセンジャーのみで利用可能です。

指定したユーザアカウントのキーワードコントロールを設定するには、該当するユーザアカウントの修正ボタンをクリックして、キーワードタブをクリックします。



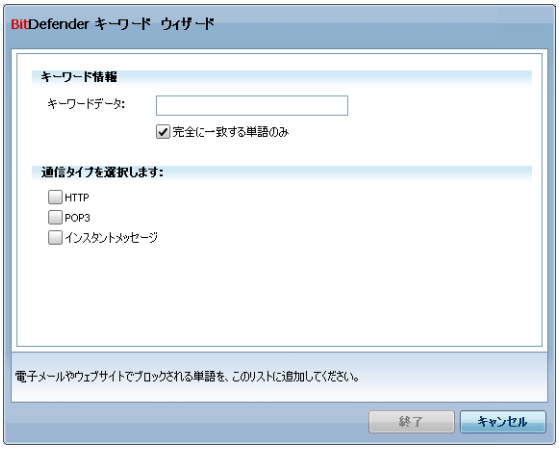

キーワードコントロール

チェックボックス キーワードコントロールを有効にするを選択することで、このコントロール機能を使うことができます。

### 20.6.1. キーワードコントロールルールを作成

単語やフレーズをブロックするには、次の手順に従ってください：

1. キーワードをブロックをクリックすると、新しいウィンドウが表示されます。




キーワードを指定する

2. 入力欄にブロックしたい単語やフレーズを入力してください。完全に一致する単語だけを検出したい場合は、 完全に一致する単語欄を選択します。
3. BitDefenderが指定した単語をスキャンするトラフィックタイプを選択してください。

| オプション | 解説 |
|---|---|
| HTTP | キーワードを含むウェブページをブロックします。 |
| POP3 | キーワードを含むメールメッセージはブロックされます。 |
| インスタントメッセンジャー | そのキーワードを含むインスタントメッセージはブロックされます。 |

4. 完了 をクリックして、ルールを追加します。

### 20.6.2. キーワードコントロールルールを管理

設定されたキーワードコントロールルールは、ウィンドウの下側にあるテーブル内に一覧になっています。別のトラフィック形式の単語や現在のステータスが、キーワードコントロールルールごとに一覧になっています。

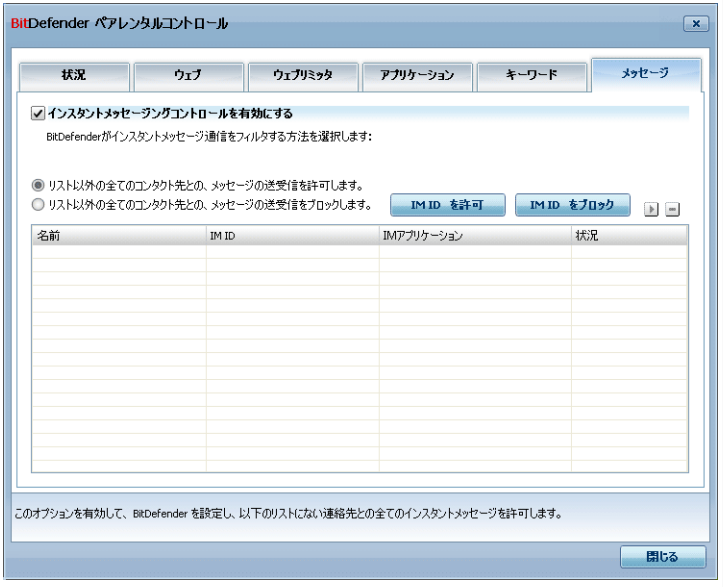
ルールを編集するには、それを選択し、 編集ボタンをクリックするか、設定画面で必要な変更を行ってください。 あるルールを削除するには、それを選択して 削除 ボタンをクリックします。

## 20.7. インスタントメッセンジャー（IM）コントロール

インスタントメッセンジャー（IM）コントロールで、お子様がチャットできるIMコンタクト先を指定できます。

**注意**
IMコントロールはYahooメッセンジャーとWindows Live（MSN）メッセンジャーでのみ利用可能です。

指定したユーザアカウントのIMコントロールを設定するには、該当するユーザアカウントの変更 ボタンをクリックして、メッセージングタブをクリックします。



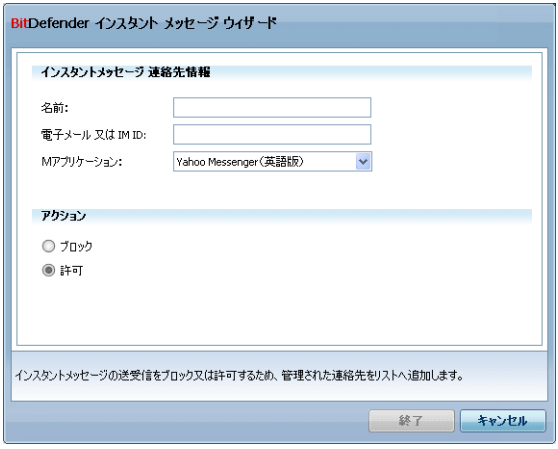

インスタントメッセージングコントロール

チェックボックス インスタントメッセンジャーコントロールを有効にする を選択することで、このコントロール機能を使うことができます。

### 20.7.1. インスタントメッセージ（IM）コントロールルールの作成

インスタントメッセージの連絡先を許可/ブロックする設定を行うには、次の手順に従ってください：

1. インスタントメッセージのIDをブロック 又は インスタントメッセージのIDを許可をクリックしてください。新しいウィンドウが表示されます：




インスタントメッセージのコンタクト先を追加する

2. 名前欄に連絡先の名前を入力します。
3. 電子メール又はインスタントメッセージID欄に、インスタントメッセージ相手先の電子メールアドレス、又はユーザ名を入力してください。
4. そのコンタクト先で通信するIMプログラムを選択する。
5. このルールに対するアクションを選択します - ブロック 又は 許可
6. 完了 をクリックして、ルールを追加します。

### 20.7.2. インスタントメッセージ(IM)コントロールルールの作成

設定されたIMコントロールルールは、ウィンドウの下側にあるテーブル内に一覧になっています。名前、IM ID、IMアプリケーション、及び現在のステータスが、IMコントロールルールごとに一覧になっています。

ルールを編集するには、それを選択し、 編集ボタンをクリックするか、設定画面で必要な変更を行ってください。 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。

BitDefenderペアレンタルコントロールは、ルールが作成されていないインスタントメッセージの連絡先に行う処理内容を選択しなければなりません。ブロック又はリスト内のものを除き、全てのインスタントメッセージの連絡先を許可を選択してください。

# 21. 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。

## 21.1. 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、上級者モードのプライバシーコントロール>状態で行います。


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。

### 21.1.1. 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 | 解説 |
|---|---|
| 弱 | 全ての保護機能は無効です。 |
| デフォルト | 個人情報コントロールだけが有効です。 |
| 強 | 個人情報コントロール、レジストリコントロール、Cookieコントロール及びScriptコントロール が有効です。 |

保護レベルを編集するにはカスタムレベルをクリックします。 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。

## 21.2. 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。 お客様のWindowsアカウントが管理者のアカウントの場合は、お客様が作成したルールを、別のコンピュータのユーザがWindowsユーザアカウントにログインした際にも適用することができます。

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。

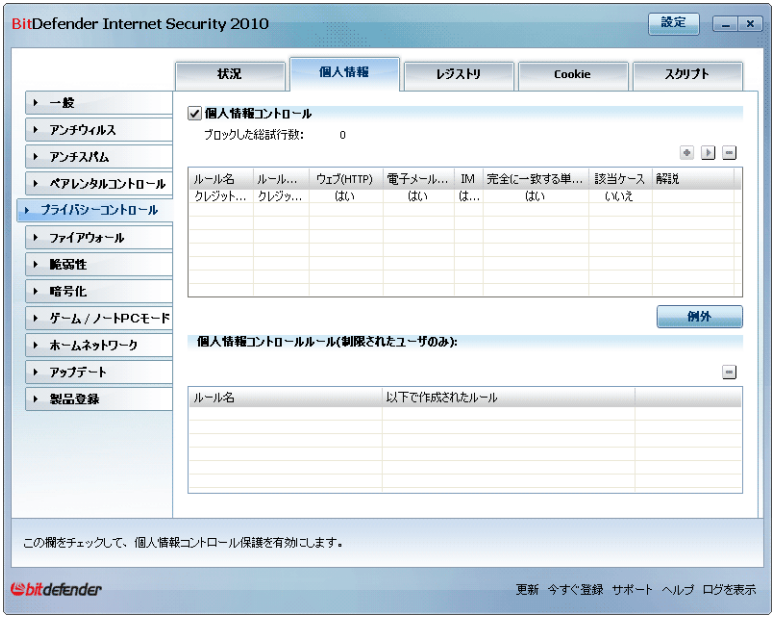
  そのようなアプリケーションがアンチウィルスの検知をなんとか逃れたとしても適切な個人情報保護ルールが作成されていれば、盗み出したデータをメールやweb、インスタントメッセンジャーを使って送ることができません。

- 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。

個人情報コントロールを設定するには、上級者モードのプライバシーコントロール>個人情報で行います。




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：

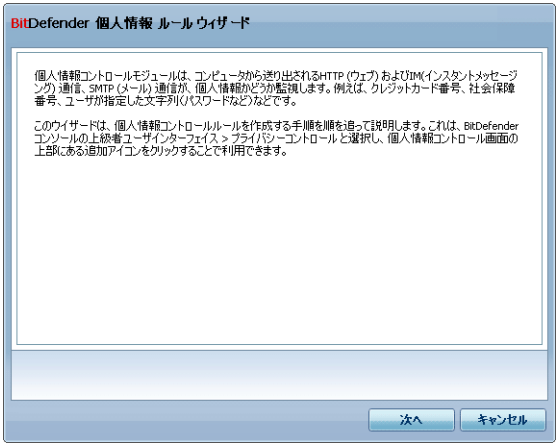
1. 個人情報コントロールを有効にするチェックボックスを選択します。
2. あなたの重要なデータを守るルールを作成します　詳細については「個人情報のルールを作成」（p. 214）を参照してください。
3. 必要に応じて除外を定義することもできます。　詳細については「除外を定義」（p. 217）を参照してください。
4. お客様がコンピュータの管理者の場合は、他の管理者が作成した個人情報ルールからご自身を除外することができます。

   詳細については、「他の管理者が定義したルール」（p. 219）を参照してください。

### 21.2.1. 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。

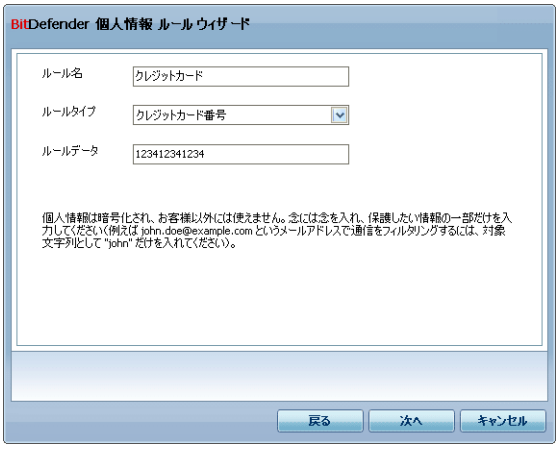
手順 1/4 - はじめに




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：

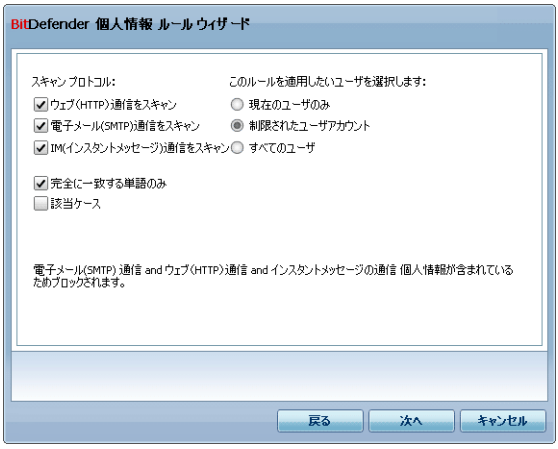
- ルール名 - 編集欄に新しい名前を入力してください。
- ルールの形式 - 住所、名前、クレジットカード、PIN（個人識別番号）、SSN（ソーシャルセキュリティ番号）などのルールの形式を選択してください。
- ルールデータフィールドに、送信したくない文字列の種類を入力します。 例えばクレジットカード番号を保護する場合には、ここに全ての形式または形式の一部を入力します。

**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 - トラフィックの種類とユーザを選択




トラフィックの種類とユーザを選択

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：

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

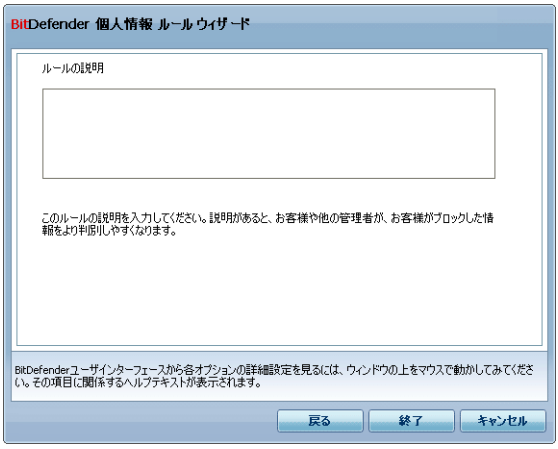
ルールのデータが単語全体と一致した場合のみ、あるいはルールのデータと検出された文字列の大文字小文字が一致した場合のみ、ルールが適用されるように指定できます。

ルールを適用するユーザを指定します。

- このユーザのみ有効 - このルールは、お客様のユーザのみ有効になります。
- 制限されたユーザアカウント - ルールは、お客様と制限された全てのWindowsアカウントに適用します。
- 全てのユーザ - ルールは全てのWindowsのアカウントユーザに適用します。

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

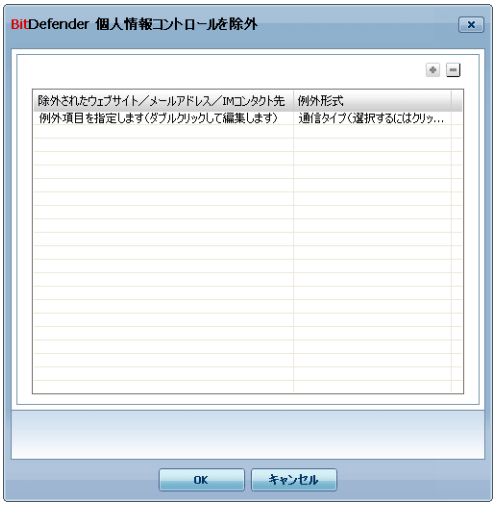
編集欄にルールの簡単な説明を入力します。 ルールに該当してブロックされた情報は表示されないときには、この説明が役に立ちます。

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。

## 21.2.2. 除外を定義

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。

除外を管理するためのウィンドウを開くには、除外をクリックしてください。




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. 除外する項目を指定　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、電子メールアドレス、インスタントメッセージのコンタクト先名を入力します。
3. トラフィック形式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。
   - 電子メールアドレスを指定したい場合は、電子メール(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、それを選択して 削除ボタンをクリックします。

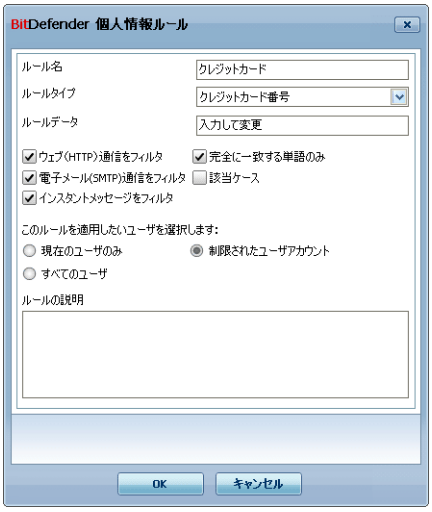
OKをクリックして変更を保存します。

### 21.2.3. 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、それを選択し、 編集ボタンをクリックするか、それをダブルクリックしてください。新しいウ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。

### 21.2.4. 他の管理者が定義したルール

お使いのシステムで、管理権限を所有しているのがお客様だけではない場合、別の管理者が個人情報ルールを作成することができます。 ログオン時に、他のユーザが作成したルールを適用したくない場合は、BitDefenderは、お客様が作成していないルールを排除することができます。

個人情報コントロールのルールの下にある表で、他の管理者が作成したルールの一覧を確認することができます。各ルールの名前、作成者は表で一覧になっています。

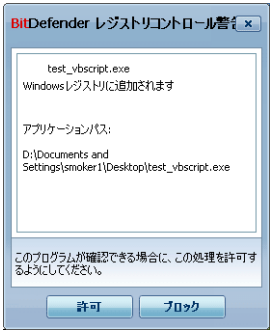
ルールからお使いのPCを除外するには、項目を選択して、 削除 ボタンをクリックします。

## 21.3. 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ィ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

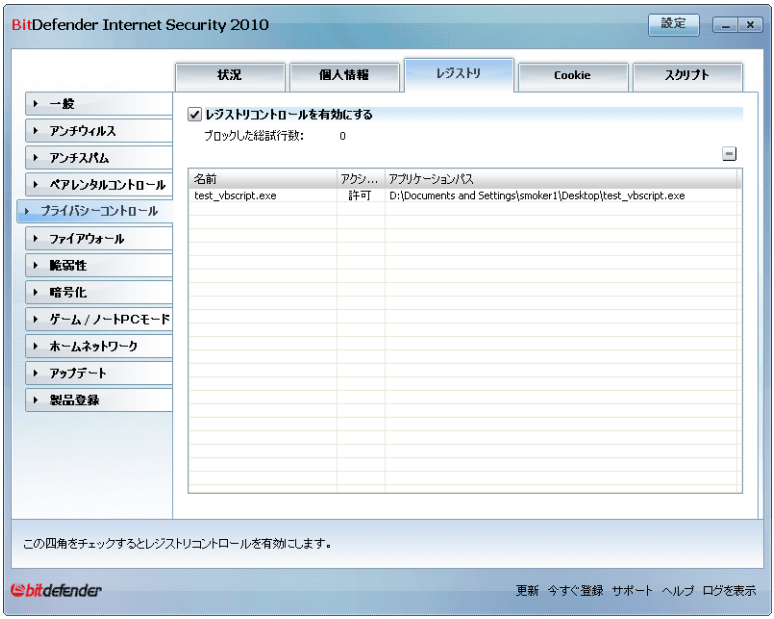
Windowsのレジストリを変更しようとしているプログラムを見ることができます。

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

レジストリコントロールを設定するには、上級者モードのプライバシーコントロール>レジストリで行います。




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。

## 21.4. 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。

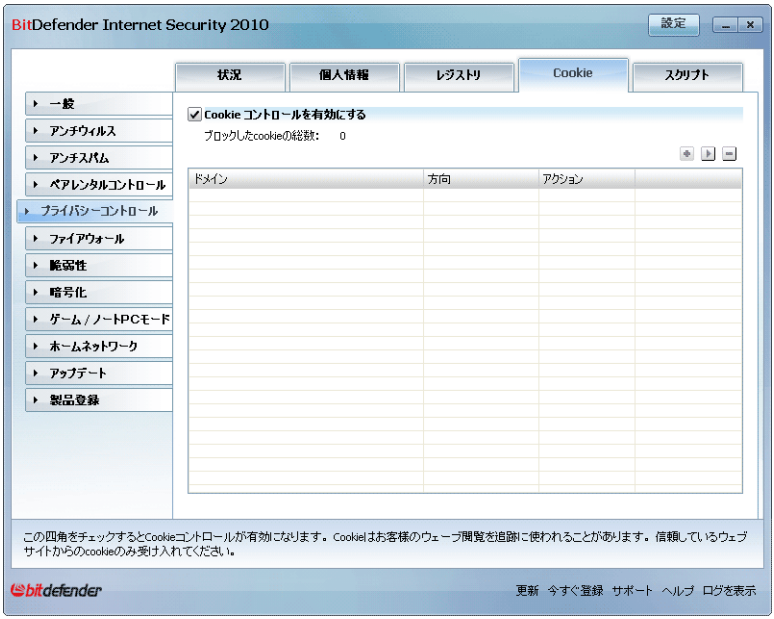
はい又はいいえをクリックすると、ルールの作成及び適用が行われ、ルール表に記載されます。

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、上級者モードのプライバシーコントロール>Cookieで行います。




Cookieコントロール

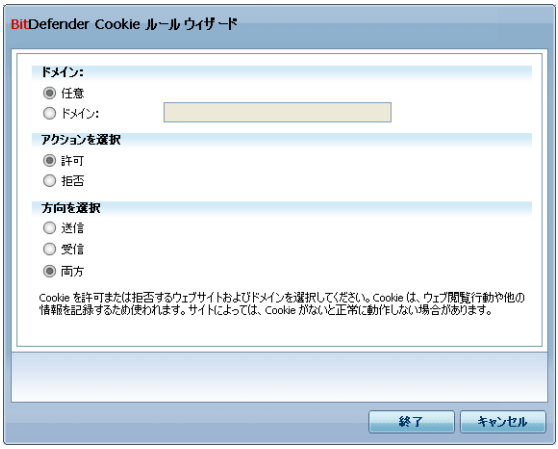
これまでに作成したルールが表に記載されます。

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、そのルールを選択して、 編集ボタンをクリックかダブルクリックしてください。設定ウィンドウで編集をしてください。

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。

### 21.4.1. 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 | 解説 |
|---|---|
| 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 | 解説 |
|---|---|
| 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。 |
| 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。

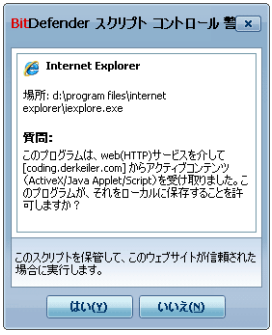
終了をクリックします。

## 21.5. 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。

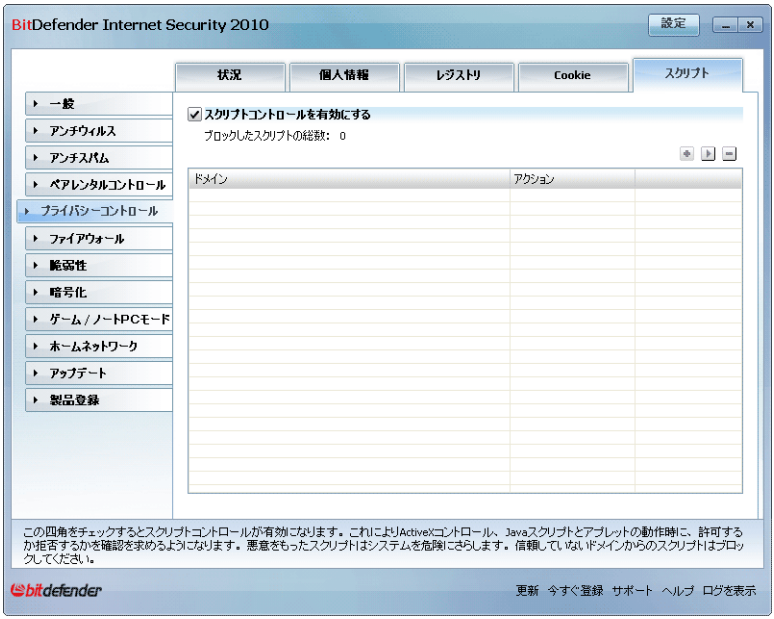



スクリプト警告

リソース名を確認できます。

はい又はいいえをクリックすると、ルールの作成及び適用が行われ、ルール表に記載されます。

スクリプトコントロールを設定するには、上級者モードのプライバシーコントロール>スクリプトで行います。




スクリプトコントロール

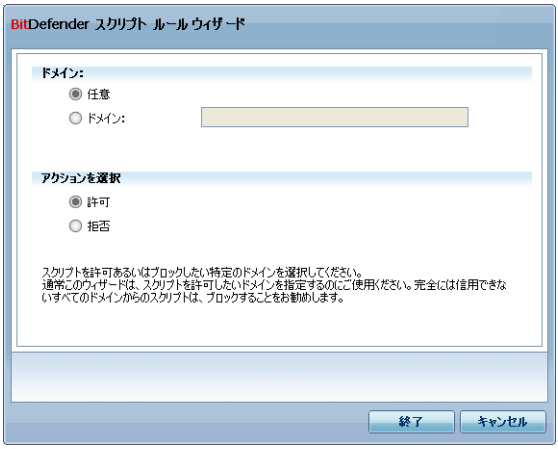
これまでに作成したルールが表に記載されます。

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、そのルールを選択して、編集ボタンをクリックかダブルクリックしてください。設定ウィンドウで編集をしてください。

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。

### 21.5.1. 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 | 解説 |
|---|---|
| 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。

# 22. ファイアウォール

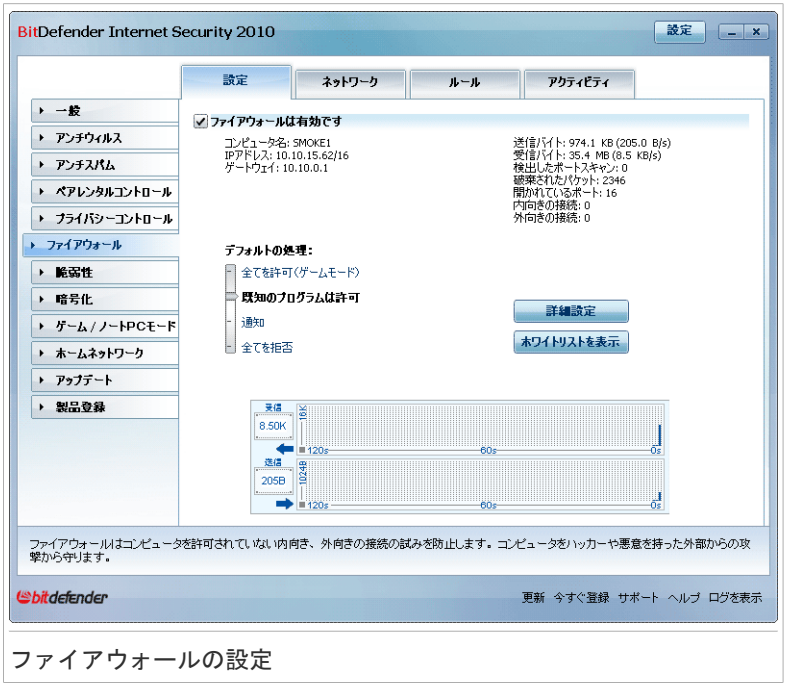
ファイアウォールは、許可されていない送受信接続からコンピュータを保護します。これは門番を置くのと似ています - インターネット接続を監視して、インターネットへ誰を通し、誰をブロックするか管理します。

**注意**
ADSLなどのブロードバンド接続を使用している場合は、特にファイアウォールが重要です。

ステルスモードでは、コンピュータは悪意のあるソフトウェアやハッカーから“隠されて”います。ファイアウォールモジュールは、ポートスキャン（多くの場合、攻撃の準備として“アクセスポイント”を見つけるためにマシンに対して送られるパケットの流れ）を自動的に検出して、保護することができます。

## 22.1. 設定

ファイアウォール保護の設定は、上級者モードのファイアーウォール>設定で行います。




ファイアウォールの設定

BitDefenderファイアウォールを有効にするか無効にするか確認できます。 ファイアウォールステータスを変更するには、該当するチェックボックスをクリアもしくは選択します。

**重要項目**
インターネットの攻撃から保護するため、ファイアウォールは有効にしておいてください。

２つの情報カテゴリーがあります：

- ネットワーク設定概要. コンピュータ名、IPアドレス、デフォルトゲートウェイを確認できます。 ひとつ以上のネットワークアダプタがある場合（２つ以上のネットワークに接続する構成）、各アダプタごとにIPアドレス、ゲートウェイの設定を確認できます。
- 統計データ. ファイアウォールの活動について各種統計を確認できます：
  - 送信バイト数
  - 受信バイト数
  - 検知されたポートスキャン数と、BitDefenderでブロックされた回数 ポートスキャンはハッカーによってよく使われる手法で、コンピュータ上で開いているポートを見つけ、それを利用しようとします。
  - 無視されたパケット数
  - 開いているポート数
  - 通信中の外部からの接続数
  - 通信中の外部への接続数

通信中の接続と開いているポート数をみるにはアクティビティ タブに行きます。

この画面の下部に、送受信される通信に関するBitDefenderの統計情報が表示されます。グラフには直近２分間のインターネット通信量が表示されます。

**注意**
ファイアウォールが無効になっている場合でも、グラフは表示されます。

### 22.1.1. デフォルトのアクションを設定

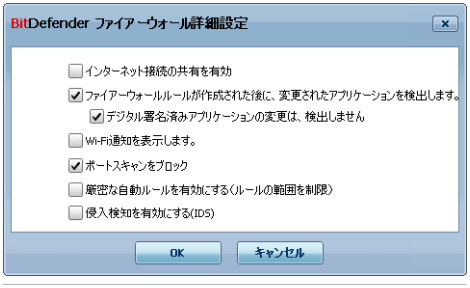
デフォルトでは、BitDefenderはホワイトリストにある主要なプログラムは自動的にネットワークサービスやインターネットへのアクセスを許可します。 そのほかのプログラムに対しては、BitDefenderは警告画面を表示して、どのように対応すべきか確認を求めてきます。 指定した処理は、そのアプリケーションがネットワーク、インターネットへアクセスする毎に適用されます。

スライダーをドラッグして、ネットワーク/インターネットアクセスが必要なアプリケーションに対してとるデフォルトのアクションを設定することができます。 デフォルトアクションには次のようなものがあります：

| デフォルトアクション | 解説 |
|---|---|
| 全てを許可 | 現在のルールを適用し、現在のルールと合致しない通信要求をすべて、確認なしに許可します。 このモードは使わないことをお勧めしますが、ネットワーク管理者やゲーマーには便利かもしれません。 |
| 主要プログラムを許可 | この現在のルールを適用して、BitDefenderが信頼できるとしている（ホワイトリスト内の）プログラムによる発信接続要求を確認なしに許可します。その他の接続要求には、BitDefenderがお客様の許可を確認します<br><br>ホワイトリストに記載されたプログラムは、世界的に広く利用されているアプリケーションです。サーバクライアントやオペレーティングシステムのアプリケーションに加え、著名なウェブブラウザ、オーディオ&ビデオプレーヤー、チャット、ファイル共有プログラムなどが含まれます。 完全なホワイトリストを表示するには、ホワイトリストを表示するをクリックします。 |
| 報告 | 現在のルールを適用し、現在のルールに合致しないすべての通信要求について、ユーザの指示を仰ぎます。 |
| 全てブロック | 現在のルールを適用して、ルールに合致しない通信の試みは全てブロックします。 |

### 22.1.2. 詳細ファイアウォール設定

詳細設定をクリックすると、さらに詳細なファイアウォールの設定を構成できます。




ファイアウォールの詳細設定

以下のオプションを指定できます：

- Internet Connection Sharing（ICS）対応を有効 - Internet Connection Sharing（ICS）への対応を有効にします。

  注意
  このオプションは、システムのICSを自動的に有効にするわけではなく、オペレーティングシステムでICSを有効にした場合に、この接続形式を許可するだけです。

  Internet Connection Sharing（ICS）は、ローカルエリアネットワークのメンバーが、コンピュータを経由してインターネットへ接続できるようにします。これは特別/特定のインターネット接続（例えばワイヤレス接続）を使っており、それをネットワークのメンバーと共有したい時に便利です。

  ローカルエリアネットワークのメンバーとインターネット接続を共有すると、リソースの消費レベルが高くなり、ある種のリスクを伴います。またポートを占有するかもしれません（インターネット接続を利用しているメンバーがポートを開いた場合）。

- ファイアーウォールルールの作成後に変更されたアプリケーションを検出 - インターネットへ接続しようとする各アプリケーションが、そのアクセスを制御しているルールが追加されてから変更されたかどうかをチェックします。アプリケーションが変更されていたら、そのアプリケーションのインターネットの利用を許可あるいは拒否できる警告が表示されます。

  通常、アプリケーションはアップデートによって変更されます。しかし、ユーザのコンピュータおよびネットワーク上の他のコンピュータに感染する目的で、マルウェアによって変更される可能性もあります。

  注意
  このオプションを選択して、そのアクセスを制御するルールが作成されてから変更が加えられたことが分かっているアプリケーションだけを許可することをお勧めします。

  署名付きアプリケーションは信頼でき、高いセキュリティレベルを持つと考えられます。 このイベントについて、署名付きアプリケーションが変更されても、警告せずにインターネットへの接続を許可するなら、デジタル署名付きアプリケーションの変更は検出しないをチェックしてください。

- Wi-Fi 通知を表示する - 無線ネットワークに接続した際に特定のネットワークイベントを、情報ウィンドウで表示します（新しいコンピュータがネットワークに追加されたなど）。

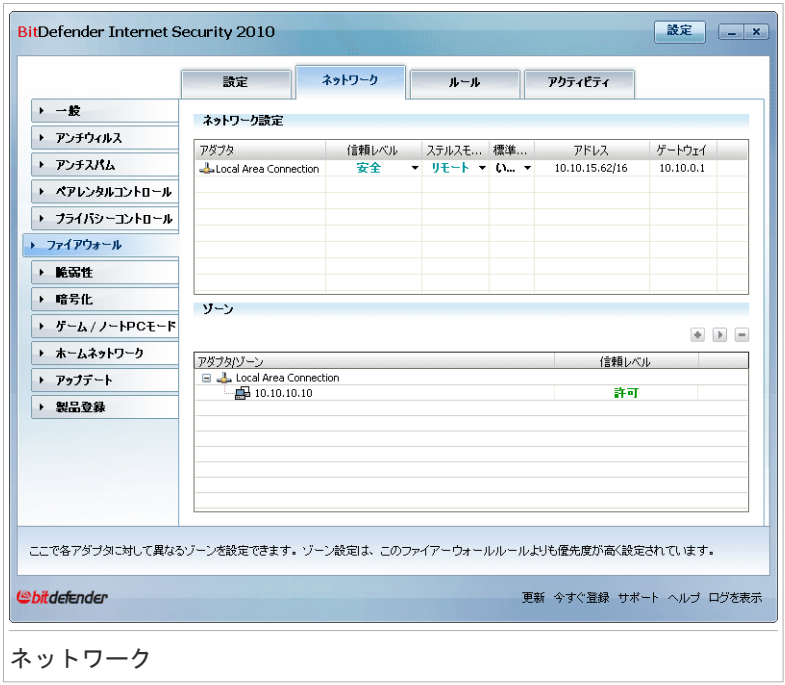
- ポートスキャンをブロックする - どのポートが開いているかを探査する試みを検知してブロックします。

ポートスキャンはハッカーがよく使う手口で、コンピュータのどのポートが開いているかを調べるものです。　彼らはセキュアではない脆弱なポートを見つけると、それを利用してコンピュータに侵入を試みます。

- 厳密な自動ルールを有効にする - ファイアウォール警告ウィンドウによる厳密なルールを作成します。　このオプションを選択するとBitDefenderは各プロセスがネットワークやインターネットアクセスを要求するアプリケーションを開こうするとユーザにとるべきアクションを確認してルールを作成します。
- 侵入検知システム(IDS)を有効にする - ヒューリスティックモニターを有効にして、ネットワークサービスやインターネットアクセスを利用しようとするアプリケーションを監査します。

## 22.2. ネットワーク

ファイアウォールの設定は、上級者モードのファイアーウォール>ネットワークで行います。




ネットワーク

ネットワーク設定 テーブルにある各列では、現在接続しているネットワークについて詳細な情報を表示しています：

- アダプター - お使いのコンピュータがネットワーク、インターネットへの接続で使用しているネットワークアダプタ。
- 信頼レベル - このネットワークアダプターに対して設定された信頼レベル このネットワークアダプタの設定に応じて、BitDefenderは自動的にアダプタに信頼レベルを適用したり追加の情報を表示します。
- ステルスモード - 他のコンピュータからこのコンピュータを検知できるか否か。
- 一般プロファイル - 一般ルールをこの接続に適用するか否か。
- アドレス - このアダプタに振られたIPアドレス
- ゲートウェイ - インターネットへの接続に使用しているIPアドレス

### 22.2.1. 信頼レベルの変更

BitDefenderはネットワークアダプタごとに信頼レベルを設定します。 アダプタに適用されている信頼レベルは、各ネットワークの信頼度を示しています。

信頼レベルに基づき特別なルールがアダプタに対して作成され、システムとBitDefenderプロセスがネットワークとインターネットにどのようにアクセスするかが規定されます。

ネットワーク設定 テーブル、信頼レベル 列の下において、各アダプタごとに設定された信頼レベルを確認できます。 信頼レベルを変更するには、信頼レベル カラムで矢印をクリックして、希望するレベルを選択します。

| 信頼レベル | 解説 |
|---|---|
| 完全信頼 | 各アダプタに対してファイアウォールを無効にします。 |
| ローカル信頼 | お使いのコンピュータと、ローカルネットワーク上のコンピュータとの間で行われる通信を許可します。 |
| 安全 | ローカルネットワークにあるコンピュータとのリソースの共有を許可します。 ローカル（自宅、オフィス）ネットワークでは自動的にこのレベルに設定されます。 |
| 危険 | お使いのコンピュータへ接続するネットワークもしくはインターネットコンピュータをブロックします。 公共のネットワーク（インターネットサービスプロバイダーからIPアドレスを取得している）では自動的にこのレベルに設定されます。 |
| ローカル遮断 | お使いのコンピュータとインターネットアクセスを提供しているローカルネットワーク上のコンピュータ間でのすべての通信をブロックします。 安全ではない（オープンな）ワイア |

| 信頼レベル | 解説 |
| --- | --- |
| | レスネットワーク環境では自動的にこの信頼レベルに設定されます。 |
| 完全遮断 | 各アダプタを通過するあらゆるネットワーク、インターネット通信を完全にブロックします。 |

### 22.2.2. ステルスモードを設定

ステルスモードは、お使いのコンピュータを、ネットワーク上またはインターネット上に悪意のあるソフトウェアやハッカーから隠します。 ステルスモードを設定するには ▾ にある矢印をステルス カラムでクリックして希望するオプションを選択します。

| ステルスオプション | 解説 |
| --- | --- |
| オン | ステルスモードが機能しています。 お使いのコンピュータはローカルネットワーク、インターネットの両方から見られることがありません。 |
| オフ | ステルスモードは機能していません。 ローカルネットワーク、インターネットから誰でもpingを行い、お使いのコンピュータを探知することができます。 |
| リモート | お使いのコンピュータはインターネットからは検知されません。 しかしローカルネットワークのユーザはpingを行い、お使いのコンピュータを検知することができます。 |

### 22.2.3. 一般設定の構成

ネットワークアダプタのIPアドレスが変更された場合はBitDefenderは信頼レベルをそれに従って変更します。 同じ保護レベルを使い続けるなら▾ にある矢印を 一般 カラムでクリックして はいを選択します。

### 22.2.4. ネットワークゾーン

特定のアダプタに対して許可する/しないコンピュータを追加できます。

信頼ゾーンとは完全に信頼しているコンピュータのことです。 お使いのコンピュータと信頼されたコンピュータ間で、全ての通信は許可されます。 安全ではないワイアレスネットワーク環境において、特定のコンピュータとリソースを許可するには、許可するコンピュータにそれらを追加します。

ブロックゾーンとは、お使いのコンピュータとは全く通信しないコンピュータのことです。

ゾーン テーブルでは現在のネットワークゾーンをアダプタごとに表示しています。

ゾーンを追加するには 追加 ボタンをクリックします。

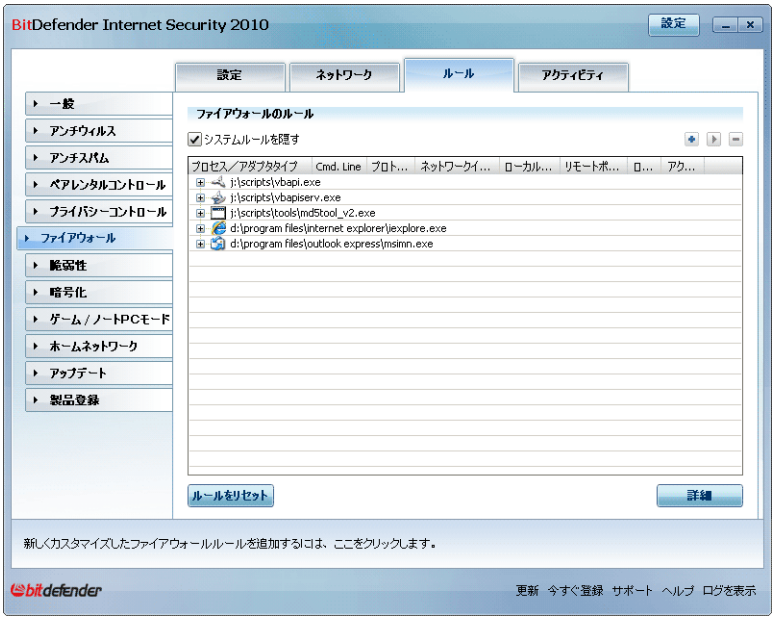

ゾーンの追加

次のように実行します：

1. 追加したいコンピュータのIPアドレスを選択します。
2. アクションを選択：
   - 許可 – お使いのコンピュータと選択したコンピュータ間のすべての通信を許可します。
   - 拒絶 – お使いのコンピュータと選択したコンピュータ間の全ての通信をブロックします。
3. OKをクリックします。

## 22.3. ルール

ネットワーク上のリソースやインターネットへのアプリケーションのアクセスを制御するファイアーウォールルールの管理は、上級者モードのファイアーウォール> ルールで行います。




ファイアウォールのルール

ファイアウォールルールが作成されたアプリケーション（プロセス）を確認することができます。 システムルールを隠すチェックボックスをクリアするとシステム、BitDefenderプロセスに関するルールをみることができます。

特定のアプリケーションに対して作られたルールをみるには、アプリケーション横にある＋をクリックします。 テーブルの各カラムをみることで、ルールの詳細な情報をみることができます：

- プロセス/アダプタのタイプ - ルールが適用されたプロセス、ネットワークアダプタのタイプ。 ルールは自動的に作成され、アダプタを通過するネットワーク、インターネットアクセスをフィルタリングします。 ルールを作成、または既存のルールを編集して、特定のアダプタ（例えばワイアレスネットワークアダプタ）を介したアプリケーションのネットワーク、インターネットアクセスをフィルタを制御できます。
- コマンドライン - Windowsのコマンドラインインターフェイスでそのプロセス起動を行ったコマンド(cmd).
- プロトコル - ルールが適用されているIPプロトコル。 次のものがあります：

| プロトコル | 解説 |
|---|---|
| すべて | 全てのIPプロトコルを含みます。 |
| TCP | Transmission Control Protocol - TCPは、２つのホストが接続を構築し、データストリームを交換できるようにします。TCPはデータの配達を保証すると共に、パケットが送り出されたのと同じ順番で届けられることを保証します。 |
| UDP | User Datagram Protocol - UDPは、IPを基本とした効率の高い通信を目的としています。ゲームやビデオを使った他のアプリケーションで、よく使用されます。 |
| 番号 | （TCP/UDPではない）IPプロトコルを示す番号。 IPプロトコルに割り当てられている番号の完全なリストは www.iana.org/assignments/protocol-numbers で確認することができます。 |

- ネットワークイベント - ルールが適用されているネットワークイベント。 次のイベントが考慮されます：

| イベント | 解説 |
|---|---|
| 接続 | 接続指向のプロトコル（TCP等）が接続を確立する際に行う準備的な標準メッセージの交換。 接続指向プロトコルでは、２台のコンピュータ間でのデータ通信は接続が確立された後で行われます。 |
| 通信 | ２台のコンピュータ間のデータの流れ。 |
| 通信待ち | あるアプリケーションが、接続の確立もしくは相手のアプリケーションからの情報を受け取るためにネットワークをモニタしている状態。 |

- ローカルポート - ルールが適用されているお使いのコンピュータ上のポート。
- リモートポート - ルールが適用されているリモートコンピュータ上のポート。
- ローカル - ルールがローカルネットワーク上のコンピュータにのみ適用されているか否か。
- アクション - 指定した環境においてこのアプリケーションがネットワークもしくはインターネットへの接続が許可されているかいないか。

### 22.3.1. ルールを自動的に追加

ファイアウォールが有効の場合、インターネットへの接続が行われるたびにBitDefenderはユーザの許可を求めます：


ファイアウォールの警告

以下の項目を確認できます：インターネットへ接続しようとしているアプリケーション，アプリケーションファイルへのパス，接続先，使用されるプロトコル，アプリケーションが接続しようとするポート

アプリケーションによって行われる、個々のIPプロトコルと全ポートを使用した、ローカルホストから任意の宛先へのすべての通信（送受信）を許可するには、許可をクリックします。ブロックをクリックすると、アプリケーションによる個々のIPプロトコルを使用したインターネット接続は、完全に拒否されます。

ユーザの回答に基づいてルールの作成と適用が行われ、表に記載されます。次回このアプリケーションが接続しようとした時は、このルールがデフォルトで適用されます。

**重要項目**
信頼できるIPやドメインからの受信接続のみを許可します。

### 22.3.2. ルールの削除及びリセット

あるルールを削除するには、それを選択して ルールを削除 ボタンをクリックします。 複数のルールを同時に選択して削除することができます。

特定のアプリケーションに対して作成されたルールを全て削除するには、そのアプリケーションをリストから選択して、 ルールを削除 ボタンをクリックします。

選択した信頼レベルで、デフォルトルール設定を読み込むには、ルールのリセットをクリックします。

### 22.3.3. ルールの作成と変更

手動での新しいルールの作成、既存のルールの変更は、構成ウィンドウにあるルールパラメータの設定でおこないます。

ルールの作成. 手動でルールを作成するには次の手順でおこないます：

1. ルールを追加 ボタンをクリックします。 新しい設定画面が表示されます。
2. メインおよび詳細パラメータを必要に応じて構成します。

3. OK をクリックして新しいルールを追加します。

ルールの変更. 既存のルールの変更は次の手順でおこないます：

1. ルールの編集 rule ボタンをクリック、もしくはそのルールをダブルクリックします。 新しい設定画面が表示されます。
2. メインおよび詳細パラメータを必要に応じて構成します。
3. OKをクリックして変更を保存します。

## メインパラメータの設定

構成ウィンドウのメイン タブでメインのルールパラメータを設定します。


メインパラメータ

次のパラメータを設定できます：

- プログラムのパス. 参照 をクリックして、ルールを適用するアプリケーションを選択します。 このルールを全てのアプリケーションに適用するには 全てを選択します。
- コマンドライン. 選択したアプリケーションがWindowsコマンドラインインターフェイスからある特別なコマンドで起動された場合のみ、そのルールを適用するには 全て のチェックボックスを外して、編集フィールドに該当するコマンドを入力します。
- プロトコル. メニューからルールを適用するIPプロトコルを選択します。

- 全てのプロトコルにルールを適用するには全てを選択します。
- このルールをTCPに適用するには、TCPを選択します。
- このルールをUDPに適用するには、UDPを選択します。
- 特定のプロトコルにルールを適用するには その他を選択します。 すると編集フィールドがあらわれます。 その編集フィールドにフィルタリングしたいプロトコルの番号を入力します。

注意

IPのプロトコル番号はInternet Assigned Numbers Authority (IANA)によって定められています。 IPプロトコルに割り当てられている番号の完全なリストは www.iana.org/assignments/protocol-numbers で確認することができます。

●イベント. 選択したプロトコルに基づいて、ルールを適用したいネットワークイベントを選択します。 次のイベントが考慮されます：

| イベント | 解説 |
|---|---|
| 接続 | 接続指向のプロトコル（TCP等）が接続を確立する際に行う準備的な標準メッセージの交換。 接続指向プロトコルでは、２台のコンピュータ間でのデータ通信は接続が確立された後で行われます。 |
| 通信 | ２台のコンピュータ間のデータの流れ。 |
| 通信待ち | あるアプリケーションが、接続の確立もしくは相手のアプリケーションからの情報を受け取るためにネットワークをモニタしている状態。 |

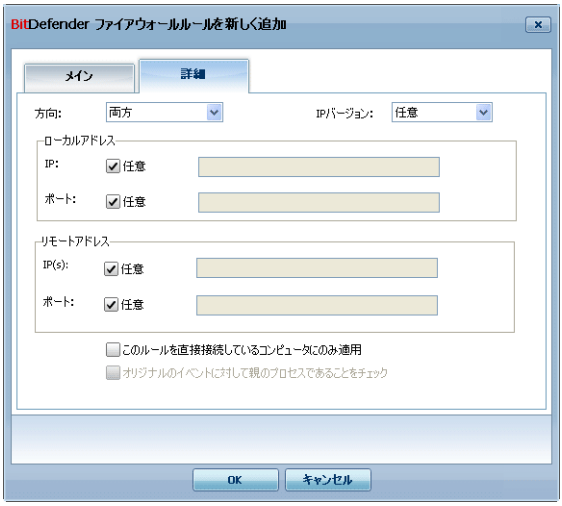
●アダプタの種類. ルールを適用するアダプタの種類を選択してください。

●アクション. 以下のアクションから一つ選択します：

| アクション | 解説 |
|---|---|
| 許可 | 指定されたアプリケーションは、指定された環境でのネットワーク/インターネットの使用が許可されます。 |
| 拒否 | 指定されたアプリケーションは、指定された環境でのネットワーク/インターネットの使用が拒否されます。 |

## 詳細パラメータの設定

構成ウィンドウの詳細 タブで、詳細なルールパラメータを設定できます。




詳細パラメータ

次の詳細パラメータを設定できます：

●方向. メニューからルールを適用する通信方向を選択します。

| 方向 | 解説 |
|---|---|
| 送信 | 送信通信にのみ、ルールが適用されます。 |
| 受信 | 受信通信にのみ、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。 |

●IPバージョン. メニューからルールを適用したいIPバージョン(IPv4、IPv6等)を選択します。

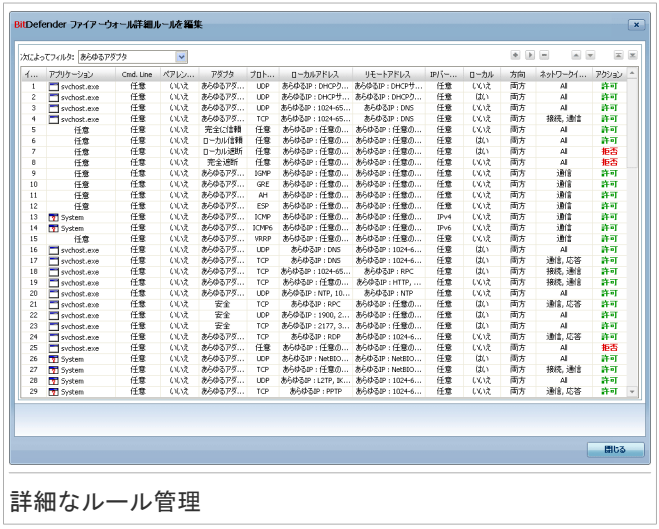
●ローカルアドレス. ルールを適用するローカルのIPアドレス、ポートの指定は次の手順でおこないます。

- もし複数のネットワークアダプターが接続されている場合は、全て チェックボックスを外して、特定のIPアドレスを入力してください。
- プロトコルとしてTCPかUDPを選択している場合は、特定のポートまたは0から65535の範囲を設定できます。すべてのポートにルールを適用するには、すべてを選択します。

- リモートアドレス. ルールを適用するリモートのIPアドレス、ポートの指定は次の手順でおこないます：
  - お使いのコンピュータと特定のコンピュータ間の通信をフィルタするには、 全て チェックボックスを外して、そのIPアドレスを入力します。
  - プロトコルとしてTCPかUDPを選択している場合は、特定のポートまたは0から65535の範囲を設定できます。すべてのポートにルールを適用するには、すべてを選択します。
- このルールを直接接続しているコンピュータにのみ適用. このオプションはローカルの通信にのみルールを適用する場合に選択します。
- オリジナルのイベントに対して親のプロセスであることをチェック. このパラメータを変更できるのは 厳密な自動ルール を選択しているときだけです(設定 タブで 詳細設定)。 厳密なルールではBitDefenderはアプリケーションがネットワーク/インターネットアクセスを行ったとき、その親のプロセスが異なる場合であってもとるべきアクションの確認を求めてきます。

## 22.3.4. 詳細なルール管理

ファイアウォールルールに対して詳細なコントロールを行うには詳細をクリックします。 新しいウィンドウが開きます。




詳細なルール管理

ファイアウォールのルールがチェックインされた順序でリスト表示されています。テーブルの各列はルールごとに包括的な情報を表示しています。

**注意**

接続の試みが行われると（それが内向き、外向きにかかわらず）、BitDefenderは各接続にマッチした最初のルールのアクションを行います。 そのため、どのルールの順番でチェックされたかが非常に重要です。

あるルールを削除するには、それを選択して ルールを削除 ボタンをクリックします。

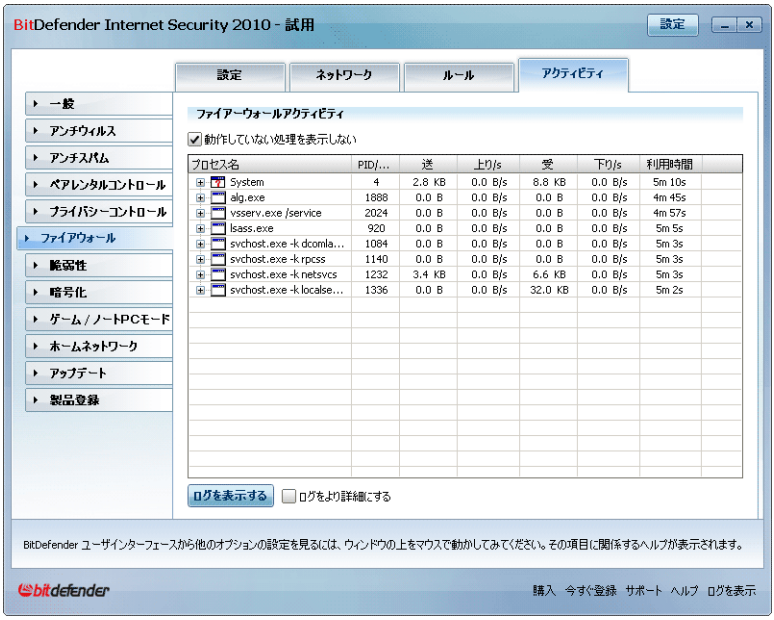
既存のルールを編集するには、それを選択して ルールの編集 ボタンをクリックするか、ダブルクリックします。

ルールの優先度を変更できます。選択したルールの優先順位を１つ上げるには、一覧内を上へ移動ボタンをクリックし、選択したルールの優先順位を１つ下げるには、一覧内を下へ移動ボタンをクリックしてください。 ルールに最も高い優先順位を与えるには、最初へ移動ボタンをクリックします。ルールに最も低い優先順位を与える場合は、最後へ移動ボタンをクリックします。

閉じるをクリックしてウィンドウを閉じてください。

## 22.4. 接続コントロール

アプリケーション毎に現在のネットワーク／インターネット（TCPおよびUDP）の状況を監視したり、BitDefenderファイアーウォールログを表示するには、上級者モードのファイアウォール>アクティビティを開きます。




接続コントロール

アプリケーション別に並び替えたすべての通信を確認できます。各アプリケーションには、発信&受信通信速度および送受信された総データ量に関する統計に加え、開いている接続およびポートを確認できます。

活動していないプロセスもみる場合には、活動していないプロセスを隠す チェックボックスを外します。

アイコンの意味は次のとおりです：

- 外向き接続を表示
- 内向き接続を表示
- お使いのコンピュータで開いているポート。

ウィンドウには、現在のネットワーク/インターネットアクティビティがリアルタイムに表示されます。接続あるいはポートが閉じていると、対応する統計項目が灰色表示され、ある時点で非表示になります。 通信を生成するか、開いていたポートをユーザが閉じたアプリケーションに対応する、すべての統計項目にも同じことが起こります。

ファイアーウォールモジュールに関連したイベント（ファイアーウォールの有効/無効、通信のブロック、変更設定）、またこのモジュールで検知された活動（ポートスキャン、接続試みのブロック、ルールに基づいた通信ブロック）　をみるには、BitDefenderファイアーウォールログファイルを ログを表示をクリックして確認します。 このファイルは現在のWindowsユーザの共通フォルダの次のパスに配置されています： ...BitDefender¥BitDefender Firewall¥bdfirewall.txt.

もしより詳細な情報をログに残したいなら、より詳細なログを記録を選択します。

# 23. 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に保ち続けることです。 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お客様に通知いたします。

## 23.1. 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、上級者モードの脆弱性>ステータスで行います。


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。

### 23.1.1. 脆弱性の解消

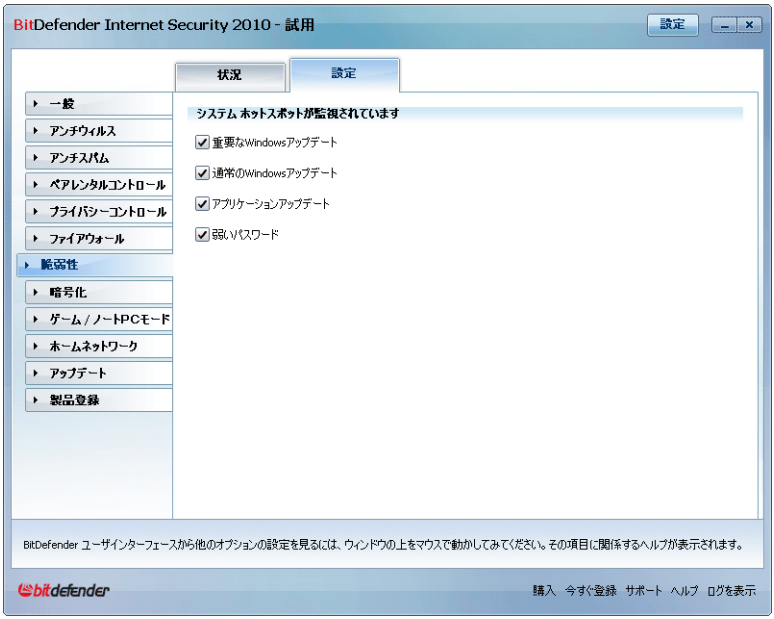
問題に応じて、以下に指定した脆弱性を修復します：

- Windowsアップデートが有効な場合、インストールをクリックして、インストールします。それはアクション欄にあります。
- 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。
- Windowsユーザアカウントのパスワード強度が弱い場合は、修正をクリックして、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。　詳細については、次を参照してください。「脆弱性チェックウィザード」（p. 69）

## 23.2. 設定

自動的に脆弱性チェックを行うよう設定するには、上級者モードの脆弱性>設定で行います。




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。

# 24. 暗号化

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。

## 24.1. 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。

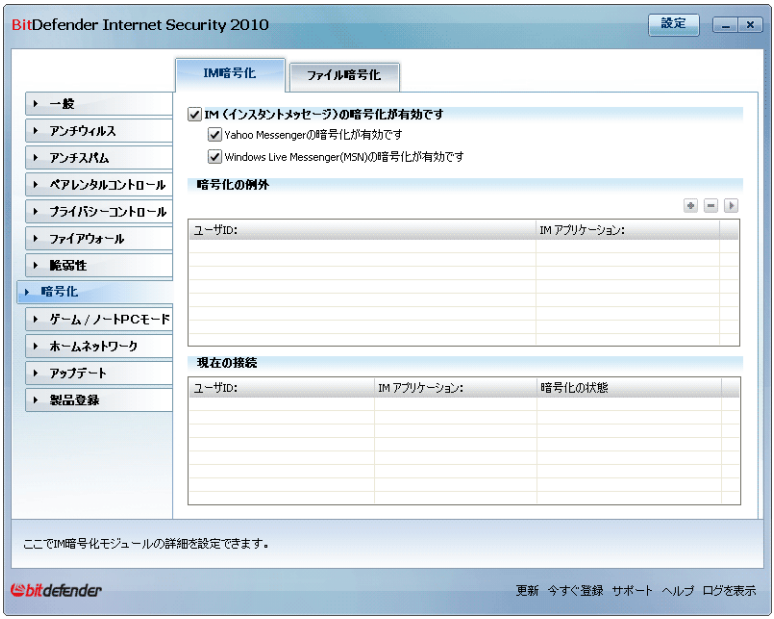
**重要項目**

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!、他のWindows Live (MSN)のいずれかを使用している相手との会話は、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、上級者モードの暗号化>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. 296)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。

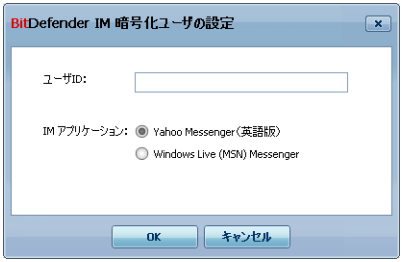
２つの表が表示されています：

- 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。

### 24.1.1. 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。

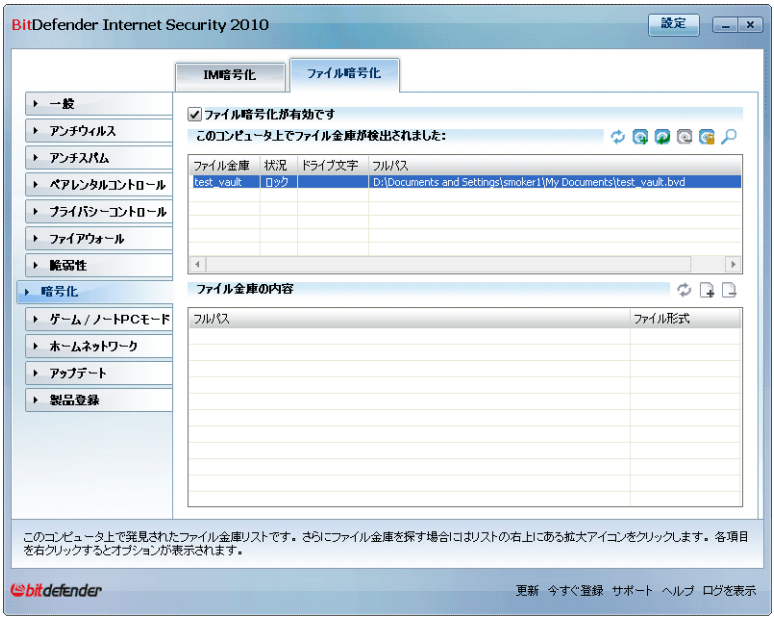
## 24.2. ファイル暗号化

BitDefenderのファイル暗号化は、お使いのコンピュータ上に作成される、暗号化され、パスワードがかけられた論理的なドライブ（保管庫）です。そこに秘密のドキュメントを格納することができます。 ファイル金庫に格納されたデータはパスワードを知っているユーザのみがアクセスできます。

セキュリティのためにはファイル金庫を開いたり、データを格納したり、閉じたりするのにパスワードが必要です。 金庫を開いている間は新しいファイルを追加したり、現在のファイルのアクセスしたり、それらを変更することができます。

物理的には、このファイル金庫はローカルのハードディスクに格納された１つのファイルで.bvdの拡張子をもっています。 ファイル金庫は実際は物理的なファイルなので、他のOS（Linuxなど）からもこれにアクセスすることができますが、そこの格納されている情報は暗号化されているためよみとることができません。

お使いのコンピュータ上のファイル金庫の管理は、 上級者モードの暗号化>ファイル暗号化で行います。




ファイル金庫

ファイル金庫を無効にするには 、チェック欄ファイル暗号化を有効にするをクリアにして、 はいをクリックします。 ファイル金庫を無効にすると全ての金庫のファイルがロックされるため、その金庫にあるファイルにアクセスすることができなくなります。

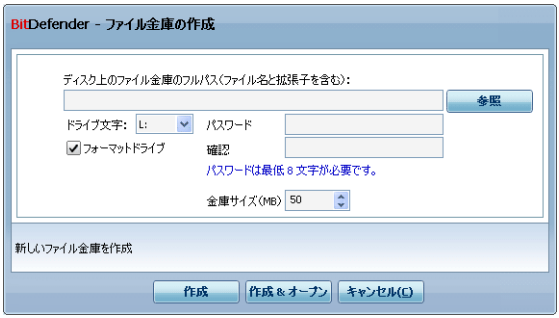
上の表ではお使いのコンピュータ上にあるファイル金庫が表示されています。 そこで名前、状態（オープン/ロック）、ドライブ文字、ファイル金庫へのフルパスを確認することができます。 下の表に選択した金庫の中身が表示されています。

### 24.2.1. 金庫の作成

新しい金庫の作成は次の手順で行います：

- 金庫を作成をクリック。
- ファイル金庫の表で右クリックして 作成を選択します。
- デスクトップ上またはコンピュータにあるフォルダで右クリックしてBitDefender ファイル金庫にカーソルを当てて作成を選択します。

新しいウィンドウが開きます。




ファイル金庫の作成

次のように実行します：

1. 場所と金庫ファイルの名前を指定。
   - 閲覧をクリックして金庫の場所を選択し、任意のファイル名で保存します。
   - 該当欄に金庫名を入力してマイドキュメントに作成します。 マイドキュメントを開くために、 start スタートメニューをクリックしてマイドキュメントをクリックします。
   - ディスク上の金庫ファイルまでのフルパスを入力。 例えば、C:¥my_vault.bvd
2. メニューからドライブ文字を選択。 金庫をオープンと、マイコンピュータ上に選択したドライブ名で仮想ディスクドライブが表示されます。
3. 金庫の新しいパスワードを新しいパスワード 及び 新しいパスワード(確認) 欄に入力します。 金庫を開いたり、そのファイルにアクセスする際には必ずパスワードが要求されます。
4. ドライブのフォーマット を選択すると金庫の仮想ドライブがフォーマットされます。 その金庫にファイルを追加する前にドライブをフォーマットする必要があります。
5. デフォルトの金庫のサイズ(50 MB) を変更するには、金庫のファイルフィールドでサイズを入力します。
6. 作成 をクリックすると、その選択した場所に金庫を作成します。 マイコンピュータ上に仮想ディスクドライブとして金庫を作成して表示するには 作成&オープン をクリックします。

BitDefenderはただちに処理結果をお伝えいたします。 エラーが発生した際、そのエラーメッセージを問題解決に使用してください。 OKをクリックしてウィンドウを閉じます。

注意
すべてのファイル金庫を同じ場所に保存すれば、すぐにみつけることができるので便利です。

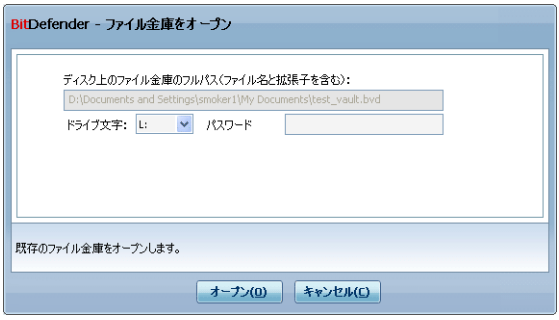
### 24.2.2. 金庫をオープンする

金庫にあるファイルにアクセスして作業するためには、必ずその金庫をオープンしなければなりません。 金庫をオープンすると仮想ディスクドライブがマイコンピュータ上に現れます。 このドライブは金庫に割り当てられたドライブ名で表示されます。

金庫をオープンするには、次のいずれかの手順で行います：

- テーブルから金庫を選択して 金庫をオープンをクリックします。
- テーブルにある金庫を右クリックして 開くを選択します。
- コンピュータ上にある金庫のファイルを右クリックしてBitDefenderファイル金庫にカーソルをあてて 開くを選択。

新しいウィンドウが開きます。




ファイル金庫をオープン

次のように実行します：

1. メニューからドライブ文字を選択。
2. 金庫にかけるパスワードをパスワードフィールドに入力します。
3. 開くをクリックしてください。

BitDefenderはただちに処理結果をお伝えいたします。 エラーが発生した際、そのエラーメッセージを問題解決に使用してください。 OKをクリックしてウィンドウを閉じます。

### 24.2.3. 金庫をロックする

ファイル金庫での作業を終えたら、かならずデータを守るためロックする必要があります。 ファイル金庫をロックすることで、その金庫ディスクドライブはマイコンピュータから消えます。それに伴い、この金庫に格納されているデータへのアクセスは完全にブロックされます。

金庫をロックするには、次のいずれかの手順を行います：

- テーブルから金庫を選択して 金庫をロックをクリックします。
- テーブルにある金庫を右クリックしてロックを選択します。
- コンピュータ上にある仮想ディスクドライブを右クリックして BitDefenderファイル金庫にカーソルをあてて ロックを選択。

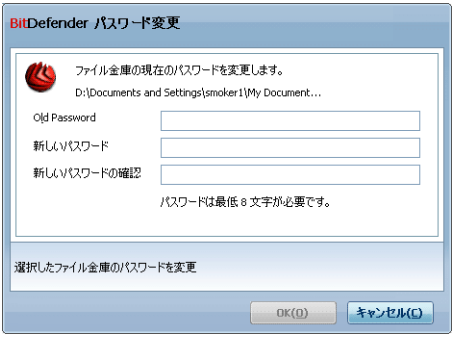
BitDefenderはただちに処理結果をお伝えいたします。 エラーが発生した際、そのエラーメッセージを問題解決に使用してください。 OKをクリックしてウィンドウを閉じます。

### 24.2.4. 金庫のパスワードを変更

パスワードを変更するにはまずその金庫がロックされている必要があります。 金庫のパスワードの変更は次のいずれかを行います：

- テーブルから金庫を選択して パスワードの変更をクリックします。
- 表にある金庫を右クリックしてパスワードの変更を選択します。
- コンピュータ上にある金庫のファイルを右クリックしてBitDefenderファイル金庫にカーソルをあてて 金庫のパスワードを変更を選択。

新しいウィンドウが開きます。




金庫のパスワードを変更

次のように実行します：

1. 現在の金庫のパスワードを古いパスワード欄に入力します。
2. 金庫の新しいパスワードを新しいパスワードと新しいパスワード(確認) 欄に入力します。

**注意**

パスワードは半角で最低で８文字が必要です。 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。

3. OKをクリックするとパスワードが変更されます。

BitDefenderはただちに処理結果をお伝えいたします。 エラーが発生した際、そのエラーメッセージを問題解決に使用してください。 OKをクリックしてウィンドウを閉じます。

### 24.2.5. 金庫にファイルを追加

金庫にファイルを追加するには次の手順でおこないます：

1. 金庫テーブルからファイルを追加したい金庫を選択します。
2. 金庫がロックされている場合、まずそれをオープンする必要があります(右クリックして 金庫をオープン)を選択します。
3. ファイルを追加をクリック。 新しいウィンドウが開きます。
4. 金庫に追加したいファイル/フォルダを選択。
5. OKをクリックして選択したオブジェクトを金庫にコピーします。

いったん金庫がオープンされると、その金庫である仮想ディスクドライブを直接操作することができます。 次の手順に従ってください：

1. マイコンピュータをクリックします （  スタートメニューから マイドキュメント)をクリックします。
2. その金庫に該当する仮想ディスクドライブを入力します。 その金庫をオープンする際に割り当てたドライブ文字をみつけます。
3. その仮想ディスクドライブに直接ファイルやフォルダをコピーペーストまたはドラッグamp;ドロップします。

### 24.2.6. 金庫からファイルを除去

金庫からファイルを除去するには次の手順で行います：

1. 金庫表から除去したいファイルがある金庫を選択します。

2. 金庫がロックされている場合、まずそれをオープンする必要があります(右クリックして 金庫をオープン)を選択します。
3. 金庫の中身を表示している表から除去するファイルを選択します。
4. ファイル／フォルダを削除をクリックします。

金庫がオープンになっている場合は仮想ディスクドライブの金庫から直接ファイルを除去することができます。 次の手順に従ってください：

1. マイコンピュータをクリックします （  スタートメニューから マイドキュメント)をクリックします。
2. その金庫に該当する仮想ディスクドライブを入力します。 その金庫をオープンする際に割り当てたドライブ文字をみつけます。
3. ファイルやフォルダの削除は通常のWindowsの操作で行います（削除したいファイルを右クリックして削除を選択します)。

# 25. 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。

## 25.1. 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。

●BitDefenderファイアウォールは全てを許可に設定されます。 これにより新規の接続は（内向き、外向きであっても）自動的に許可されます。使用されているポートやプロトコルに関係ありません。

●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、上級者モードのゲーム/ノートPCモード>ゲームモードで行います。


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。

### 25.1.1. 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：

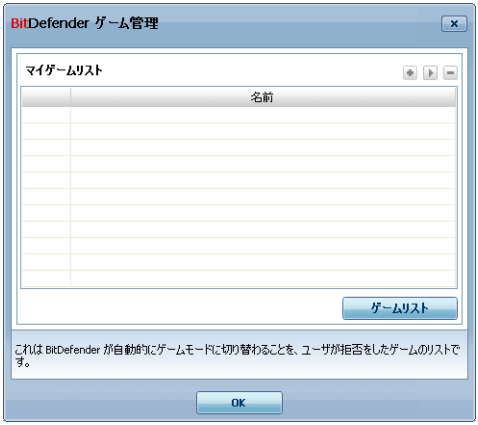
- BitDefenderが提供するデフォルトのゲームリストを使用 - BitDefenderが持っている主要なゲームリストにあるゲームが起動されると自動的にゲームモードに移行します。 このリストを見る場合には、 ゲーム管理 をクリックして、ゲームリストを選択します。
- アプリケーションがフルスクリーン時にゲームモードに移行する - アプリケーションがフルスクリーン表示になった場合に自動的にゲームモードに移行します。
- ゲームリストに追加するかを確認 - フルスクリーンを終えたときにユーザにアプリケーションを追加するかの確認を行います。 ゲームリストに新しいアプリケー

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。

### 25.1.2. 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、ゲームリストをクリックします。
- 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。

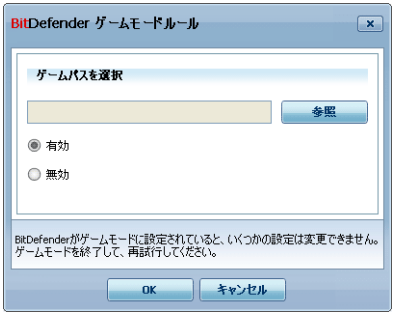
ゲームリストを管理するには、この表の一番上にあるボタンを使用します：

- 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。

## 25.1.3. 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：

- このモジュールを有効にして、アンチウィルススキャンタスクスケジュールを変更します - ゲームモードを実行中にスケジュールされたスキャンタスクを保護します。 以下のオプションから選択できます：

| オプション | 解説 |
|---|---|
| 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。 |

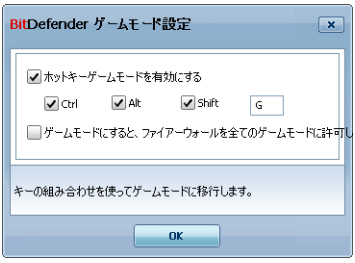
ゲームモードでBitDefenderファイアウォールを自動的に無効にするには次の手順を行います：

1. 詳細設定 新しいウィンドウが開きます。
2. ゲームモード時にファイアーウォールを全て許可(ゲームモード)に設定を選択します。
3. OKをクリックして変更を保存します。

### 25.1.4. 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。

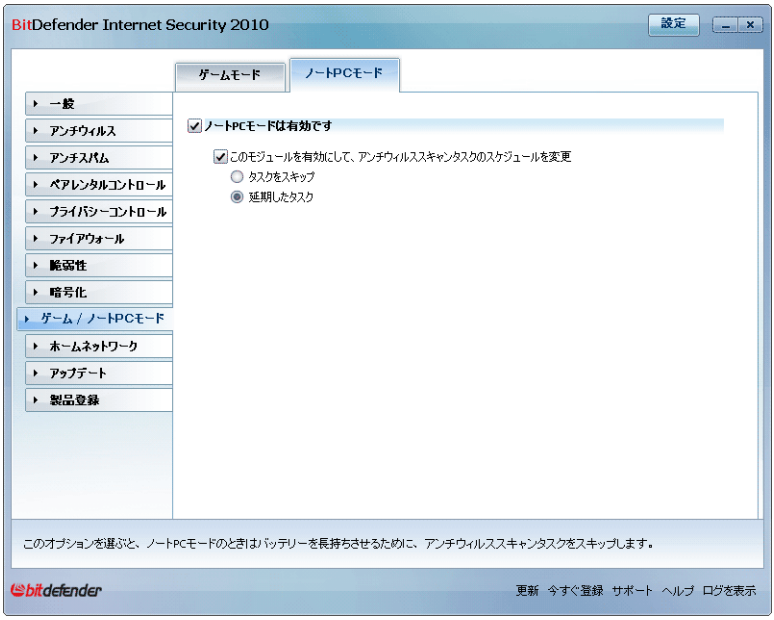
## 25.2. ノートＰＣモード

ノートＰＣモードはノートパソコンユーザ用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、上級者モードのゲーム／ノートPCモード>ノートPCモードで行います。




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。

### 25.2.1. ノートＰＣモードの設定

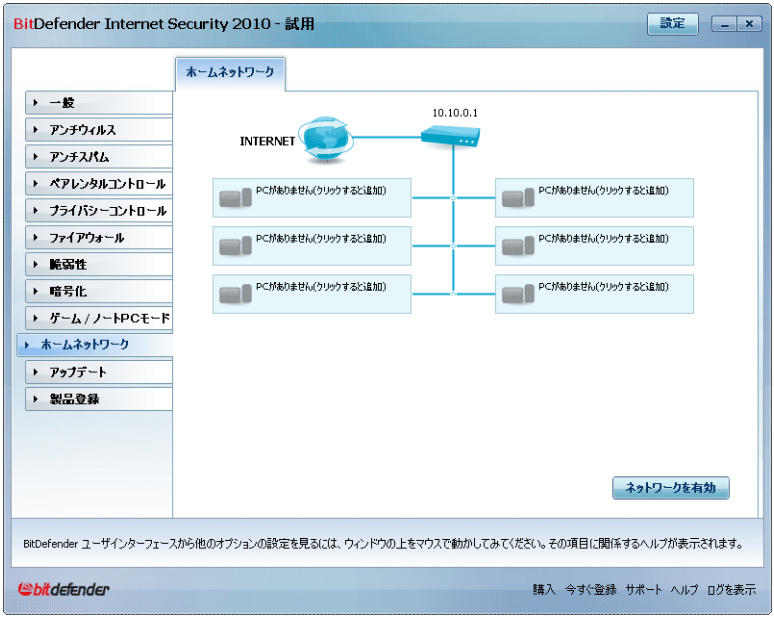
スケジュールタスクのふるまいを設定するには次のオプションを使用します：

- このモジュールを有効にして、アンチウィルススキャンタスクスケジュールを変更します - ノートPCモードを実行中にスケジュールされたスキャンタスクを保護します。 以下のオプションから選択できます：

| オプション | 解説 |
| --- | --- |
| 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 | 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。 |

# 26. ホームネットワーク

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

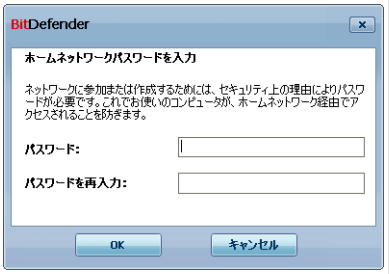
BitDefender製品がインストールされている家庭内のコンピュータを管理するには、次の手順を行ってください：

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

## 26.1. BitDefenderネットワークに参加する

BitDefender ホームネットワークに参加するには、以下の手順に従ってください：

1. ネットワークを有効に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。

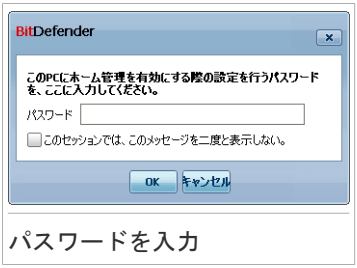
ネットワークマップ上にコンピュータ名が表示されます。

## 26.2. 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。

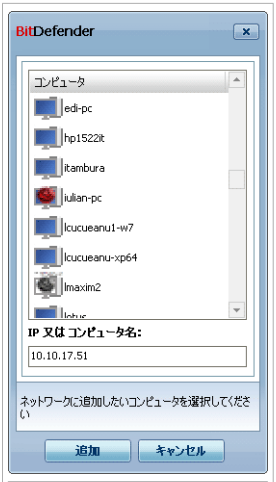
BitDefenderホームネットワークにコンピュータを追加するには、次の手順を行ってください：

1. コンピュータを追加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。

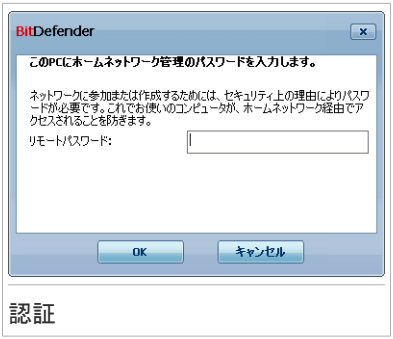



コンピュータを追加

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。



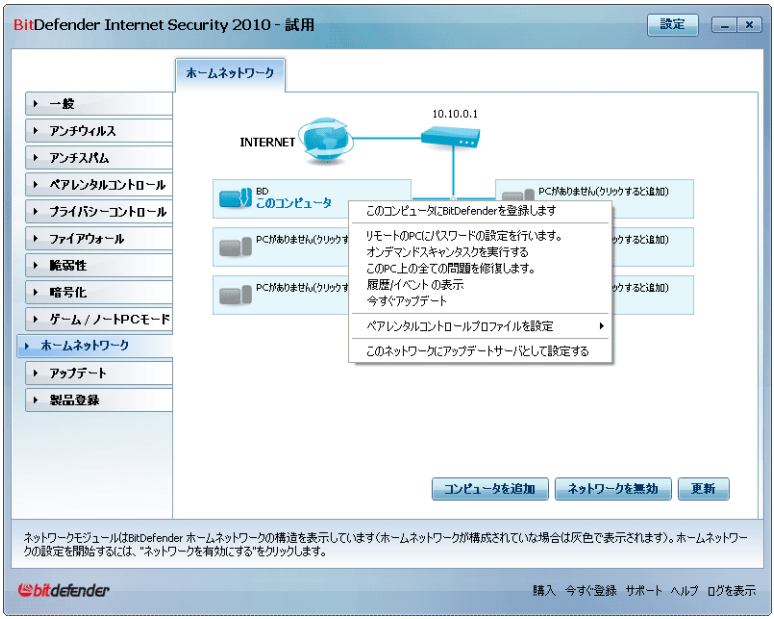

認証

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。

## 26.3. 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クリックすると、リモートコンピュータで実行できる全ての管理作業を確認することができます。

- ホームネットワークからPCを削除

  ネットワークからPCを削除できます。

- このコンピュータにBitDefenderを登録する

  ライセンスキーを入力して、このコンピュータにBitDefenderを登録することができます。

- リモートPCにパスワードを設定する

  パスワードを作成して、このPCでBitDefenderの設定に接続できないように設定します。

- オンデマンドスキャンタスクを実行

リモートコンピュータでオンデマンドスキャンを実行することができます。以下のスキャンタスクを実行することができます：マイドキュメントのスキャン、システムスキャン、完全システムスキャン

- このPCの全ての問題点を修正

  以下の全ての問題を修正ウィザードに従って、このコンピュータのセキュリティに影響を与えている問題を修正することができます。

- 履歴/イベントを表示

  このコンピュータにインストールされているBitDefender製品の、履歴&イベント機能にアクセスすることができます。

- 今すぐアップデートする

  このコンピュータにインストールされているBitDefender製品のアップデート処理を開始してください。

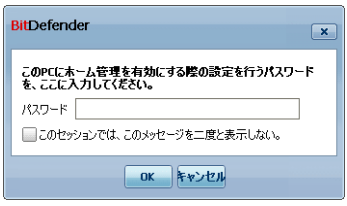
- ペアレンタルコントロールプロファイルの設定

  このコンピュータのペアレンタルコントロールウェブフィルタで使用される年齢カテゴリを設定することができます：子ども、十代の若者、大人

- このネットワークをアップデートサーバに設定

  このネットワーク内のコンピュータにインストールされている全てのBitDefender製品のアップデートサーバとして、このコンピュータを設定することができます。このオプションを使用するとインターネットトラフィックを削減します。なぜならば、ネットワーク内の1つのコンピュータだけがインターネットに接続して、アップデートのダウンロードを行うためです。

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。

# 27. 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：

- アンチウィルスエンジン用アップデート – 新しい脅威が現れた時、今後もそのウィルスから保護するためには、ウィ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ィルス定義のアップデートとも呼ばれます。
- アンチスパムエンジン用アップデート – ヒューリスティックおよびURLフィルタには新しいルールが追加され、イメージフィルタには新しいイメージが追加されます。これにより、アンチスパムエンジンの効率が向上します。このアップデート形式は、アンチスパム用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。

## 27.1. 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、上級者モードのアップデート>アップデートで行います。


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。

### 27.1.1. 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。

### 27.1.2. 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。

## 27.2. 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、上級者モードのアップデート>設定で行います。


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。

## 27.2.1. 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、プロキシを設定をクリックして、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. 277)を参照してください。

### 27.2.2. 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。

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

どのように自動アップデート処理が実行されるか指定するには、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。

### 27.2.3. 手動アップデート設定

手動アップデート（ユーザ請求によるアップデート）を実行する方法を指定するには、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。

### 27.2.4. 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。

### 27.2.5. 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。

プロキシの設定を管理するには、プロキシの設定をクリックします。新しいウィンドウが表示されます。


プロキシマネージャ

プロキシ設定には３種類あります：

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

- カスタムプロキシ - 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。

# 28. 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、上級者モードの製品登録へ進みます。

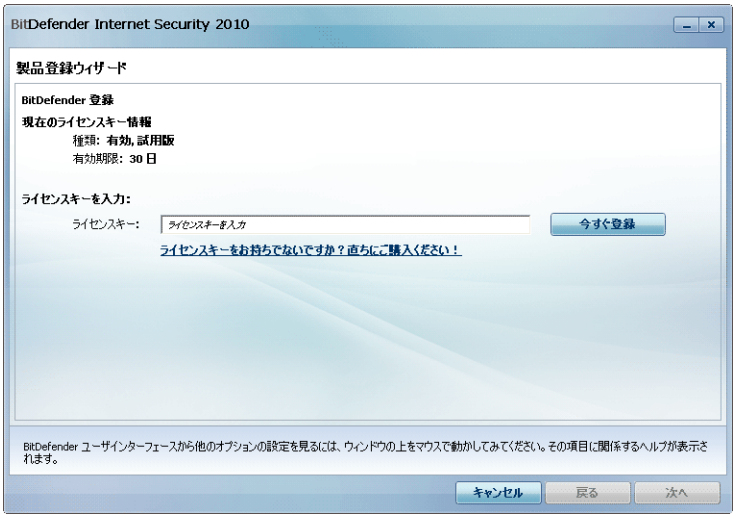

製品登録

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。

## 28.1. BitDefender Internet Security 2010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 登録状況では、お使いのライセンスキーが切れるまでの残日数を確認することができます。

BitDefender Internet Security 2010を登録:

1. ライセンスキーを入力します。

   **注意**
   ライセンスキーは以下に記載されています：
   ●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。

2. 今すぐ登録するをクリックします。
3. 終了をクリックします。

## 28.2. BitDefenderアカウントを作成

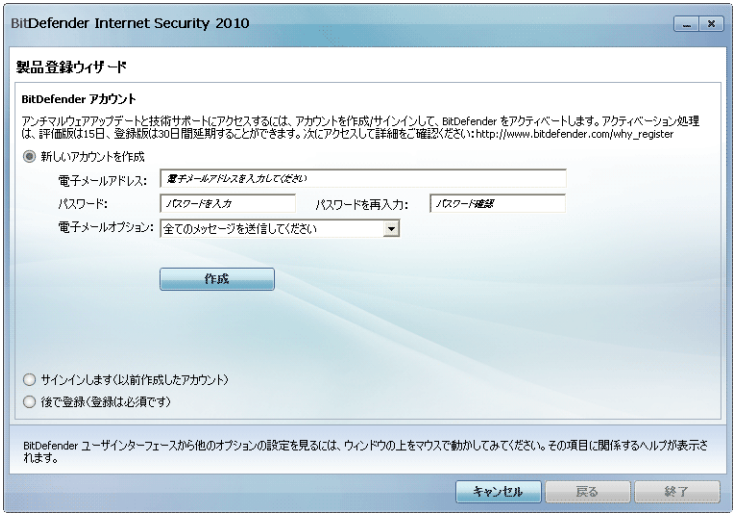
製品登録においてBitDefenderアカウントを作成する必要があります。 BitDefenderアカウントを持つことでBitDefenderの各種アップデート、無料のテクニカルサポート、また製品をお得に購入できるご案内を受けることができます。 登録した電子

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アカウントを作成されていない場合は、 製品をアクティベートをクリックして、アカウント登録画面を開きます。




アカウント作成

もし、いまBitDefenderアカウントを作成されない場合には、後で登録を選択し、終了をクリックしてください。 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. 282）
- 「既にBitDefenderアカウントを持っている場合」（p. 283）

## まだBitDefenderアカウントをお持ちでない場合

正しくBitDefenderアカウントを作成するには、次の手順に従ってください：

1. 新しいアカウントを作成するを選択します。

2. 該当する欄に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。

   注意
   アカウントが有効になると、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からアカウントにログインしてください。

3. 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お客様のメールアドレスに送信することがあります。 メニューから有効なオプションを選択してください：
   ●全てのメッセージを受信
   ●製品に関するメッセージだけを受信
   ●全てのメッセージを受け取らない
4. 作成をクリックしてください。
5. 終了をクリックして、ウィザードを閉じてください。
6. 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。

## 既にBitDefenderアカウントを持っている場合

お客様が既に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、お客様のアカウントのパスワードを入力して、サインインをクリックしてください。 終了をクリックして、ウィザードを閉じてください。

有効なアカウントを持っていて、BitDefenderがそれを検出しない場合は、そのアカウントで製品を登録するために次の手順に従ってください。

1. サインイン（以前に作成されたアカウント）を選択してください。
2. 該当欄にお使いのアカウントの電子メールアドレスとパスワードを入力してください。

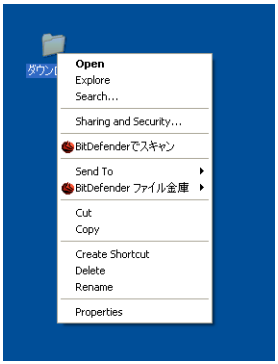
   注意
   パスワードを忘れた場合は、パスワードを忘れたら？をクリックし指示に従ってください。

3. 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お客様のメールアドレスに送信することがあります。 メニューから有効なオプションを選択してください：
   - 全てのメッセージを受信
   - 製品に関するメッセージだけを受信
   - 全てのメッセージを受け取らない
4. サインインをクリックしてください。
5. 終了をクリックして、ウィザードを閉じてください。

# Windowsと第三者ソフトウェアの統合

# 29. 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に統合されていますので、簡単にファイルのウィルススキャンを行うことができ、また他のユーザが重要なファイルにアクセスするのを防ぎます。 コンテキストメニューからBitDefenderの機能を見つけるには BitDefender アイコンを探します。

●BitDefenderでスキャン
●BitDefenderファイル金庫

## 29.1. BitDefender 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）を試みます。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指示します。

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を開いて、ユーザインターフェイスを'上級者モード'に切り替えてください。

2. 左メニューにあるアンチウィルスをクリックします。
3. ウィルススキャン タブをクリックします。
4. 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。
5. 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。
6. OKをクリックして変更を保存します。
7. 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。

**重要項目**
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。

## 29.2. BitDefender ファイル金庫

BitDefenderファイル金庫を使えば、コンピュータ上の重要なドキュメントを安全に格納することができます。

- ファイル金庫は安全な領域で個人情報や重要なファイルを保存するためのものです。
- このファイル金庫はbvd拡張子をもった暗号化されたファイルです。 いったん暗号化されると、その中にあるデータは盗難やセキュリティ違反にも強固になります。
- このbvdファイルをマウントすると、新しい論理パーティション（新しいドライブ）が表示されます。このしくみを理解するには、ISOイメージをVitualCDとしてマウントすることに近いと考えるとわかりやすくなるとおもいます。

  マイコンピュータを開くと、新しいドライブがファイル金庫として表示されています。この中でファイル操作（コピー、削除、変更など）ができます。ここにあるファイルは、このドライブの中にある限り守られています（それはマウント時にパスワードが必要だからです）。

  終了したらそのファイル金庫をロック（アンマウント）して内容の防御を開始します。

コンピュータ上にあるBitDefenderファイル金庫は、 BitDefender アイコンと.bvd拡張子を持っています。

注意

ここではWindowsコンテキストメニューにある機能を使ってBitDefenderファイル金庫を作成し管理する方法を説明します。 ファイル金庫はBitDefenderの画面から作成して管理することもできます。

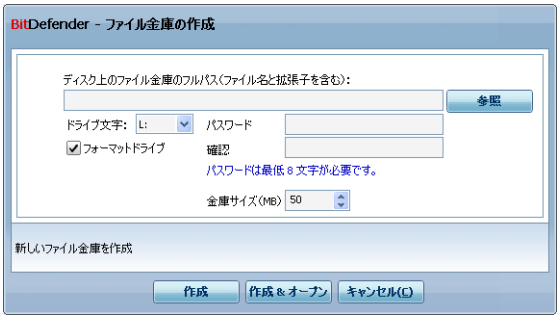
- 中級者モードで、 ファイル金庫 タブを開いて、クイックタスク領域にあるオプションを使います。 ウィザードを使って各タスクを実行することができます。
- より簡単な方法として、上級者モードに切り替えて左メニューから 暗号化 をクリックします。 ファイル暗号化 タブで、既存のファイル金庫とその中身を確認、管理できます。

### 29.2.1. ファイル金庫を作成

金庫は実際には .bvd 拡張子をもったファイルにすぎません。 ファイル金庫を開いたとき、仮想ドライブがマイコンピュータ内に表示され、そこにファイルを安全に格納することができます。 金庫を作成したとき、コンピュータにどこに、どの名前で保存するかを指定します。またパスワードを指定して、内容を守ります。 パスワードを知っている人だけが金庫をオープンして、中にあるドキュメントやデータにアクセスすることができます。

金庫を作成するには次の手順を行います：

1. デスクトップ上またはコンピュータにあるフォルダで右クリックしてBitDefenderファイル金庫にカーソルを当ててファイル金庫を作成を選択します。 以下のウィンドウが開きます：




ファイル金庫の作成

2. 場所と金庫ファイルの名前を指定。
   - 閲覧をクリックして金庫の場所を選択し、任意のファイル名で保存します。

- 該当欄に金庫名を入力してマイドキュメントに作成します。 マイドキュメントを開くために、 start スタートメニューをクリックしてマイドキュメントをクリックします。
- ディスク上の金庫ファイルまでのフルパスを入力。 例えば、C:¥my_vault.bvd

3. メニューからドライブ文字を選択。 金庫をオープンと、マイコンピュータ上に選択したドライブ名で仮想ディスクドライブが表示されます。
4. 金庫の新しいパスワードを新しいパスワード 及び 新しいパスワード(確認) 欄に入力します。 金庫を開いたり、そのファイルにアクセスする際には必ずパスワードが要求されます。
5. ドライブのフォーマット を選択すると金庫の仮想ドライブがフォーマットされます。 その金庫にファイルを追加する前にドライブをフォーマットする必要があります。
6. デフォルトの金庫のサイズ(50 MB) を変更するには、金庫のファイルフィールドでサイズを入力します。
7. 作成 をクリックすると、その選択した場所に金庫を作成します。 マイコンピュータ上に仮想ディスクドライブとして金庫を作成して表示するには 作成&オープン をクリックします。

BitDefenderはただちに処理結果をお伝えいたします。 エラーが発生した際、そのエラーメッセージを問題解決に使用してください。 OKをクリックしてウィンドウを閉じます。

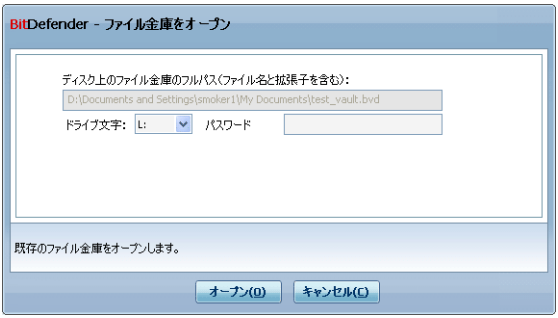
**注意**
すべてのファイル金庫を同じ場所に保存すれば、すぐにみつけることができるので便利です。

## 29.2.2. ファイル金庫をオープンする

金庫にあるファイルにアクセスして作業するためには、必ずその金庫をオープンしなければなりません。 金庫をオープンすると仮想ディスクドライブがマイコンピュータ上に現れます。 このドライブは金庫に割り当てられたドライブ名で表示されます。

金庫をオープンするには次の手順を行います :

1. コンピュータ内にあるオープンしたい金庫の .bvd ファイルを探します。
2. このファイルを右クリックしてBitDefenderファイル金庫 にカーソルを当て、オープンを選択します。 またはそのファイルをダブルクリックまたは、右クリックして オープンを選択すればよりはやく利用できるようになります。 以下のウィンドウが開きます :




ファイル金庫をオープン

3. メニューからドライブ文字を選択。
4. 金庫にかけるパスワードをパスワードフィールドに入力します。
5. 開くをクリックしてください。

BitDefenderはただちに処理結果をお伝えいたします。 エラーが発生した際、そのエラーメッセージを問題解決に使用してください。 OKをクリックしてウィンドウを閉じます。

### 29.2.3. ファイル金庫をロック

ファイル金庫での作業を終えたら、かならずデータを守るためロックする必要があります。 ファイル金庫をロックすることで、その金庫ディスクドライブはマイコンピュータから消えます。それに伴い、この金庫に格納されているデータへのアクセスは完全にブロックされます。

金庫をロックするためには次の手順を行います：

1. マイコンピュータをクリックします （ start スタートメニューから マイドキュメント)をクリックします。
2. ロックしたい仮想ディスクドライブを指定します。 その金庫をオープンする際に割り当てたドライブ文字をみつけます。
3. 該当する仮想ディスクドライブを右クリックして、BitDefender ファイル金庫にカーソルをあてて ロックをクリックします。

ファイル金庫を表す.bvdを右クリックすることもでき、BitDefenderファイル金庫を示して、 終了をクリックします。

BitDefenderはただちに処理結果をお伝えいたします。 エラーが発生した際、そのエラーメッセージを問題解決に使用してください。 OKをクリックしてウィンドウを閉じます。

注意

もし複数の金庫がオープンしている場合には、BitDefender上級者モード画面を使用します。 暗号化, ファイル暗号化 タブで、既存の金庫について表示しているテーブルをみることができます。この情報にはどの金庫がオープンされているか、及びドライブ文字の内容が含まれています。

### 29.2.4. ファイル金庫に追加

金庫にファイルやフォルダを追加する前に、この金庫をオープンしておく必要があります。 金庫がオープンしている状態では、コンテキストメニューを使ってファイルやフォルダを簡単に追加することができます。 金庫にコピーしたいファイルやフォルダを右クリックしてBitDefender ファイル金庫 、 ファイル金庫に追加を指示します。

- もし金庫が１つだけオープンしている場合は、ファイルやフォルダはそのまま金庫にコピーされます。
- 複数の金庫がオープンしている場合は、どの金庫にコピーするか選択を求められます。メニューからのドライブ文字を選択して OK をクリックして項目をコピーします。

その金庫がオープンしてできた仮想ディスクドライブを使うことができます。 次の手順に従ってください：

1. マイコンピュータをクリックします （ start スタートメニューから マイドキュメント)をクリックします。
2. その金庫に該当する仮想ディスクドライブを入力します。 その金庫をオープンする際に割り当てたドライブ文字をみつけます。
3. その仮想ディスクドライブに直接ファイルやフォルダをコピーペーストまたはドラッグamp;ドロップします。

### 29.2.5. ファイル金庫から削除

ファイル金庫からファイルやフォルダを除去するためには、金庫がオープンされていなければなりません。 金庫からファイルを除去するには次の手順で行います：

1. マイコンピュータをクリックします （ start スタートメニューから マイドキュメント)をクリックします。
2. その金庫に該当する仮想ディスクドライブを入力します。 その金庫をオープンする際に割り当てたドライブ文字をみつけます。

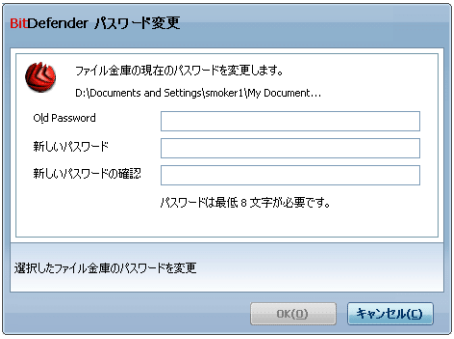
3. ファイルやフォルダの削除は通常のWindowsの操作で行います（削除したいファイルを右クリックして削除を選択します）。

### 29.2.6. 金庫のパスワードを変更

パスワードによって金庫の中身は許可されていないアクセスから守られます。 パスワードを知っている人だけが金庫をオープンして、中にあるドキュメントやデータにアクセスすることができます。

パスワードを変更するにはまずその金庫がロックされている必要があります。 金庫のパスワードの変更は次手順で行います：

1. コンピュータ内にあるその金庫に該当する .bvd ファイルを探します。
2. このファイルを右クリックしてBitDefenderファイル金庫　にカーソルを当て、金庫のパスワードを変更を選択します。 以下のウィンドウが開きます：




金庫のパスワードを変更

3. 現在の金庫のパスワードを古いパスワード欄に入力します。
4. 金庫の新しいパスワードを新しいパスワードと新しいパスワード(確認）欄に入力します。

> **注意**
>
> パスワードは半角で最低で８文字が必要です。 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。

5. OKをクリックするとパスワードが変更されます。

BitDefenderはただちに処理結果をお伝えいたします。 エラーが発生した際、そのエラーメッセージを問題解決に使用してください。 OKをクリックしてウィンドウを閉じます。

# 30. 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。

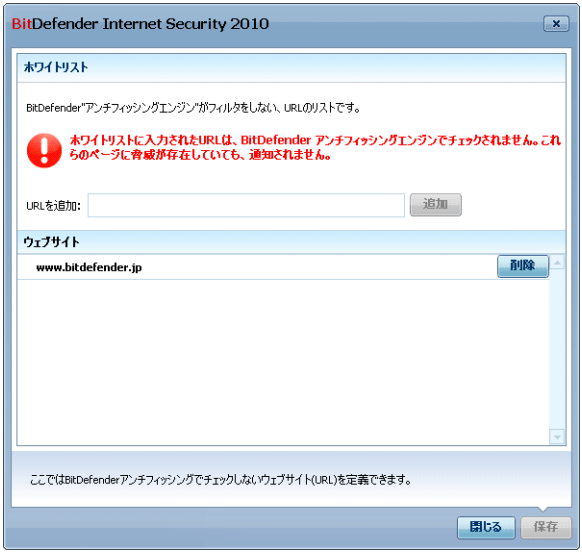

アンチフィッシングツールバー

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 – 現在のウェブブラウザで、BitDefenderアンチフィッシングプロテクションの有効／無効を切り替えます。
- 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 – ホワイトリストを開きます。




アンチフィッシング 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。

# 31. インスタントメッセンジャープログラムへの統合

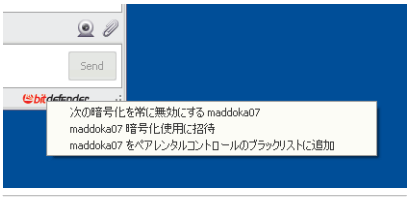
BitDefenderでは重要なドキュメントやYahoo! MessengerやMSNメッセンジャーでの会話を暗号化することができます。

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せす。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：

- 永久的に次のコンタクトの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。
- コンタクト先 をペアレンタルコントロールのブラックリストに追加. コンタクト先をペアレンタルコントロールのブラックリストに追加後、ペアレンタルコントロールが有効になっている場合は、これ以上そのコンタクト先からのインスタントメッセージを受け取ることができません。 ブラックリストからコンタクト先を除去するには、ツールバーをクリックして 削除連絡先をペアレンタルコントロールリストから選択します。

# 32. メールクライアントとの連携

BitDefender Internet Security 2010 にはアンチスパムモジュールがあります。アンチスパムは受信したメッセージを検査して、それらがスパムであると特定します。 BitDefenderにスパムメッセージを検知すると件名の先頭に[SPAM] を付けます。

**注意**
アンチスパム保護は全てのPOP3/SMTPメールクライアントに対応しています。

BitDefenderは直観的な使いやすいツールバーを通して、以下のメールクライアントに統合されます：

- Microsoft Outlook
- Outlook Express
- Windows Mail
- Mozilla Thunderbird

BitDefenderは自動的にスパムメッセージを特定のフォルダに移動します：

- Microsoft Outlookではスパムメッセージは 迷惑メール フォルダに移動します。そのフォルダは 削除済み項目 フォルダにあります。 The スパム フォルダはBitDefenderのインストール時に作成されます。
- Outlook Express と Windows Mailではスパムメッセージは直接削除済み項目に移動されます。
- Thunderbirdではスパムメッセージは スパム フォルダに移動されます。そのフォルダは ごみ箱 フォルダにあります。 The スパム フォルダはBitDefenderのインストール時に作成されます。

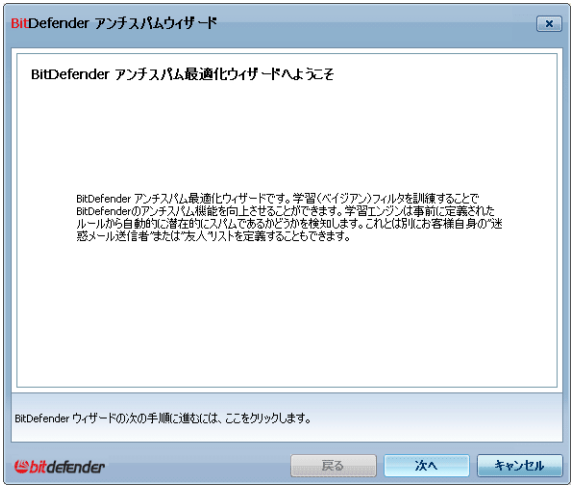
他のメールクライアントを使用している場合には、ルールを作成してメールメッセージにBitDefenderが[SPAM] とつけられたものを適当な隔離フォルダに移動するようにしなければなりません。

## 32.1. アンチスパム設定ウィザード

BitDefenderをインストール後、初めてメールクライアントを起動した時、迷惑メール対策フィルタの効率を上げるため友人リストおよびスパマーリスト の作成とベイジアンフィルタトレーニングを行うウィザードが表示されます。

**注意**
ウィザードは、ウィザード ボタン（ アンチスパムツールバー内）をクリックすれば、いつでも起動できます。

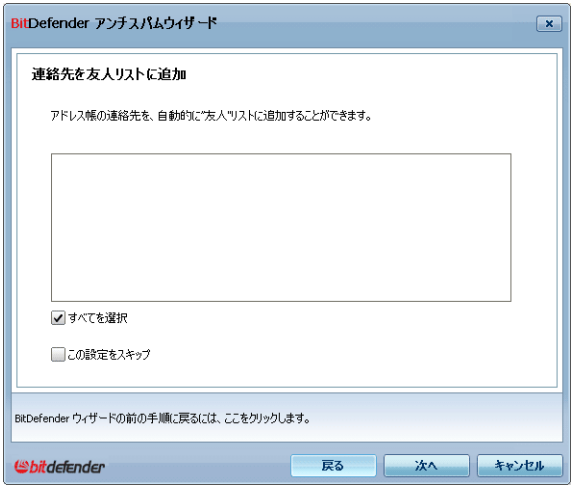
### 32.1.1. 手順 1/6 - はじめに




はじめに

次へをクリックします。

### 32.1.2. 手順 2/6 - 友人リストに登録



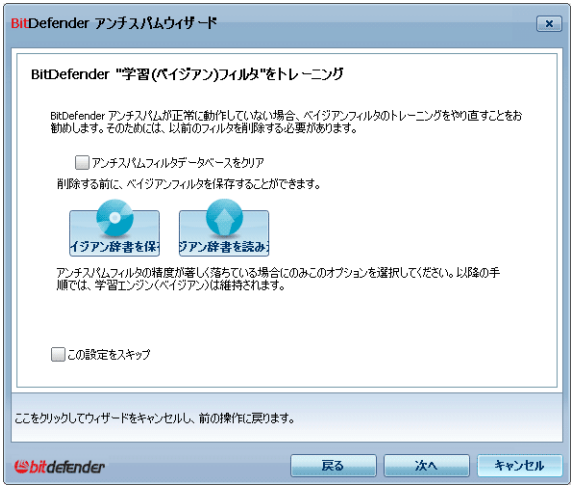

友人リストに登録します。

アドレス帳のすべてのアドレスをここで確認できます。友人リストに追加したい項目を選択してください（すべてを選択することをお勧めします）。追加したアドレスからは内容に関わらずすべてのメールメッセージを受け取ります。

すべてのアドレスを友人リストへ追加するにはすべてを選択をチェックします。

この設定をスキップしたい場合は、この手順をスキップするを選択します。 次へをクリックしてください。

### 32.1.3. 手順 3/6 - ベイジアンデータベースを削除




ベイジアンデータベースを削除

迷惑メール対策フィルタの精度が下がってくる可能性があります。これはおそらく、不適切な学習を行ったことが原因です（つまり、多くの通常メールメッセージを迷惑メールとしたり、その逆を行ったということです）。フィルタの精度が下がった場合は、フィルタデータベースを削除して、このウィザードの次の手順に従って再度学習させてください。

ベイジアンデータベースをリセットしたい場合はアンチスパムフィルタデータベースを消去を選択します。

ベイジアンデータベースをファイルに保存できるので、それを他のBitDefender製品や、BitDefenderの再インストール後に使用することができます。 ベイジアンデータベースを保存するには、 フィルタを保存ボタンをクリックして、お好きな場所に保存します。 このファイルは.dat拡張子が付いています。

以前に保存したベイジアンデータベースを読み込むには、フィルタをロードボタンをクリックして、該当するファイルを開きます。

この設定をスキップしたい場合は、この手順をスキップするを選択します。 次へをクリックしてください。

### 32.1.4. 手順 4/6 - 通常メールでベイジアンフィルタを訓練


ベイジアンフィルタを通常メールで訓練

通常のメールメッセージが保存されたフォルダを選択してください。これらのメッセージがアンチスパムフィルタの学習に使用されます。

ディレクトリー覧の下に２つの詳細オプションがあります：

- 全てのサブフォルダを含む - 選択対象のサブフォルダを含めます。
- 自動的に友人リストに追加する - 送信者を友人リストに追加します。

この設定をスキップしたい場合は、この手順をスキップするを選択します。 次へをクリックしてください。

### 32.1.5. 手順 5/6 - ベイジアンフィルタを迷惑メールで訓練


ベイジアンフィルタを迷惑メールで訓練

迷惑メールメッセージが保存されているフォルダを選択してください。これらのメッセージが迷惑メールフィルタの学習に使用されます。

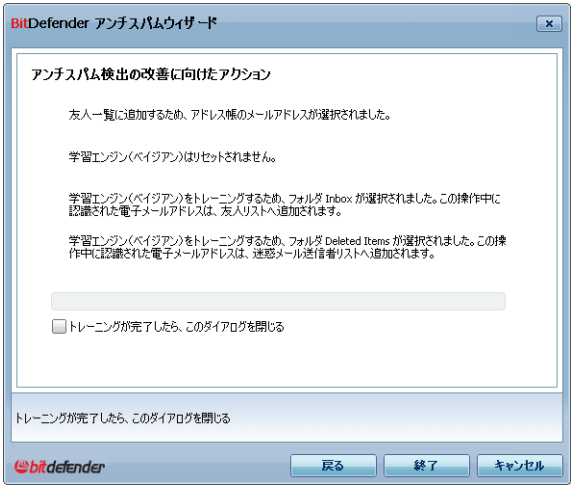
**重要項目**
選択したフォルダに通常メールが含まれていないことを確認してください。含まれているとアンチスパム機能の精度が目に見えて低下します。

ディレクトリー覧の下に２つの詳細オプションがあります：

- 全てのサブフォルダを含む - 選択対象のサブフォルダを含めます。
- 自動的に迷惑メール送信者リストに追加する - 送信者を迷惑メール送信者リストに追加します。 これらの送信者からの電子メールメッセージは、常に迷惑メールとしてマークされて、処理が実行されます。

この設定をスキップしたい場合は、この手順をスキップするを選択します。 次へをクリックしてください。

### 32.1.6. 手順 6/6 - まとめ



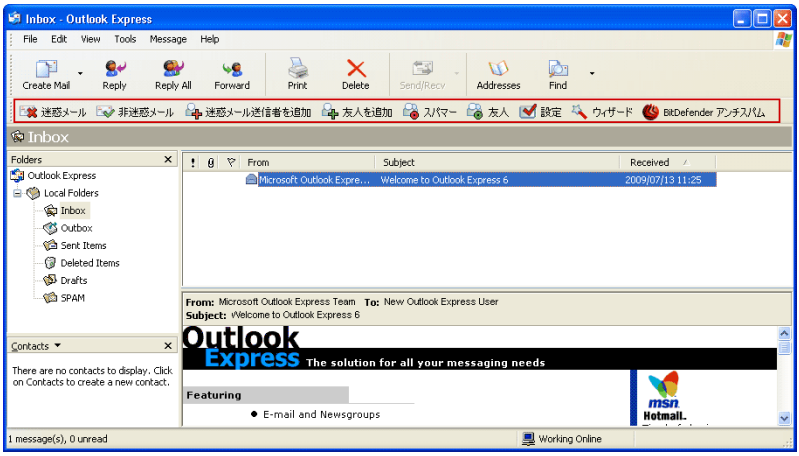

概要

設定ウィザードで行ったすべての設定をここで確認できます。前の手順へ戻って変更することもできます（戻るをクリックしてください）。

変更を加える必要がなければ終了をクリックしてウィザードを終了してください。

## 32.2. アンチスパムツールバー

お使いのメールクライアントの上部に、アンチスパムツールバーが表示されます。アンチスパムツールバーによって、メールクライアントから直接、アンチスパム保護を操作管理することができます。 正しいメッセージをBitDefenderがスパムと判断した場合、それを簡単に修正することができます。




アンチスパムツールバー

BitDefenderツールバーの各ボタンの説明を、以下に示します：

- 迷惑メール – メッセージをベイジアンモジュールへ送り、選択されたメールが迷惑メールであることを伝えます。メールはSPAMとタグされ、Spamフォルダへ移動されます。

  今後受け取る同じパターンを持つメールは、次からはSPAMとタグされます。

  **注意**
  メールメッセージは１つあるいは必要なだけ選択できます。

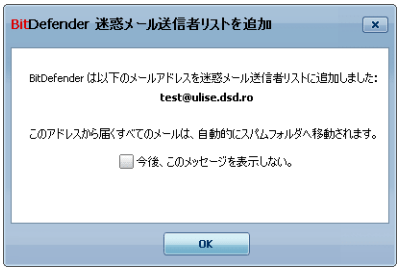
- 非迷惑メール – メッセージをベイジアンモジュールに送り、選択されたメールはBitDefenderがタグするべき迷惑メールではなかったことを伝えます。 電子メールは迷惑メールフォルダから、受信箱のディレクトリに移動されます。

  今後受け取る同じパターンを持つメールは、次からはSPAMとはタグされません。

  **注意**
  メールメッセージは１つあるいは必要なだけ選択できます。

  **重要項目**
  非迷惑メールボタンはBitDefenderがスパム（迷惑メール）からマークを外すことができます（これらのメールは迷惑メール フォルダにあります）

● 迷惑メール送信者を追加 – 選択した電子メールの送信者を迷惑メール送信者リストに追加します。




迷惑メール送信者を追加

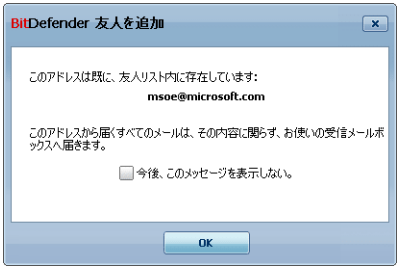
迷惑メール送信者のアドレスを一覧に追加する時、確認されないようにするには、今後このメッセージを表示しないを選択します。

OKをクリックしてウィンドウを閉じます。

今後このアドレスから届くメールメッセージは、SPAMとタグされます。

注意
送信者は１人あるいは必要なだけ選択できます。

● 友人リストに追加する – 選択した電子メールの送信者を友人リストに追加します。




友人を追加

友人のアドレスを一覧に追加する時に確認されないようにするには、今後このメッセージを表示しないを選択します。

OKをクリックしてウィンドウを閉じます。

このアドレスから届くメールメッセージは、その内容に関わらず常に受け取ります。

注意
送信者は１人あるいは必要なだけ選択できます。

- 迷惑メール送信者リストは、その内容に関わらずお客様がメッセージを一切受け取りたくないすべての電子メールアドレスの一覧です。

**注意**
迷惑メール送信者リストのアドレスから受け取ったメールはすべて、それ以降の処理なしに自動的にSPAMとマークされます。


スパマーリスト

スパマーリストの項目追加や削除を、ここで行うことができます。

メールアドレスを追加する場合は、メールアドレスオプションにチェックし、アドレスを入力して、ボタンをクリックします。アドレスがスパマーリストに表示されます。

**重要項目**
構文：name@domain.com

ドメインを追加するには、ドメイン名オプションにチェックし、ドメインを入力して、ボタンをクリックします。ドメインがスパマーリストに表示されます。

**重要項目**
構文：

- @domain.com, *domain.com, domain.com - domain.comから届いたすべての受信メールメッセージに、SPAMタグが付加されます；
- *domain* - domainから届いたすべての受信メールメッセージ（ドメイン末尾に関わらず）に、SPAMタグが付加されます；
- *com - ドメイン末尾がcomのすべての受信メールメッセージにSPAMタグが付加されます；

警告

正当なウェブベースの電子メールサービスのドメインを迷惑メール送信者一覧に追加しないでください。（Yahoo、Gmail、Hotmail等） さもなければ、このようなサービスに登録しているユーザから受信した電子メールメッセージは、迷惑メール送信者として検出されてしまいます。 例えば、yahoo.comを迷惑メール送信者一覧に追加すると、 yahoo.com から送信された全ての電子メールメッセージが[spam]として区別されてしまいます。

メールアドレスをWindowsのアドレス帳 / Outlook Express フォルダからMicrosoft Outlook / Outlook Express / Windows Mailへ読み込むには、メールアドレスの読み込み元ドロップダウンメニューから適切なオプションを選択します。

Microsoft Outlook Express / Windows Mailでは新しいウィンドウが表示され、そこでスパマーリストに追加したいメールアドレスが保存されたフォルダを選択できます。選んだら選択をクリックします。

どちらの場合もメールアドレスは、読み込み一覧に表示されます。追加したい項目を選び、をクリックしてスパマーリストに追加します。をクリックするとすべてのメールアドレスが一覧に追加されます。

一覧から項目を削除するには、それを選択して、削除ボタンをクリックします。一覧から全ての項目を削除するには、一覧を削除するボタンをクリックして、はいを選択します。

迷惑メール送信者リストをファイルに保存することができるので、それを別のコンピュータや製品の再インストール後に使用することができます。 迷惑メール送信者リストを保存するには、保存ボタンをクリックして、お好きな場所に保存します。 このファイルは.dat拡張子が付いています。

以前保存した迷惑メール送信者リストを読み込むには、読み込むボタンをクリックして、.bwl ファイルを開きます。 以前保存した一覧を読み込んだ際に、現在の一覧の内容をリセットするには、現在の一覧を上書きするを選択してください。

適用およびOKをクリックしてスパマーリストを保存して閉じます。

- 友人 - 内容に関わらず常に受け取りたいメールメッセージの送信者アドレスがすべて保管された友人リストを開きます。

**注意**
友人リストのアドレスから届いたメールはすべて、それ以上の処理は行われずに自動的に受信ボックスへ届きます。


友人リスト

友人リストの項目追加または削除をここで行うことができます。

メールアドレスを追加したい場合はメールアドレスオプションにチェックし、アドレスを入力して⊠ボタンをクリックします。アドレスが友人リストに表示されます。

**重要項目**
構文：name@domain.com

ドメインを追加するにはドメイン名オプションにチェックし、ドメインを入力して⊠ボタンをクリックします。ドメインが友人リストに表示されます。

**重要項目**
構文：

- @domain.com, *domain.com, domain.com - domain.comから受信したメールメッセージはすべて、その内容に関わらず受信ボックスに届きます；
- *domain* - domainから受信したメールメッセージはすべて（その末尾が何であれ）その内容に関わらず受信ボックスに届きます；

- *com - comで終わるドメインを持つ受信メールメッセージはすべて、その内容に関わらず受信ボックスに届きます ;

メールアドレスをWindowsのアドレス帳 / Outlook Express フォルダからMicrosoft Outlook / Outlook Express / Windows Mailへ読み込むには、メールアドレスの読み込み元ドロップダウンメニューから適切なオプションを選択します。

Microsoft Outlook Express/Windows Mailの場合は新しいウィンドウが表示され、そこで友人リストに追加したいメールアドレスが保存されたフォルダを選択できます。対象を選び選択をクリックします。

どちらの場合もメールアドレスは読み込み一覧に表示されます。追加したい項目を選んで▸をクリックし友人リストに追加します。▸▸をクリックするとすべてのメールアドレスが一覧に追加されます。

一覧から項目を削除するには、それを選択して、削除ボタンをクリックします。一覧から全ての項目を削除するには、一覧を削除するボタンをクリックして、はいを選択します。

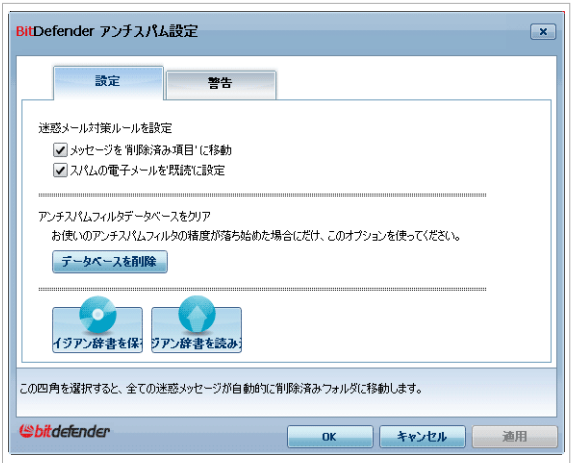
友人リストをファイルに保存することができるので、それを別のコンピュータや製品の再インストール後に使用することができます。　友人リストを保存するには、保存ボタンをクリックして、お好きな場所に保存します。 このファイルは.dat拡張子が付いています。

以前保存した友人リストを読み込むには、読み込むボタンをクリックして、.bwlファイルを開きます。 以前保存した一覧を読み込んだ際に、現在の一覧の内容をリセットするには、現在の一覧を上書きするを選択してください。

**注意**
友人の名前およびメールアドレスを友人リストに追加することをお勧めします。BitDefenderはそのリストに記載された送信者からのメッセージはブロックしません ; 従って、友人を追加すると信頼できるメッセージの届く精度が向上します。

適用およびOKをクリックして友人リストを保存して閉じます。

- 設定 - 設定ウィンドウが開き、そこでアンチスパムモジュールに対するオプションを指定できます。




設定

以下のオプションを指定できます：

- メッセージを削除された項目へ移動 - 迷惑メールを削除された項目（Microsoft Outlook Express/Windows Mailの場合のみ）に移動します；
- メッセージを'既読'マーク - 新しい迷惑メールが届いても煩わされないようにすべての迷惑メールを既読とマークします。

お使いのアンチスパムフィルタの精度が低い場合、フィルタデータベースを一度消去してベイジアンフィルタを再度学習させた方がよいかもしれません。アンチスパムデータベースを消去するにはベイジアンデータベースをリセットを選択してください。

ベイジアンデータベースをファイルに保存できるので、それを他のBitDefender製品や、BitDefenderの再インストール後に使用することができます。 ベイジアンデータベースを保存するには、 フィルタを保存ボタンをクリックして、お好きな場所に保存します。 このファイルは.dat拡張子が付いています。

以前に保存したベイジアンデータベースを読み込むには、フィルタをロードボタンをクリックして、該当するファイルを開きます。

警告（アラート）タブでは 迷惑メール送信者として追加と 友達に追加ボタンの確認ウィンドウを無効にすることができます。

**注意**
警告ウィンドウではメールメッセージを１通選択してください警告の表示も有効/無効に設定できます。メールメッセージを１通でなくグループで選択すると、この警告は表示されます。

- ウィザード - アンチスパム設定ウィザードを開くと、BitDefenderアンチスパムフィルタリングをより一層使いこなすための、ベイジアンフィルタの使い方を手助けします。 アドレス帳のアドレスを、友人リスト/迷惑メール送信者リスト、に追加することもできます。
- BitDefenderアンチスパム - BitDefenderユーザインターフェースを開きます。

方法

# 33. 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. 57)

## 33.1. 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疑われる場合。
- インターネットからダウンロードしたファイルで危険だと疑われる場合。
- 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する場合。

## 33.2. 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。 ユーザインターフェースの設定ごとに、スキャンタスクを実行する手順が異なります。

### 初級者モードでスキャンタスクを実行する

初級者モードでは、今すぐスキャンをクリックすると、コンピュータ全体に標準レベルのスキャンを実行できます。 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。

## 中級者モードでスキャンタスクを実行する

中級者モードで、事前に設定した複数のスキャンタスクを実行することができます。カスタムスキャンタスクを設定及び実行し、カスタムスキャンオプションを使用して、お使いのコンピュータ上で、指定した場所をスキャンします。 中級者モードでのスキャンタスクの実行手順：

1. セキュリティタブをクリックします。
2. クイックタスクの左側で、システムスキャンをクリックして、 コンピュータ全体を標準レベルでスキャンを開始します。別のスキャンタスクを実行するには、 にある矢印をクリックして、対象のスキャンタスクを選択します。 カスタムスキャンの設定及び実行は、カスタムスキャンをクリックしてください。 利用可能なスキャンタスク：

| スキャンタスク | 解説 |
|---|---|
| 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。デフォルト設定では、 ルートキット以外の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、ウィルス，スパイウェア，アドウェア，ルートキット 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 | 現在の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。 |
| カスタムスキャン | このオプションは、カスタムスキャンタスクの設定と実行が可能です。スキャンの内容、標準のスキャンオプションの指定をすることができます。 カスタムスキャンタスクを保存することができ、後に中級者モードや上級者モードでそこにアクセス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。 カスタムスキャンの実行を選択すると、代わりにカスタムスキャンウィザードを全て行う必要があります。

### 上級者モードでスキャンタスクを実行する

上級者モードでは、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。 上級者モード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 | 解説 |
|---|---|
| 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、ウィルス，スパイウェア，アドウェア，ルートキット 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。 |
| 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。デフォルト設定では、 ルートキット以外の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 | 現在の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。

## 33.3. 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。 もしシステムが強力な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 2010 → BitDefender手動スキャン. 新しいウィンドウが開きます。
2. フォルダを追加をクリックして、スキャン対象を選択してください。 新しいウィンドウが開きます。
3. 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。
4. OKをクリックします。
5. 継続をクリックして、スキャンを開始します。
6. 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。

## 33.4. スキャンアクティビティバーを使う

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。 この小さなウィンドウは、デフォルトで、上級者モードにのみ有効です。

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. 33)を参照してください。

# 34. 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を開いて、ユーザインターフェイスを'上級者モード'に切り替えてください。
2. 左メニューにあるアンチウィルスをクリックします。
3. 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 | 解説 |
|---|---|
| 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、ウィルス，スパイウェア，アドウェア，ルートキット 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。 |
| 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。デフォルト設定では、 ルートキット以外の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。 |

| デフォルトタスク | 解説 |
| --- | --- |
| マイドキュメント | 現在の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。

4. 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。
5. 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。
6. 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。

# トラブルシューティングとヘルプ機能

# 35. トラブルシューティング

この章では、お客様がBitDefenderのご利用時に遭遇するかもしれない問題を取り上げ、その対処方法を記載しています。多くの問題は、正しい製品設定によって解決されます。

ここにお客様の問題が記載されていない場合、又は記載されている問題が解決しない場合は、次の章にある BitDefender 技術サポートまでお問い合わせください「サポート」 (p. 338)。

## 35.1. インストールの問題

この項目では、BitDefenderで共通するインストールに関する問題の解決策を提供します。 これらの問題は、以下のカテゴリ内にグループ化されます：

- **インストールの検証エラー**:セットアップウィザードは、お使いのシステムに特定の条件があるため、実行することができません。
- **インストールの失敗**: セットアップウィザードからインストールを開始しましたが、インストールに失敗しました。

### 35.1.1. インストールの検証エラー

セットアップウィザードを開始すると、多くの条件が検証されて、インストールが開始できるかどうかの確認を行います。 以下の表では、最も共通するインストールの検証エラー、及びそれに対する解決策を表示しています。

| エラー | 説明&解決策 |
|---|---|
| お客様は、プログラムをインストールするための権限を持っていません。 | 設定ウィザードを実行して、BitDefenderをインストールするには、管理者の権限が必要になります。 次の操作が行えます：<br>●Windows管理者のアカウントにログオンして、再度設定ウィザードを実行します。<br>●インストールファイルを右クリックして、管理者として実行するを選択します。 ユーザ名とシステムのWindows管理者のアカウントのパスワードを入力してください。 |
| インストーラが、正しくアンインストールされなかった以前のBitDefenderバージョンを検出しました。 | 以前BitDefenderがお使いのシステムにインストールされていましたが、正しくアンインストールされませんでした。そのため新しいBitDefenderをインストールすることができません。 |

| エラー | 説明&解決策 |
| --- | --- |
| | このエラーを解決して、BitDefenderをインストールするには、次の手順に従ってください：<br>1. www.bitdefender.com/uninstallをクリックして、お使いのコンピュータにアンインストールツールをダウンロードしてください。<br>2. 管理者権限を使用して、アンインストールツールを実行してください。<br>3. コンピュータを再起動してください。<br>4. 再度、設定ウィザードを起動して、BitDefenderをインストールしてください。 |
| BitDefender製品は、お使いのオペレーティングシステムと互換性がありません。 | お客様は、サポートされていないオペレーティングシステムでBitDefenderのインストールを行っています。「システム要件」 (p. 2)を確認して、BitDefenderをインストールできるオペレーティングシステムを見つけてください。<br>お使いのオペレーティングシステムが、Windows XP のサービスパック1、又はサービスパック無しの場合は、サービスパック2以上をインストール可能で、設定ウィザードを再度実行できます。 |
| インストールファイルは、違う種類のプロセッサ用に設計されています。 | このようなエラーが出た場合は、正しくないインストールファイルのバージョンを実行しようとしています。BitDefenderのインストールファイルには2つのバージョンがあります：32ビットプロセッサ用と64ビットプロセッサ用です。<br>お使いのシステムに正しいバージョンがインストールされているかを確認するには、www.bitdefender.jpから、インストールファイルを直接ダウンロードしてください。 |

### 35.1.2. インストールが失敗しました

正しいインストールが出来ない可能性がいくつかあります：

- インストール中、エラー画面が表示されます。 インストールをキャンセルするように指示があるか、あるいは、アンインストールツールを実行するボタンで、システムをクリーンアップするように促されるかもしれません。

**注意**
インストールの開始後すぐに、BitDefenderをインストールするために十分な空き容量がないことを通知されるかもしれません。この場合は、BitDefenderをインストールしたいパーティションで必要な空き容量を確保して、インストールを再び実行してください。

- インストール処理が進んでいません。恐らくお使いのシステムは停止しています。再起動を１回すればシステムのレスポンスが回復します。
- インストールが完了しましたが、BitDefenderのいくつかの、あるいは全ての機能を使用することができません。

インストールの失敗を解決して、BitDefenderのインストールを行うには、次の手順に従ってください：

1. インストールが失敗した後、システムをクリーンアップします。. インストールに失敗した場合、BitDefenderレジストリキーやファイルが、お使いのシステムに残ってしまうかもしれません。これがBitDefenderを新しくインストールすることを妨げる可能性があります。システムの性能や安定性にも影響を与えるかもしれません。従って、製品を再びインストールする前に、それらを削除してください。

   エラー画面でアンインストールツールを実行するボタンが表示された場合、ボタンをクリックして、システムをクリーンアップします。 別の方法では、次の手順があります：

   a. www.bitdefender.com/uninstallをクリックして、お使いのコンピュータにアンインストールツールをダウンロードしてください。

   b. 管理者権限を使用して、アンインストールツールを実行してください。

   c. コンピュータを再起動してください。

2. インストールが失敗した原因を検証します。. 製品を再インストールする前に、インストールの失敗を引き起こした原因を検証して、取り除いてください。

   a. 他のセキュリティソリューション製品がインストールされていないかをご確認ください。BitDefenderの通常処理を混乱させてしまう恐れがあります。このような場合は、別のセキュリティソリューション製品を全て削除して、BitDefenderの再インストールを行ってください。

   b. また、お使いのシステムが、ウィルスに感染していないかを確認する必要があります。 次の操作が行えます：

      - BitDefender Rescue CD を使用して、お使いのコンピュータをスキャンして、既存するあらゆる脅威を削除します。 詳細については、「BitDefender Rescue CD」 (p. 341)を参照してください。

- Internet Explorer ウィンドウを開いて、www.bitdefender.comへ進み、オンラインスキャンを実行してください。(オンラインスキャンボタンをクリックします)。

3. 再試行して、BitDefenderをインストールしてください。 www.bitdefender.jpからインストールファイルの最新バージョンをダウンロードして実行することをお勧めします。
4. 再度インストールに失敗した場合は、「サポート」 (p. 338)項に記載されているBitDefenderサポートにお問い合わせください。

## 35.2. BitDefenderサービスは応答していません

この項目では、次のエラーBitDefenderサービスの応答がありませんに関する解決策を記載しています。 次の内容のエラーが発生するかもしれません：

- システムトレイ内のBitDefenderアイコンは、グレーで表示されて、BitDefenderサービスは応答していないことをポップアップでお知らせします。
- BitDefenderウィンドウは、BitDefenderサービスが応答していないことを表示しています。

次の状態のいずれかにエラーの原因があるかもしれません：

- 重要なアップデートがインストールされました。
- 一時的にBitDefenderサービスへの通信エラーが発生しました。
- いくつかのBitDefenderサービスが停止しました。
- 別のセキュリティソリューションが、お使いのコンピュータ上でBitDefenderと同時に実行しています。
- お使いのシステムのウィルスが、BitDefenderの通常操作に影響を与えています。

このエラーを解決するには、次の対策を行ってください：

1. 変更が反映されるまで、しばらくお待ちください。 一時的なエラーです。
2. コンピュータを再起動して、BitDefenderが読み込まれるまで、しばらくお待ちください。BitDefenderを開いて、エラーが続いているかどうかを確認してください。 コンピュータを再起動することで、通常、問題は解決します。
3. 他のセキュリティソリューション製品がインストールされていないかをご確認ください。BitDefenderの通常処理を混乱させてしまう恐れがあります。このような場合は、別のセキュリティソリューション製品を全て削除して、BitDefenderの再インストールを行ってください。

4. エラーが存在する場合は、より深刻な問題があるかもしれません。（例えば、BitDefenderを妨げるウィルスに感染しているかもしれません。） 「サポート」(p. 338)項に記載されているBitDefenderサポートにお問い合わせください。

## 35.3. Wi-Fi（ワイヤレス）ネットワーク内で、ファイル及び共有プリンタが機能していません。

この項目は、以下のWi-FiネットワークのBitDefenderファイアーウォールに関する問題の解決策を提供しています。

- Wi-Fi ネットワーク内のコンピュータとファイルを共有できません。
- 付随するネットワークプリンタがWi-Fiネットワークへアクセスできません。
- Wi-Fiネットワーク内のコンピュータで共有されるプリンタにアクセスできません。
- Wi-Fiネットワーク内のコンピュータに付随するプリンタと共有できません。

これらの問題の解決を始める前に、セキュリティに関する情報及び Wi-Fiネットワーク内のBitDefenderファイアーウォール設定をご理解ください。 セキュリティの観点で、 Wi-Fi ネットワークは、以下のいずれかのカテゴリに分類されます。

- 保護されたWi-Fi ネットワーク. この種類のネットワークへは、許可されたWi-Fi機器のみが接続できます。ネットワークへのアクセスはパスワードが必要です。保護されたWi-Fiネットワークの例は、オフィスネットワーク内に設定されています。
- (保護されていない) Wi-Fi ネットワークを開く. 保護されていないWi-Fiネットワーク内の、あらゆるWi-Fi機器は、そこに自由に接続することができます。 保護されていないWi-Fi ネットワークが広範囲に使用されています。ほぼ全ての公共のWi-Fiネットワークを含んでいます（学校、喫茶店、飛行場等）。ワイヤレスルータを使用して設定するホームネットワークも、ルータのセキュリティを有効にするまでは、保護されていません。

  お使いのコンピュータは、不明のコンピュータに接続されているため、保護されていないWi-Fi ネットワークは、大きなセキュリティリスクを抱えています。ファイアーウォールによって適切な保護がされていないと、ネットワークに接続する誰でもが、お客様の共有にアクセスでき、コンピュータにまで侵入することができます。

保護されていないWi-Fi ネットワークと接続すると、 BitDefender は、このネットワーク内のコンピュータと自動的に通信をブロックします。インターネットにだけはアクセスできますが、ネットワーク内の別ユーザのファイルやプリンタを共有することはできません。

Wi-Fiネットワークの通信を有効にするには、2つの方法があります：

- ″信頼できるコンピュータ″ ソリューションは、Wi-Fi ネットワーク内の指定したコンピュータ（信頼できるコンピュータ）とだけ、ファイルやプリンタを共有することができます。 公共のWi-Fiネットワーク（例：学校、喫茶店のネットワーク）に接続する際、及び友人のファイルやプリンタ、あるいはWi-Fiネットワークプリンタにアクセスする際には、このソリューションをお使いください。
- ″安全なネットワーク″ ソリューションは、全てのWi-Fiネットワーク（安全なネットワーク）のファイルとプリンタ共有を許可します。 この解決策は、セキュリティ上の理由では推奨されませんが、特定の条件内では便利になるかもしれません。（例：ご自宅や、オフィスのWi-Fiネットワークで使用することが出来ます）

### 35.3.1. ″信頼できるコンピュータ″ のソリューション

BitDefenderファイアーウォールを設定するには、 Wi-Fi ネットワーク内のコンピュータのファイルやプリンタの共有を許可、あるいはWi-Fi ネットワークプリンタにアクセスします。次の手順に従ってください：

1. BitDefenderを開いて、ユーザインターフェイスを'上級者モード'に切り替えてください。
2. 左側にあるメニューからファイアーウォールをクリックします。
3. ネットワークタブをクリックします。
4. ゾーンテーブル内で、Wi-Fi ネットワークを選択して、 追加ボタンをクリックします。
5. Wi-Fi ネットワーク内で検出されたデバイスの一覧から、対象のコンピュータあるいはWi-Fi ネットワークプリンタを選択してください。 コンピュータやプリンタが自動的に検出されなかった場合は、ゾーン欄でIPアドレスを入力することができます。
6. 許可を選択します。
7. OKをクリックします。

選択されたコンピュータで、ファイルやプリンタを共有できない場合は、お使いのコンピュータのBitDefenderファイアーウォールが原因ではない場合が多いです。次のような、他の可能性がある原因をご確認ください：

- 他のコンピュータのファイアーウォールは、保護されていない（公共）Wi-Fi ネットワーク内で共有しているファイルやプリンタをブロックします。
  - そのファイアーウォールが、BitDefender2009 又はBitDefender2010 製品のものである場合は、もう一方のコンピュータでも同じ手順を行い、お使いのコンピュータとファイルやプリンタの共有を許可します。
  - Windowsファイアーウォールが使用されている場合は、以下のように、ファイルやプリンタの共有を許可する設定が可能です：Windowsファイアーウォール設定

ウィンドウを開いて、例外タブ、をクリックして、select the ファイル及びプリンタ共有欄を選択します。

- 別のファイアーウォールプログラム使用されている場合は、その説明書あるいはヘルプファイルを参照してください。

●共有プリンタの使用又は接続を妨げる可能性がある一般的な条件：

- 共有プリンタにアクセスするには、Windows管理者のアカウントにログインする必要があります。
- 共有プリンタは、指定したコンピュータやユーザのみがアクセスすることを許可されています。　プリンタを共有している場合、別のコンピュータのユーザが、プリンタへのアクセスを許可されているかどうか、プリンタの許可設定を確認してください。 共有プリンタに接続を試みている場合は、プリンタに接続する許可を得ているかどうか、別のコンピュータのユーザに確認してください。
- お使いのコンピュータ、あるいは別のコンピュータに接続しているプリンタは、共有されていません。
- 共有プリンタは、コンピュータに追加されていません。

注意
共有プリンタの管理方法(プリンタの共有、プリンタの設定又は削除、ネットワークプリンタ、又は共有プリンタへ接続)は、Windows Help 及びサポートセンター（スタートメニューの、ヘルプ及びサポートをクリック）に進んでください。

Wi-Fi ネットワークプリンタにアクセスできない場合は、お使いのコンピュータのBitDefenderファイアーウォールが原因ではない場合が多いです。 Wi-Fiネットワークプリンタへの接続は、特定のコンピュータ又はユーザのみに制限されているかもしれません。プリンタへの接続が許可されているかどうか、Wi-Fiネットワークの管理者に確認してください。

BitDefender　ファイアーウォールに問題があると思われる場合は、「サポート」(p. 338)項に記載されているBitDefenderサポートにお問い合わせください。

## 35.3.2. ″安全なネットワーク″ ソリューション

このソリューションは、ご家庭やオフィス内のWi-Fiネットワークにだけお使いいただくことをお勧めします。

BitDefenderファイアーウォールを設定するには、次の手順に従って、Wi-Fi ネットワーク全体で、ファイルやプリンタの共有を許可してください：

1. BitDefenderを開いて、ユーザインターフェイスを'上級者モード'に切り替えてください。
2. 左側にあるメニューからファイアーウォールをクリックします。

3. ネットワークタブをクリックします。
4. ネットワーク設定表の、信頼レベル欄で、 Wi-Fi ネットワークに対応するセルの▾の矢印をクリックしてください。
5. 確保したいセキュリティレベルに応じて、次のオプションからいずれかを選択してください：
   - ●危険 – 共有のアクセス許可なしで、Wi-Fiネットワーク内で共有されているファイルやプリンタにアクセスする。
   - ●安全 – ファイルと共有プリンタ両方を許可します。これは、Wi-Fi ネットワークに接続するユーザは、共有ファイルやプリンタにもアクセスできることを意味しています。

Wi-Fi ネットワーク内の指定したコンピュータで、ファイルやプリンタを共有できない場合は、お使いのコンピュータのBitDefenderファイアーウォールが原因ではない場合が多いです。 次のような、他の可能性がある原因をご確認ください：

- ●他のコンピュータのファイアーウォールは、保護されていない（公共）Wi-Fi ネットワーク内で共有しているファイルやプリンタをブロックします。
  - ▸ そのファイアーウォールが、BitDefender2009 又はBitDefender2010 製品のものである場合は、もう一方のコンピュータでも同じ手順を行い、お使いのコンピュータとファイルやプリンタの共有を許可します。
  - ▸ Windowsファイアーウォールが使用されている場合は、以下のように、ファイルやプリンタの共有を許可する設定が可能です：Windowsファイアーウォール設定ウィンドウを開いて、例外タブ、をクリックして、select the ファイル及びプリンタ共有欄を選択します。
  - ▸ 別のファイアーウォールプログラム使用されている場合は、その説明書あるいはヘルプファイルを参照してください。
- ●共有プリンタの使用又は接続を妨げる可能性がある一般的な条件：
  - ▸ 共有プリンタにアクセスするには、Windows管理者のアカウントにログインする必要があります。
  - ▸ 共有プリンタは、指定したコンピュータやユーザのみがアクセスすることを許可されています。 プリンタを共有している場合、別のコンピュータのユーザが、プリンタへのアクセスを許可されているかどうか、プリンタの許可設定を確認してください。 共有プリンタに接続を試みている場合は、プリンタに接続する許可を得ているかどうか、別のコンピュータのユーザに確認してください。
  - ▸ お使いのコンピュータ、あるいは別のコンピュータに接続しているプリンタは、共有されていません。
  - ▸ 共有プリンタは、コンピュータに追加されていません。

注意
共有プリンタの管理方法(プリンタの共有、プリンタの設定又は削除、ネットワークプリンタ、又は共有プリンタへ接続)は、Windows Help 及びサポートセンター（スタートメニューの、ヘルプ及びサポートをクリック）に進んでください。

Wi-Fi ネットワークプリンタにアクセスできない場合は、お使いのコンピュータのBitDefenderファイアーウォールが原因ではない場合が多いです。 Wi-Fiネットワークプリンタへの接続は、特定のコンピュータ又はユーザのみに制限されているかもしれません。プリンタへの接続が許可されているかどうか、Wi-Fiネットワークの管理者に確認してください。

BitDefender ファイアーウォールに問題があると思われる場合は、「サポート」(p. 338)項に記載されているBitDefenderサポートにお問い合わせください。

## 35.4. アンチスパムフィルタが正しく稼動していません

この項目は、以下のBitDefenderアンチスパムフィルタリングオペレーションに関する問題の解決策を提供しています：

- 多くの問題がない電子メールが次のように区別されました[spam].
- アンチスパムフィルタは多くの迷惑メールメッセージを区別していません
- アンチスパムフィルタはスパムメッセージを検出しませんでした

### 35.4.1. 問題がないメッセージが[spam]として区別されました。

問題がないメッセージが[spam]として区別されました。なぜならば、BitDefenderのアンチスパムフィルタが認識するスパムと類似しているからです。 アンチスパムフィルタを正しく設定すると、この問題は通常解決することができます。

BitDefenderは電子メールメッセージの受信者を、自動的に友人リストに追加します。 友人リスト内の連絡先から受信した電子メールメッセージは、問題がないものとしてい認識されます。それらはアンチスパムフィルタが確認を行わないので、[spam]として区別されることはありません。

友人リストの自動設定は、次のような状況で起こりうるエラー検出を防ぎません：

- 様々なウェブサイトに登録をしているため、多くの勧誘商業メールを受信します。このような場合の解決策は、対象の電子メールメッセージのアドレスを友人リストに追加します。
- 問題がない電子メールで最もな重要なことは、以前電子メールを送信したことがない人々、例えば、顧客やビジネスパートナー等です。 この場合他の解決策が必要です。

BitDefenderが統合するメールクライアントの1つを使用している場合は、以下の解決策をお試しください：

1. エラー検出を表示　これはアンチスパムフィルタの学習エンジン（ベイジアン）を学習させるために使用します。そして今後のエラー検出の防止に役立ちます。学習エンジンは、表示されたメッセージを分析してそれらのパターンを学習します。　次回から同じパターンと一致する電子メールメッセージは、[spam]として区別されません。
2. アンチスパムプロテクションレベルを下げます。　プロテクションレベルを下げると、アンチスパムフィルタは、電子メールを迷惑メールと分類するための迷惑メールをより多く表示します。　多くの問題がないメッセージ（勧誘商業メールを含む）が、迷惑メールとして間違って検出される場合は、この解決策をお試しください。
3. 学習エンジン（ベイジアンフィルタ）を再学習させる 前回の解決策に満足する結果が得られなかった場合は、この方法をお試しください。

**注意**

BitDefenderは、使いやすいアンチスパムツールバーを介して、最も共通して使用されるメールクライアントを統合します。　サポートされた全てのメールクライアントの一覧は、「サポートされたソフトウェア」（p. 2）をご参照ください。

別のメールクライアントを使用している場合は、エラー検出を表示することができず、学習エンジンを学習させることができません。問題を解決するには、アンチスパム保護レベルを下げることを試みてください。

## 連絡先を友人リストに追加

サポートされたメールクライアントを使用している場合は、問題がないメッセージの送信者を簡単に友人リストに追加することができます。 次の手順に従ってください：

1. メールクライアントで、友人リストに追加したい送信者からの電子メールメッセージを選択します。
2. BitDefenderアンチスパムツールバーの 友人を追加ボタンをクリックしてください。
3. 友人リストに追加するアドレスの承認を求められるかもしれません。　このメッセージを今後表示しませんを選択して、 OKをクリックします。

このアドレスから届くメールメッセージは、その内容に関わらず常に受け取ります。

別のメールクライアントを使用している場合は、連絡先をBitDefenderインターフェースから友人リストに追加することができます。 次の手順に従ってください：

1. BitDefenderを開いて、ユーザインターフェイスを'上級者モード'に切り替えてください。
2. 左側にあるメニューからアンチスパムをクリックします。
3. ステータスタブをクリックします。
4. 友人を管理をクリックしてください。 設定画面が表示されます。
5. 常に電子メールメッセージを受信したいアドレスを入力して、ボタンをクリックし、友人リストにアドレスを追加します。
6. OKをクリックして変更を保存しウィンドウを閉じます。

## エラー検出を表示

サポートされたメールクライアントを使用している場合は、簡単にアンチスパムフィルタを修正することができます。（[spam]として区別しない電子メールメッセージを表示する。）このように設定すると、アンチスパムフィルタの効率が大幅に向上します。 次の手順に従ってください：

1. お使いのメールクライアントを開いてください。
2. 迷惑メールメッセージが移動した迷惑メールフォルダを選択してください。
3. BitDefenderが[spam]として誤って区別した、問題がないメッセージを選択します。
4. BitDefenderアンチスパムツールバーの 友人を追加ボタンをクリックして、送信者を友人リストに追加します。 承認するためにOKのクリックが求められるかもしれません。 このアドレスから届くメールメッセージは、その内容に関わらず常に受け取ります。
5. BitDefenderアンチスパムツールバーの 非迷惑メール ボタンをクリックしてください。(通常メールクライアント画面の上側にあります)これは、選択されたメッセージが非迷惑メールであることを学習エンジンに学習させます。この電子メールメッセージは受信フォルダに移動されます。 次回から同じパターンと一致する電子メールメッセージはもはや、[spam]として区別されません。

## アンチスパムプロテクションレベルを下げる

アンチスパムプロテクションレベルを下げるには、次の手順に従ってください：

1. BitDefenderを開いて、ユーザインターフェイスを'上級者モード'に切り替えてください。
2. 左側にあるメニューからアンチスパムをクリックします。
3. ステータスタブをクリックします。
4. スライダーをスケールの下側に移動させます。

１つだけ保護レベルを下げることをお勧めします。結果を評価するまでしばらくお待ちください。 依然として問題がない電子メールメッセージが[spam]として区別される場合は、さらに保護レベルを下げることができます。多くの迷惑メールメッセージが検出されない場合は、保護レベルを下げるべきではありません。

### 学習エンジン（ベイジアン）を再学習させる

学習エンジン（ベイジアン）を学習させる前に、迷惑メールメッセージだけを含むフォルダと、問題がないメッセージだけを含む別のフォルダを準備します。 学習エンジンは、それらを分析してスパムと定義する特徴、あるいは通常受信する問題がないメッセージの特徴を学習します。効率良く学習させるために、それぞれのカテゴリに50メッセージ以上が必要になります。

ベイジアンデータベースをリセットして、学習エンジンを再学習させるには、次の手順に従ってください：

1. お使いのメールクライアントを開いてください。
2. BitDefenderアンチスパムツールバーで、ウィザードボタンをクリックして、アンチスパム設定ウィザードを開始してください。 このウィザードの詳細情報は、「アンチスパム設定ウィザード」 (p. 297)セクションに記載されています。
3. 次へをクリックします。
4. この手順をスキップを選択して、次へをクリックします。
5. アンチスパムフィルタのデータベースをクリアにするを選択して、次へをクリックしてください。
6. 問題がないメッセージを含むフォルダを選択して、次へをクリックします。
7. 迷惑メールメッセージを含むフォルダを選択して、次へをクリックします。
8. 終了をクリックすると、学習処理が開始します。
9. 学習が終了すると、閉じるをクリックします。

### ヘルプを依頼

この情報がお役に立たない場合は、「サポート」 (p. 338)項に記載されているBitDefenderサポートにお問い合わせください。

## 35.4.2. 多くの迷惑メールメッセージが検出されていません。

[spam]として区別されていない多くの迷惑メールメッセージ受信している場合は、効率を良くするためにBitDefender アンチスパムフィルタを設定する必要があります。

BitDefenderが統合するメールクライアントの1つを使用している場合は、以下の解決策を1つずつお試しください：

1. 検出されていない迷惑メールメッセージを表示　これはアンチスパムフィルタの学習エンジン（ベイジアン）を学習させるために使用し、通常迷惑メール検出を向上させます。　学習エンジンは、表示されたメッセージを分析してそれらのパターンを学習します。　次回から同じパターンと一致する電子メールメッセージは、[spam]として区別されます。
2. 迷惑メール送信者を迷惑メール送信者リストに追加　迷惑メール送信者リストのアドレスから受信した電子メールは、[spam]として自動的に区別されます。
3. アンチスパムプロテクションレベルを上げます。　プロテクションレベルを上げると、アンチスパムフィルタは、電子メールを迷惑メールとして分類するための迷惑メール表示を少なくします。
4. 学習エンジン（ベイジアンフィルタ）を再学習させる アンチスパム検出が満足に機能せず、検出されていない迷惑メールメッセージが表示されない場合は、この解決策を行ってください。

**注意**

BitDefenderは、使いやすいアンチスパムツールバーを介して、最も共通して使用されるメールクライアントを統合します。　サポートされた全てのメールクライアントの一覧は、「サポートされたソフトウェア」 (p. 2)をご参照ください。

別のメールクライアントを使用している場合は、迷惑メールメッセージを表示することができず、学習エンジンを学習させることができません。問題を解決するには、アンチスパム保護レベルを上げて、迷惑メール送信者を迷惑メール送信者リストに追加することを試みてください。

## 検出されていない迷惑メールメッセージを表示する

サポートされたメールクライアントを使用している場合は、どの電子メールが迷惑メールとして検出されるべきであるかを簡単に表示することができます。そうすると、アンチスパムフィルタの効率をかなり改善します。　次の手順に従ってください：

1. お使いのメールクライアントを開いてください。
2. 受信フォルダに進んでください。
3. 検出されていない迷惑メールメッセージを選択します。
4. BitDefenderアンチスパムツールバーの 迷惑メール ボタンをクリックしてください。(通常メールクライアント画面の上側にあります)これは、選択されたメッセージが迷惑メールであることを学習エンジンに学習させます。　[spam]として区別された電子メールメッセージは迷惑メールフォルダに移動します。　次回か

ら同じパターンと一致する電子メールメッセージは、[spam]として区別されます。

## 迷惑メール送信者を迷惑メール送信者リストに追加

サポートされたメールクライアントを使用している場合は、迷惑メールメッセージの送信者を簡単に迷惑メール送信者リストに追加することができます。 次の手順に従ってください：

1. お使いのメールクライアントを開いてください。
2. 迷惑メールメッセージが移動した迷惑メールフォルダを選択してください。
3. BitDefenderが[spam]として区別したメッセージを選択します。
4. BitDefenderアンチスパムツールバーの 迷惑メール送信者を追加ボタンをクリックしてください。
5. 迷惑メール送信者リストに追加するアドレスの承認を求められるかもしれません。 このメッセージを今後表示しませんを選択して、 OKをクリックします。

別のメールクライアントを使用している場合は、BitDefender インターフェースから、迷惑メール送信者を迷惑メール送信者リストに手動で追加することができます。同じ電子メールアドレスから複数の迷惑メールを受信している場合にのみ便利な機能になります。 次の手順に従ってください：

1. BitDefenderを開いて、ユーザインターフェイスを'上級者モード'に切り替えてください。
2. 左側にあるメニューからアンチスパムをクリックします。
3. ステータスタブをクリックします。
4. 迷惑メール送信者を管理をクリックしてください。 設定画面が表示されます。
5. 迷惑メール送信者の電子メールアドレスを入力して、ボタンをクリックして、迷惑メール送信者リストにアドレスを追加します。
6. OKをクリックして変更を保存しウィンドウを閉じます。

## アンチスパムプロテクションレベルを上げる

アンチスパムプロテクションレベルを上げるには、次の手順に従ってください：

1. BitDefenderを開いて、ユーザインターフェイスを'上級者モード'に切り替えてください。
2. 左側にあるメニューからアンチスパムをクリックします。
3. ステータスタブをクリックします。
4. スライダーをスケールの上側に移動させます。

### 学習エンジン（ベイジアン）を再学習させる

学習エンジン（ベイジアン）を学習させる前に、迷惑メールメッセージだけを含むフォルダと、問題がないメッセージだけを含む別のフォルダを準備します。 学習エンジンは、それらを分析してスパムと定義する特徴、あるいは通常受信する問題がないメッセージの特徴を学習します。効率良く学習させるために、それぞれフォルダ内で、50メッセージ以上が必要になります。

ベイジアンデータベースをリセットして、学習エンジンを再学習させるには、次の手順に従ってください：

1. お使いのメールクライアントを開いてください。
2. BitDefenderアンチスパムツールバーで、ウィザードボタンをクリックして、アンチスパム設定ウィザードを開始してください。 このウィザードの詳細情報は、「アンチスパム設定ウィザード」（p. 297）セクションに記載されています。
3. 次へをクリックします。
4. この手順をスキップを選択して、次へをクリックします。
5. アンチスパムフィルタのデータベースをクリアにするを選択して、次へをクリックしてください。
6. 問題がないメッセージを含むフォルダを選択して、次へをクリックします。
7. 迷惑メールメッセージを含むフォルダを選択して、次へをクリックします。
8. 終了をクリックすると、学習処理が開始します。
9. 学習が終了すると、閉じるをクリックします。

### ヘルプを依頼

この情報がお役に立たない場合は、「サポート」（p. 338）項に記載されているBitDefenderサポートにお問い合わせください。

## 35.4.3. アンチスパムフィルタは迷惑メールメッセージを検出しません。

迷惑メールメッセージが、 [spam]として区別されない場合は、BitDefenderアンチスパムフィルタに問題があるかもしれません。 この問題を解決する前に、次の状態のいずれかが原因でないかをご確認ください：

- BitDefenderアンチスパムプロテクションは、POP3 プロトコル経由の電子メールメッセージの受信設定を行ったメールクライアントのみ、有効になります。 これは以下を意味しています：

- ウェブベースの電子メールサービス経由で受信したメッセージ（Yahoo, Gmail, Hotmail等）に対して、BitDefenderはスパムに対するフィルタリングを行いません。
- お使いの電子メールクライアントが、POP3 以外のプロトコル(例 IMAP4)を使用して電子メールメッセージの受信を設定している場合は、BitDefenderアンチスパムフィルタは、スパムに対するチェックを行いません。

**注意**

POP3は、メールサーバから電子メールメッセージをダウンロードするために、最も使用されているプロトコルの内の１つです。 電子メールメッセージをダウンロードするメールクライアントのプロトコルがお分かりにならない場合は、電子メールクライアントを設定された方にご確認ください。

●BitDefender Internet Security 2010は、Lotus Notes POP3通信はスキャンしません。

以下の可能性がある原因もご確認ください：

1. アンチスパムが有効かどうかをご確認ください。
   a. BitDefenderを開く。
   b. ウィンドウの右上にある設定 ボタンをクリックしてください。
   c. セキュリティ設定のカテゴリで、アンチスパムの状態をご確認ください。

   アンチスパムが無効になっていると、これが問題を引き起こしている原因となります。 アンチスパムを有効にすると、アンチスパム処理を監視して、問題が解決されたかどうかを確認します。
2. 大変考えにくいケースですが、お客様または(他のユーザ)が、BitDefenderが迷惑メールメッセージを[spam]としてマークしないよう設定していないか、ご確認ください。
   a. BitDefenderを開いて、ユーザインターフェイスを'上級者モード'に切り替えてください。
   b. メニューの左側にあるアンチスパムをクリックして、設定タブを選択します。
   c. 件名に迷惑メール表示を追加が選択されているかをご確認ください。

有効な解決策は、製品の修復又は再インストールです。一方で、BitDefenderのサポートにお問い合わせを希望される場合に関しては、この「サポート」 (p. 338)項をご確認ください。

## 35.5. BitDefenderの削除に失敗しました

この項目は、BitDefenderを削除する時に発生する可能性があるエラーの解決策を記載しています。 起こりうる状況が二つあります：

- 削除中、エラー画面が表示されます。 画面に、システムをクリーンアップするアンインストールツールを実行するボタンが表示されます。
- 削除処理が進んでいません。恐らくお使いのシステムは停止しています。 キャンセルをクリックして、削除を停止してください。この操作ができない場合は、システムを再起動してください。

削除に失敗した場合、BitDefenderレジストリキーやファイルが、お使いのシステムに残ってしまうかもしれません。これがBitDefenderを新しくインストールすることを妨げる可能性があります。。システムの性能や安定性にも影響を与えるかもしれません。 お使いのシステムから BitDefenderを完全に削除するためには、アンインストールツールを実行しなければなりません。

画面にエラーが表示されて削除に失敗した場合は、アンインストールツールを実行するボタンをクリックして、システムをクリーンアップしてください。 別の方法では、次の手順があります：

1. www.bitdefender.com/uninstallをクリックして、お使いのコンピュータにアンインストールツールをダウンロードしてください。
2. 管理者権限を使用して、アンインストールツールを実行してください。 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。
3. コンピュータを再起動してください。

この情報がお役に立たない場合は、「サポート」 (p. 338)項に記載されているBitDefenderサポートにお問い合わせください。

# 36. 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。

## 36.1. 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ィルス保護や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。

## 36.2. 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。

## 36.3. 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。

### 36.3.1. ウェブアドレス

営業：sales@bitdefender.jp
テクニカルサポート: www.bitdefender.com/help
文書制作：documentation@bitdefender.com
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
ウィルス報告：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

### 36.3.2. 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: www.bitdefender.es/ayuda
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://www.bitdefender.ro/suport
ウェブサイト http://www.bitdefender.ro

# BitDefender Rescue CD

# 37. 概要

BitDefender Internet Security 2010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、既存のすべてのハードドライブをスキャンし、ウィルス駆除できる起動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ィ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。アンチウィ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ィ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）をスキャンしてウィルス駆除できるデスクトップアンチウィ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/

## 37.1. 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。

## 37.2. 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。

# 38. 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。

## 38.1. BitDefender Rescue CDを起動

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

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


起動画面

起動時にウィ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。

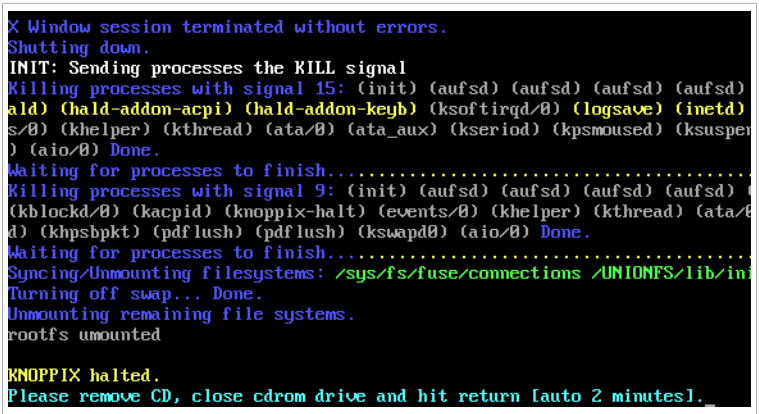

デスクトップ

## 38.2. 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。

## 38.3. どうやってアンチウィ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。

指定したディレクトリのみをスキャンしたい場合は、代わりに以下のいずれかを使用することができます：

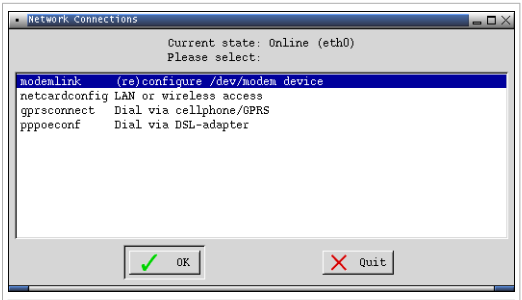
- Unices用のBitDefenderスキャナを使用してください。
  1. デスクトップ上のアイコン'スキャナの開始'をダブルクリックしてください。BitDefender Scanner for Unicesが起動します。
  2. スキャナをクリックすると、新しいウィンドウが表示されます。
  3. スキャンしたいディレクトリを選択して、開く をクリックすると、最初に起動したときに表示される同じウィザードを使用して、スキャンを開始します。
- コンテキストメニューを使用する - フォルダを閲覧し、ファイルあるいはディレクトリを右クリックして、 送信先を選択してください。続いて BitDefender スキャナを選んでください。
- 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/
```

## 38.4. 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 | 解説 |
| --- | --- |
| 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。

## 38.5. BitDefederのアップデート方法

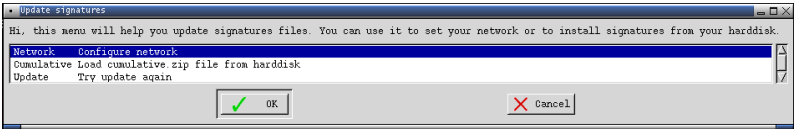
起動時に、ウィルスシグネチャは自動的に更新されます。しかしながら、BitDefenderをアップデートするには、この手順をスキップする場合と、起動後にアップデートを行う場合との、２つの方法があります。

●Unices用のBitDefenderスキャナを使用してください。

1. デスクトップ上のアイコン'スキャナの開始'をダブルクリックしてください。BitDefender Scanner for Unicesが起動します。
2. アップデートをクリックしてください。

●デスクトップ上のシグネチャのアップデートショートカットを使用します。

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。

### 38.5.1. 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、ウィ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、以下のオプションのいずれかをお使いください：

●Unices用のBitDefenderスキャナを使用してください。

1. デスクトップ上のアイコン'スキャナの開始'をダブルクリックしてください。BitDefender Scanner for Unicesが起動します。
2. 設定をクリックすると、新しいウィンドウが表示されます。
3. アップデート設定の下にある、　このHTTPプロキシを有効にするチェック欄を選択してください。　プロキシホスト(以下のように指定されます:　ホスト[:port])、プロキシユーザ（以下のように指定されます: [domain¥]ユーザ名）及びパスワードを指定します。　プロキシサーバが有効でないとき直接接続を使用するため、有効でないプロキシサーバを回避する欄を選択してください。
4. 保存をクリックしてください
5. アップデートをクリックしてください

●Terminalを使用（root権限で実行）

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

## 38.6. 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。次のウィ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。

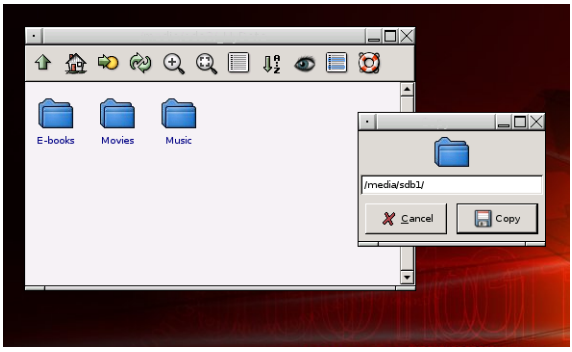
a. デスクトップにあるターミナルエミュレータのショートカットをダブルクリックします。

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。次のウィンドウが開きます。




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。

## 38.7. コンソールモードの使い方

画像ユーザインターフェースの実行に十分な高い表示解像度でない場合は、コンソールモードで、BitDefender Rescue CD を実行することができます。テキストモードで、お使いのコンピュータをフルスキャンすることが可能です。

コンソールモードでCDを実行するには、お使いのコンピュータのBIOS を設定して、CDを取り出し、ドライブにCDを入れて、コンピュータを再起動してください。画面が立ち上がると、コンソールモードでknoppixを開始を選択してください。

起動後、画面上の指示に従って、お使いのコンピュータのスキャンを実行してください。

BitDefenderは、ハードドライブ上でパーティションを検出し、スキャン開始前にマルウェアのシグネチャのデータベースを自動的にアップデートします。感染したファイルが検出された場合は、BitDefenderはウィルス駆除を行います。スキャンの完了後、スキャンの記録が表示されます。

**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。

# 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。

ウィルスを追い出す
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ィルスです。起動セクタウィルスに感染したディスケットから起動しようとすると、ウィ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、その時点からウィ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
スキャン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
新しいウィ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、特定のウィ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ィ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。

マクロウィルス
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ィルスです。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ィ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ィ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。

多形性ウィルス
感染させるファイル毎にその形式を変化させるウィルスです。一貫したバイナリパターンを持たないので、このようなウィ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。ウィルスと違い、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、コンピュータのウィ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ィ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。

ウィルス
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。多くのウィルスは、自分自身を複製して増殖します。コンピュータウィルスはすべて、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ィルスは、比較的簡単に作成できます。そんな単純なウィルスでも、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ィルスでは、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。

ウィルス定義
アンチウィルスプログラムがウィルスを検出して駆除するために使う、ウィ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。