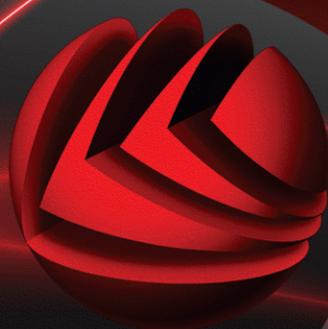


bitdefender



INTERNET SECURITY ²⁰⁰⁸

ユーザガイド

BitDefender Internet Security 2008

ユーザガイド

発行 2008. 04. 14

製作著作© 2008 BitDefender

法的表示

無断複写・複製・転載を禁じます。この図書のいかなる部分も、BitDefender の公式な代理人からの書面による許可がない限り、コピー、記録、あるいは他のあらゆる情報保管および抽出手段を含め、電子的あるいは機械的にしろ、どのような形態あるいはどのような方法でも複製または転送することを禁止します。レビューに簡単な引用を行うことは、引用元を併記すれば可能です。しかし内容を編集することは一切できません。

警告および免責条項 この製品およびその関連図書は、著作権で保護されています。図書に記載された情報は、「現状まま」を前提に提供されており、一切の保証はありません。この図書の作成は注意深く行われていますが、記載された情報が間接あるいは直接の原因となった、または原因ではないかと疑われる、損失あるいは損害に対して一切法的責任を負いません。

この図書には、BitDefender が管理していないサードパーティのウェブサイトへのリンクが含まれています。BitDefender では、すべてのリンクされたサイトについて、その内容に責任を負いません。この図書に記載されたサードパーティのウェブサイトを訪問する場合は、お客様自身の責任で行ってください。BitDefender では、こうしたリンクをお客様の利便性のために提供しているだけであり、リンクを記載したことにより、BitDefender がそうしたサードパーティのサイトの内容について支持したり、認めたり、責任を負ったりすることを意味するものではありません。

商標 この図書には、商標名が記載されている場合があります。この図書上のすべての登録商標および商標は、それぞれの所有者の所有物であり、参照の目的のみで使用されています。



目次

ライセンスおよび保証	ix
はじめに	xiii
1. この図書で使われている決まり事	xiii
1.1. 字体の決まり事	xiii
1.2. 警告	xiv
2. この図書の構造	xiv
3. コメントのお願い	xv
インストール	1
1. BitDefender Internet Security 2008のインストール	2
1.1. システム要項	2
1.2. インストール手順	3
1.3. 初回設定ウィザード	6
1.3.1. 手順1/6 - BitDefender Internet Security 2008の登録	7
1.3.2. 手順2/6 - BitDefenderアカウントを作成	8
1.3.3. 手順3/6 - リアルタイムウイルスレポート (RTVR) について	10
1.3.4. 手順4/6 - 実行するタスクを選択	11
1.3.5. 手順5/6 - タスクが完了するまでお待ちください	12
1.3.6. 手順6/6 - 概要を表示	13
1.4. アップグレード	13
1.5. BitDefender を修復あるいは削除	14
基本的な管理	16
2. はじめに	17
2.1. システムトレイ内の BitDefender アイコン	18
2.2. スキャン処理バー	19
2.3. BitDefender の手動スキャン	20
2.4. ゲームモード	21
2.4.1. ゲームモードを使用	21
2.4.2. ゲームモードのホットキーを変更	22
3. セキュリティの状態	23
3.1. ペアレンタルコントロール状態ボタン	25
3.2. PCセキュリティ状態ボタン	25
3.3. ネットワークセキュリティ状態ボタン	26
3.4. 個人識別情報コントロール状態ボタン	27

4. クイックタスク	28
4.1. セキュリティ	28
4.1.1. BitDefender のアップデート	28
4.1.2. BitDefender によるスキャン	30
5. 履歴	36
6. 登録	38
6.1. 手順 1/3 - BitDefender Internet Security 2008 を登録	38
6.2. 手順2/3 - BitDefenderアカウントを作成	39
6.3. 手順 3/3 - BitDefender Internet Security 2008 を登録	41
詳細なセキュリティ管理	43
7. 設定コンソール	44
7.1. 一般設定	45
7.1.1. 一般設定	46
7.1.2. ウィルスレポートの設定	48
7.1.3. 設定を管理	48
8. アンチウイルス	49
8.1. オンアクセススキャン	50
8.1.1. 保護レベルを設定	51
8.1.2. カスタム保護レベル	52
8.1.3. リアルタイム保護を無効にする	56
8.2. オンデマンドスキャン	56
8.2.1. スキャンタスク	57
8.2.2. ショートカットメニューを使う	60
8.2.3. スキャンタスクを作成	61
8.2.4. スキャンタスクを設定	61
8.2.5. スキャンするオブジェクト	72
8.2.6. スキャンログを表示	80
8.3. スキャンから除外されるオブジェクト	82
8.3.1. スキャンからパスを除外	84
8.3.2. スキャンから拡張子を除外	86
8.4. 隔離領域	89
8.4.1. 隔離されたファイルを管理	90
8.4.2. 隔離領域設定を構成	91
9. ファイアウォール	93
9.1. ファイアウォールの知識	93
9.1.1. ファイアウォールプロフィールの説明	94

9.1.2.	ネットワークゾーンの説明	95
9.1.3.	ファイアウォールの操作	96
9.2.	ファイアウォールの状態	98
9.2.1.	保護レベルを設定	99
9.3.	通信コントロール	100
9.3.1.	ルールを自動で追加	101
9.3.2.	ルールを手動で追加	102
9.3.3.	ルールを管理	107
9.3.4.	プロフィール編集	108
9.3.5.	プロフィールをリセット	109
9.4.	詳細設定	110
9.4.1.	ICMP フィルタ設定	111
9.4.2.	詳細ファイアウォール設定	113
9.5.	接続コントロール	115
9.6.	ネットワークゾーン	116
9.6.1.	ゾーンを追加	119
10.	アンチスパム	121
10.1.	アンチスパムの知識	121
10.1.1.	アンチスパムフィルタ	121
10.1.2.	アンチスパム操作	124
10.2.	アンチスパムの状態	125
10.2.1.	手順1/2 - しきい値レベルを設定	127
10.2.2.	手順2/2 - アドレス一覧に登録	128
10.3.	アンチスパム設定	132
10.3.1.	アンチスパム設定	133
10.3.2.	基本迷惑メールフィルタ	134
10.3.3.	詳細な迷惑メールフィルタ	134
10.4.	メールクライアントとの連携	135
10.4.1.	アンチスパムツールバー	135
10.4.2.	アンチスパム設定ウィザード	144
11.	個人情報コントロール	150
11.1.	個人情報コントロールの状態	150
11.1.1.	個人情報コントロール	151
11.1.2.	アンチフィッシング保護	152
11.2.	詳細設定 - 個人識別情報コントロール	153
11.2.1.	個人識別情報のルール	155
11.2.2.	例外を指定	157
11.2.3.	ルールを管理	158
11.3.	詳細設定 - レジストリコントロール	159
11.4.	詳細設定 - Cookie コントロール	161

11.4.1. 設定ウィザード	163
11.5. 詳細設定 - スクリプトコントロール	165
11.5.1. 設定ウィザード	167
11.6. システム情報	168
11.7. アンチフィッシングツールバー	170
12. ペアレンタルコントロール	173
12.1. ペアレンタルコントロール設定の保護	173
12.2. ペアレンタルコントロールの状態	174
12.2.1. ペアレンタルコントロールを選択	175
12.2.2. ヒューリスティック・ウェブフィルタを設定	176
12.3. ウェブコントロール	177
12.3.1. 設定ウィザード	178
12.3.2. 例外を指定	180
12.3.3. BitDefender のウェブブラックリスト	181
12.4. アプリケーションコントロール	181
12.4.1. 設定ウィザード	182
12.5. キーワードフィルタ	183
12.5.1. 設定ウィザード	184
12.6. ウェブ時間制限	186
13. アップデート	188
13.1. 自動アップデート	189
13.1.1. アップデートを請求	190
13.1.2. 自動アップデートを無効にする	190
13.2. アップデート設定	191
13.2.1. アップデートの場所を設定	192
13.2.2. 自動アップデート設定	193
13.2.3. 手動アップデート設定	194
13.2.4. 詳細設定	194
13.2.5. プロキシを管理	195
BitDefender Rescue CD	197
14. 概要	198
14.1. システム要項	198
14.2. 同梱されるソフトウェア	199
15. BitDefender Rescue CD の使い方	202
15.1. BitDefender Rescue CD を起動	202
15.2. BitDefender Rescue CD の停止	204
15.3. どうやってアンチウイルススキャンを実行するのですか?	205

- 15.4. どうやってプロキシ経由で BitDefender をアップデートするのですか? 206
- 15.5. データをどうやって保存するのですか? 206

問い合わせ先 209

- 16. サポート 210
 - 16.1. BitDefender Knowledge Base 210
 - 16.2. ヘルプを依頼 211
 - 16.2.1. Web Self Service を開いてください 211
 - 16.2.2. サポートチケットを開く 211
 - 16.3. 連絡先 212
 - 16.3.1. ウェブアドレス 212
 - 16.3.2. 支店 212

用語集 215

ライセンスおよび保証

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

はじめに

このガイドは、お使いのパーソナルコンピュータのためのセキュリティソリューションとして、BitDefender Internet Security 2008を選択したすべてのユーザを対象に書かれています。この図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。

この図書は、お客様にBitDefender Internet Security 2008とそれを開発した会社およびチームについて解説し、インストール手順を説明し、その設定の方法を説明します。BitDefender Internet Security 2008の使い方、アップデート、試験、カスタマイズのしかたを説明します。BitDefender を最大限有効に使う方法が分かります。

その内容が、お客様にとって楽しく、有意義であることを願っています。

1. この図書で使われている決まり事

1.1. 字体の決まり事

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

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

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

1.2. 警告

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



注意

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



重要項目

お客様が注意すべき内容で、読み飛ばしてはいけません。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大な情報です。内容に従って、損することはあり得ません。非常な危険を伴う内容を含みますので、よく読んで理解してください。

2. この図書の構造

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

インストール. ワークステーションへの BitDefender のインストール方法が、順を追って説明されています。これは、分かりやすい BitDefender Internet Security 2008 のインストールに関するマニュアルです。正しいインストールのための必須条件に始まり、すべてのインストール手順がガイドされています。最後に、BitDefender をアンインストールする場合の、削除操作も説明してあります。

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

詳細なセキュリティ管理. BitDefender が提供するセキュリティ機能の詳細な説明です。この章では、詳細設定コンソールにあるすべてのオプションについて説明します。お使いのコンピュータを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。

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

問い合わせ先. 予期しない事態が起きた時、相談するための連絡先です。

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

3. コメントのお願い

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

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



重要項目

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

インストール

1. BitDefender Internet Security 2008 のインストール

このユーザガイドのBitDefender Internet Security 2008のインストールの項では、以下の内容を説明します：

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

1.1. システム要項

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

- **動作環境**：Windows 2000 SP4 / XP SP2 32b & 64b / Vista 32b & 64b; Internet Explorer 6.0 (以降)
- **対応する電子メールクライアント**：Microsoft Outlook 2000 / 2003 / 2007 ; Microsoft Outlook Express ; Microsoft Windows Mail ; Thunderbird 1.5 and 2.0

Windows 2000

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

Windows XP

- **800 MHz以上のプロセッサ**
- **最小256 MBのRAMメモリ (1 GB推奨)**

- 最小60 MBのハードディスク空き容量

Windows Vista

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

BitDefender Internet Security 2008の試用版は、次の BitDefender のウェブサイトからダウンロードできます：<http://www.bitdefender.com>

1.2. インストール手順

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

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



インストール手順

以下の手順に従ってBitDefender Internet Security 2008をインストールしてください：

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

お使いのコンピュータへインストールする際に、他のアンチウイルス製品が既に存在すると、BitDefender Internet Security 2008が警告します。該当する製品をアンインストールするには、削除をクリックしてください。検出された製品を削除せずにインストールを続けるには、次へをクリックしてください。



警告

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

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

次へをクリックしてください。

5. インストール処理に関するオプションを選択してください。いくつかは、デフォルトで選択されています：
 - 「お読みください」ファイルを開く - インストールの最後で、「お読みください」ファイルを開きます。
 - デスクトップにショートカットを保存 - インストールの最後で、BitDefender Internet Security 2008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。
 - 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 2008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勧めます。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てください。



重要項目

インストール中に、**ウィザード**が表示されます。ウィザードはお使いのBitDefender Internet Security 2008の登録、BitDefender アカウント作成、重要なセキュリティのタスクを実行するための BitDefender 設定を手引きします。ウィザードの手順を完了して、次の手順に進んでください。

6. 終了をクリックしてください。 設定ウィザードがインストールを完了するために、お使いのシステムを再起動するよう促される場合があります。 できるだけ早く、実行することをお勧めします。

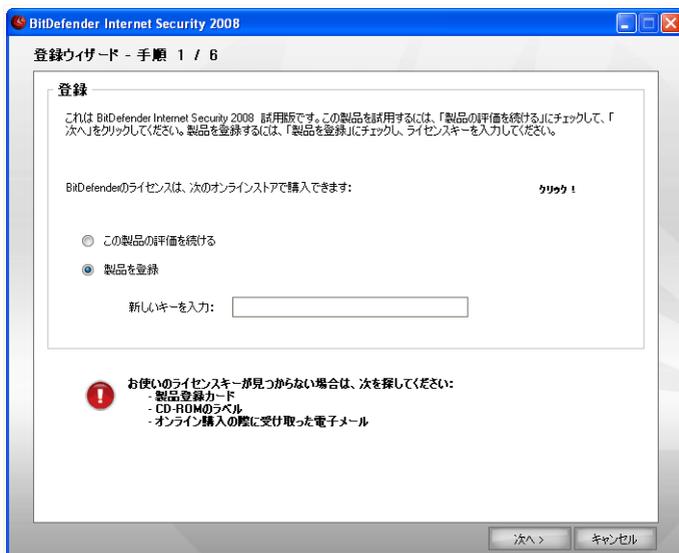
インストール先としてデフォルト設定を使った場合、BitDefenderという名前の新しいフォルダがProgram Filesに作成され、その中にBitDefender 2008というサブフォルダがあります。

1.3. 初回設定ウィザード

インストール中にウィザードが表示されます。ウィザードは、お使いのBitDefender Internet Security 2008の登録、BitDefender アカウント作成、重要なセキュリティのタスクを実行するための BitDefender 設定を手引きします。

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 2008 をインストールする前にお使いのシステムが安全であることを確認するためにも、ウィザードの利用をお勧めします。

1.3.1. 手順1/6 – BitDefender Internet Security 2008の登録



登録

BitDefender Internet Security 2008を登録するには、製品を登録を選んでください。新規キーを入力欄にライセンスキーを入力してください。

製品の評価を続けるには、製品の評価を継続を選択してください。

次へをクリックしてください。

1.3.2. 手順2/6 – BitDefenderアカウントを作成

製品を登録

技術サポートを受けたり、お使いのライセンスキーを安全に保管して後で取り出したり、特價販売などを利用するために、BitDefenderアカウントを作成するか、既存のアカウントにログインしてください。

既存のBitDefenderアカウントにログイン

電子メール:

パスワード: [パスワードをお忘れですか？](#)

新しいBitDefenderアカウントを作成

電子メール:

パスワード:

パスワードを再入力:

名:

姓:

国:

アカウントは後で作成

次へ > キャンセル

アカウントの作成

BitDefender アカウントを持っていません

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



注意

アカウントを後日作成される場合は、該当するオプションを選択してください。

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

- 電子メール - お使いの電子メールアドレスをご入力ください。
- パスワード - 上で指定したユーザの有効なパスワードを入力してください。

**注意**

パスワードは、半角英数字で4文字以上にしてください。

- パスワードを再入力 - 上で入力したパスワードを再度入力してください。
- 名 - お名前をご入力ください。
- 姓 - 苗字をご入力ください。
- 国 - お住まいの国名を選択してください。

**注意**

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

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

次へをクリックしてください。

すでに BitDefender アカウントを持っています

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

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

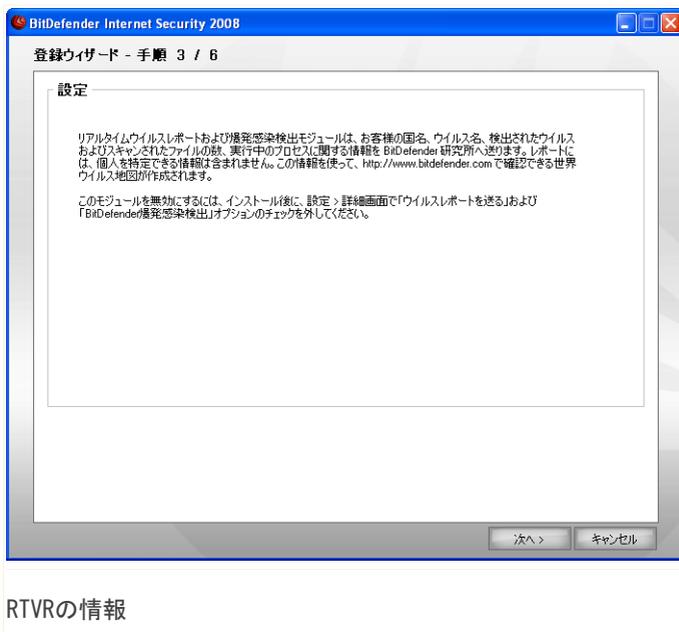
**注意**

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

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

次へをクリックしてください。

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



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

1.3.4. 手順4/6 – 実行するタスクを選択



タスクを選択

BitDefender Internet Security 2008がお使いのシステムのために重要なセキュリティのタスクを実行するように設定します。

次のオプションが指定できます：

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



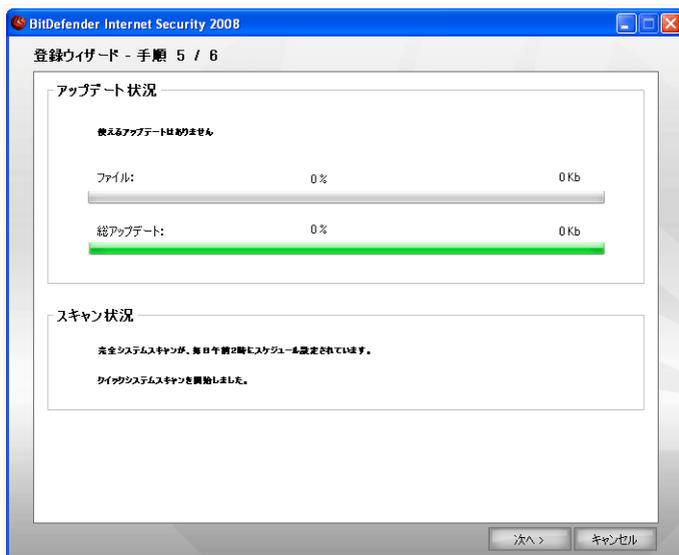
重要項目

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

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

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

1.3.5. 手順5/6 - タスクが完了するまでお待ちください

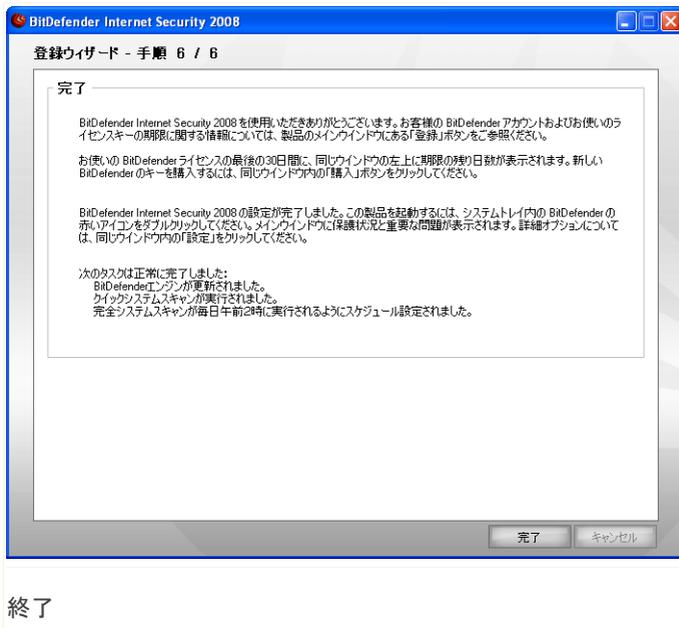


タスクの状況

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

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

1.3.6. 手順6/6 - 概要を表示



これが設定ウィザードの最後の手順です。

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

1.4. アップグレード

アップグレードの方法は、次から選べます：

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

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



重要項目

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

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

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



重要項目

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

1.5. BitDefender を修復あるいは削除

BitDefender Internet Security 2008を修復または削除するには、Windows スタートメニューから次のパスを辿ってください：スタート → プログラム → BitDefender 2008 → 修復、削除。

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

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



重要項目

製品を修復する前に、友達一覧および迷惑メール送信者一覧を保存することをお勧めします。BitDefender 設定やペイジアンデータベースも保存できます。修復処理が完了したら、それらを読み込んでください。

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、修復処理が開始します。

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 2008を再インストールしてください。

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

- 削除 - インストールされているすべてのコンポーネントを削除します。



注意

クリーンに再インストールする場合は、削除を選択することをお勧めします。

BitDefender の削除を選ぶと、新しいウィンドウが開きます。



重要項目

BitDefender を削除すると、ウイルス、スパイウェア、ハッカーから、もう保護されません。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 2008 を削除開始するには、削除をクリックしてください。

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

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



注意

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

BitDefender の削除中にエラーが起きました

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

基本的な管理

2. はじめに

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

BitDefender Security Center を利用するには、Windows のスタートメニューから、次のパスを辿ってください：スタート → プログラム → BitDefender 2008 → BitDefender Internet Security 2008あるいは、システムトレイの  BitDefender アイコンをダブルクリックすれば、もっと早く利用できます。



BitDefender Security Center

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

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

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

■クイックタスク画面：お使いのシステムを安全に保ち、データを守ります。

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

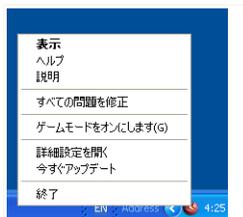
リンク	説明
購入	製品を購入するためのページを開きます。
マイアカウント	お客様の BitDefender アカウントのページを開きます。
登録	登録ウィザードを開きます。
ヘルプ	ヘルプファイルを開きます。
サポート	BitDefender のサポートウェブページを開きます。
設定	詳細設定画面を開きます。
履歴	BitDefender の履歴&イベントを記載したウインドウを開きます。

2.1. システムトレイ内の BitDefender アイコン

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

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

表示 - BitDefender Security Center を開きます。



BitDefender アイコン

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

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

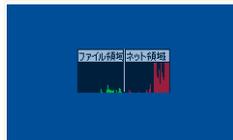
お使いのシステムに影響する重大な問題がある場合、エクスクラメーションマーク (!) が  BitDefender アイコン上に表示されます。 マウスカーソルをアイコン上に移動すると、お使いのシステムに影響する問題の数を確認できます。

2.2. スキャン処理バー

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

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

ネットゾーンに表示された赤い棒は、0から100間での目盛りで、毎秒（インターネットから送受信され）転送されたキロバイト（Kbyte）数を表示します。



処理バー



注意

スキャン処理バーは、リアルタイム保護あるいはファイアウォールが無効のとき、対応する（ファイルゾーンあるいはネットゾーン）部分に赤いバツ印を表示して知らせます。

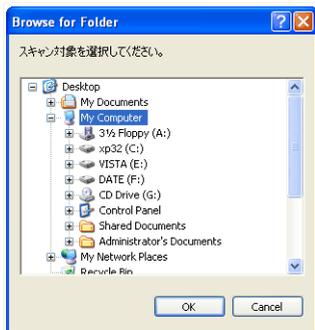
スキャン処理バーを使ってオブジェクトをスキャンできます。スキャンしたいオブジェクトをドラッグして、バーの上にドロップしてください。詳細については、「ドラッグ&ドロップスキャン」（p. 73）を参照してください。

グラフィカルなインターフェースを表示したくなければ、右クリックして隠すを選んでください。このウィンドウを完全に隠すには、設定コンソールで詳細をクリックし、スキャン処理バーを有効にする（処理状況を画面にグラフ表示）のチェックを外してください。

2.3. BitDefender の手動スキャン

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

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



BitDefender の手動スキャン

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

2.4. ゲームモード

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

- BitDefender の警告とポップアップ表示がすべて無効になります。
- BitDefender リアルタイム保護レベルは、消極的に設定されています。
- BitDefender Firewall は、ゲームモードに設定されています。

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

2.4.1. ゲームモードを使用

ゲームモードは、次の方法のいずれかで使えるようになります：

- システムトレイの BitDefender アイコンを右クリックし、ゲームモードをオンにするを選択します。
- Alt+Gキー（デフォルトのホットキー）を押します。



重要項目

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

2.4.2. ゲームモードのホットキーを変更

ホットキーを変更するには、次の手順で行ってください：

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



注意

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

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

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

■編集欄で、使用したい文字キーに対応する文字を入力します。

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



注意

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

3. セキュリティの状態

セキュリティの状態は、体系的に整理されて管理しやすい、コンピュータ上のセキュリティ脆弱性の一覧を表示します。BitDefender Internet Security 2008は、お使いのコンピュータのセキュリティに影響する問題があれば、すぐにお客様に通知します。

セキュリティの状態を表す4種類のボタンがあります：

- PC セキュリティ
- ネットワークセキュリティ
- 個人識別情報コントロール
- ペアレンタルコントロール

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

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

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

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



セキュリティの問題

セキュリティの問題一覧とその状態の簡単な説明が表示されます。

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

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



重要項目

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

問題を後で修正するなら、閉じるをクリックします。

3.1. ペアレンタルコントロール状態ボタン

ペアレンタルコントロール状態ボタンが緑なら、ペアレンタルコントロールは有効です。灰色なら、無効です。

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の状態ボタンをクリックしてください。
2. 次の操作を行えます：
 - ペアレンタルコントロールをすべてのユーザで有効にするには、今すぐ修正をクリックしてください。
 - ペアレンタルコントロールを特定のユーザだけに有効にするには、そのユーザに対応する修正ボタンをクリックしてください。

3.2. PCセキュリティ状態ボタン

セキュリティ状況ボタンが緑なら、心配することはありません。それ以外の場合、ボタンが黄、赤、灰なら、お使いのコンピュータが中位あるいは高い危険にさらされています。

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

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

問題	色
前回のシステムスキャンが古い	黄
前回のシステムスキャンが非常に古い	赤
リアルタイム保護が無効	赤
アンチウイルス保護レベルの設定が消極的	黄
自動アップデートは無効です	赤
前回のアップデートは1日前です	赤

問題	色
アンチスパムは無効	灰色

問題を修正するには、次の手順で行ってください：

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

3.3. ネットワークセキュリティ状態ボタン

ネットワークセキュリティ状態ボタンが緑なら、心配することは何ともありません。それ以外の場合は、ボタンが赤になると、お使いのコンピュータが高い危険にさらされています。

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

問題	色
ファイアウォールは無効	赤
ステルスモードは無効	赤
ワイヤレス接続が安全ではありません	赤

問題を修正するには、次の手順で行ってください：

1. ネットワークセキュリティ状態ボタンをクリックしてください。
2. 一つずつ修正するには修正ボタンをクリックし、すべてを一括して修正するにはすべてを修正ボタンをクリックしてください。
3. 問題がその場で修正されない場合、ウィザードに沿って修正してください。

3.4. 個人識別情報コントロール状態ボタン

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

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

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

問題を修正するには、次の手順で行ってください：

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

4. クイックタスク

4つの状態ボタンの下には、クイックタスク画面があります。

4.1. セキュリティ

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

セキュリティモジュールに入るには、セキュリティタブをクリックしてください。

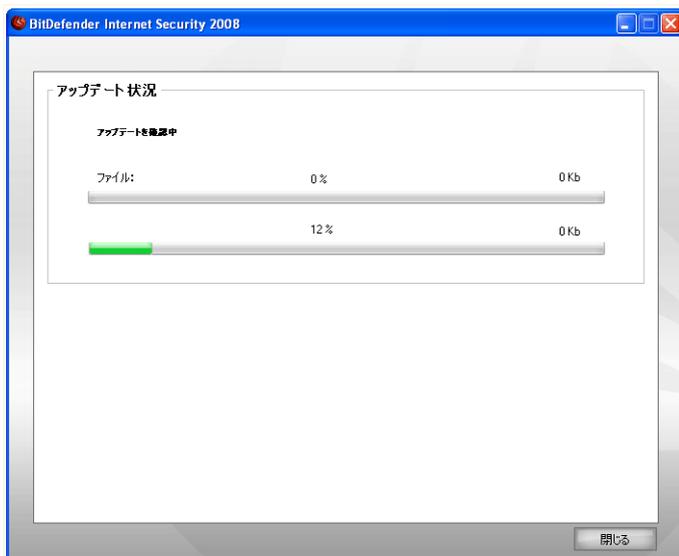
次のボタンが使えます：

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

4.1.1. BitDefender のアップデート

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

デフォルトでは、お使いのコンピュータの起動時、およびその後は1時間毎にアップデートをチェックします。BitDefender をアップデートするには、今すぐアップデートをクリックしてください。アップデート処理が開始され、次のようなウ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、順次上書きされていきます。この方法により、アップデート処理は製品の動作に影響せず、同時に脆弱性も除外されます。

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



注意

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

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

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

再起動をクリックすると、すぐにシステムを再起動します。

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

4.1.2. BitDefender によるスキャン

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

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



注意

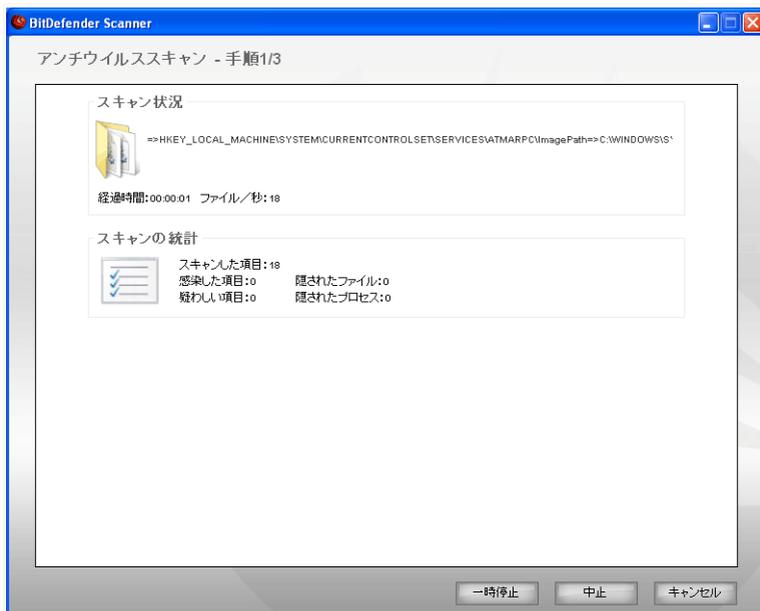
ディープシステムスキャンおよび完全システムスキャンのタスクは、システム全体を調べるため、スキャン処理には時間がかかります。ですから、これらのタスクは比較的暇なときに実行するか、できればシステムが使われていないときに実行することをお勧めします。

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

次の3つの手順に従って、スキャン処理を完了させてください。

手順1/3 - スキャン

BitDefenderは、選択したオブジェクトのスキャンを開始します。



スキャン

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



注意

スキャンの内容によっては、スキャン処理に時間がかかる場合があります。

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

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

BitDefender がスキャンを完了するまでお待ちください。

手順2/3 - アクションを選択

スキャンが完了したら、スキャンの結果を表示するウィンドウが新たに開きます。



アクション

お使いのシステムに影響する問題の数を確認できます。

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

問題のそれぞれのグループごと一括して実行されるアクションを選ぶか、問題ごとに個別のアクションを指定できます。

メニューには、次のオプションが表示されます：

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

指定したアクションを適用するには、続けるをクリックしてください。

手順3/3 - 結果を表示

BitDefender が問題の修正を完了したら、スキャンの結果が新しいウ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。レポートファイルは、対応するタスクのプロパティウインドウにある **ログ** 画面に自動で保存されます。



重要項目

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

終了をクリックして、ウインドウを閉じてください。

BitDefender はいくつかの問題を解決できませんでした

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

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

BitDefender はパスワード保護された項目を検出しました

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

これらの項目が安全であることを確認するには：

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

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

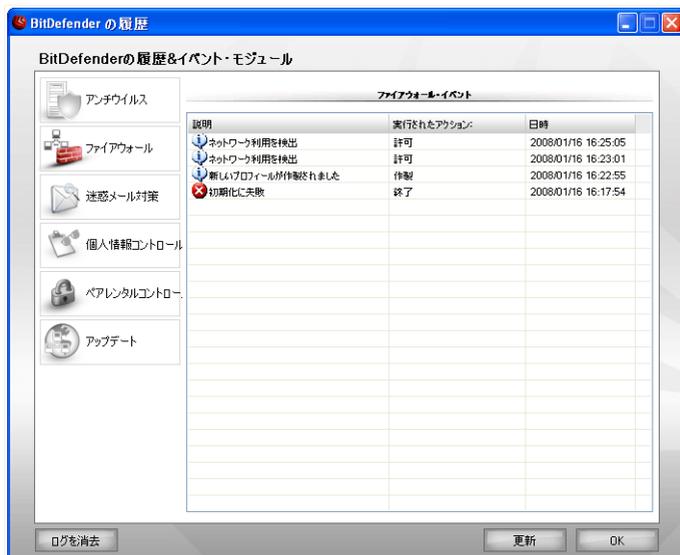
BitDefender は疑わしいファイルを検出しました

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

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

5. 履歴

BitDefender Security Center ウィンドウの下部にある履歴リンクは、BitDefender の履歴&イベントを表示する別のウ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。



イベント

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

- アンチウイルス
- ファイアウォール
- アンチスパム
- 個人情報

- ペアレンタルコントロール
- アップデート

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

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

6. 登録

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

6.1. 手順 1/3 – BitDefender Internet Security 2008 を登録

登録ウィザード - 手順 1 / 3

登録

これはBitDefender Internet Security 2008 試用版です。この製品を試用するには、「製品の評価を継続」にチェックして、「次へ」をクリックしてください。製品を登録するには、「製品を登録」にチェックし、お客様のライセンスキーを入力してください。

BitDefender のライセンスは、次のオンラインストアで購入できます: **クリック!**

この製品の評価を続ける
 製品を登録

新しいキーを入力:


お使いのライセンスキーが見つからない場合は、次を探してください:
 - 製品登録カード
 - CD-ROM のラベル
 - オンライン購入の際に受け取った電子メール

次へ > キャンセル

登録

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

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

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

次へをクリックしてください。

6.2. 手順2/3 – BitDefender アカウントを作成

登録ウィザード - 手順 2 / 3

製品を登録

技術サポートを受けたり、お使いのライセンスキーを安全に保管して後で取り出したり、特價販売などを利用するために、BitDefender アカウントを作成するか、既存のアカウントにログインしてください。

既存の BitDefender アカウントにログイン

電子メール:

パスワード: [パスワードをお忘れですか？](#)

新しい BitDefender アカウントを作成

電子メール:

パスワード:

パスワードを再入力:

名:

姓:

国:

アカウントは後で作成

次へ > キャンセル

アカウントの作成

BitDefender アカウントを持っていません

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

**注意**

アカウントを後日作成される場合は、該当するオプションを選択してください。

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

- 電子メール - お使いの電子メールアドレスをご入力ください。
- パスワード - 上で指定したユーザの有効なパスワードを入力してください。

**注意**

パスワードは、半角英数字で4文字以上にしてください。

- パスワードを再入力 - 上で入力したパスワードを再度入力してください。
- 名 - お名前をご入力ください。
- 姓 - 苗字をご入力ください。
- 国 - お住まいの国名を選択してください。

**注意**

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

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

次へをクリックしてください。

すでに BitDefender アカウントを持っています

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

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

**注意**

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

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

次へをクリックしてください。

6.3. 手順 3/3 – BitDefender Internet Security 2008 を登録

**概要**

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

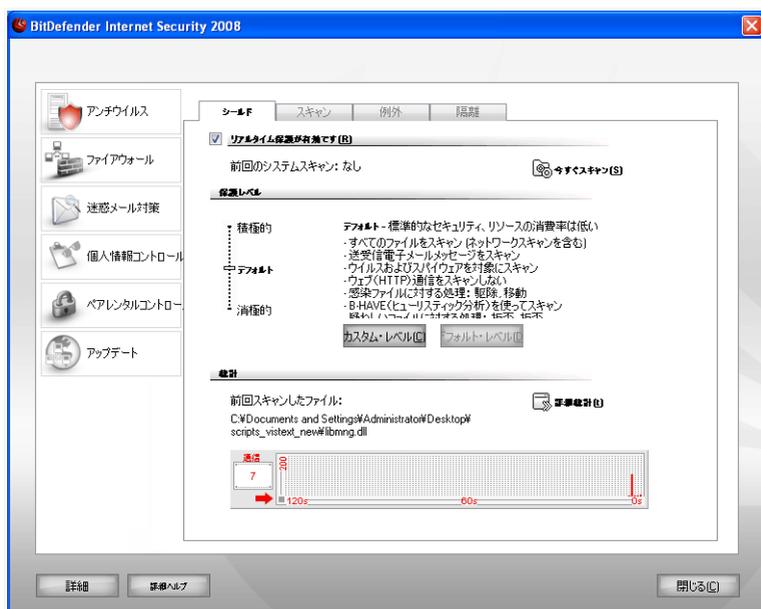
完了をクリックして、ウィンドウを閉じてください。

詳細なセキュリティ管理

7. 設定コンソール

BitDefender Internet Security 2008には、BitDefender の詳細な設定と管理を行える設定コンソールがついています。

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



設定コンソール

設定コンソールは、次のモジュールに分かれています：アンチウイルス、ファイアウォール、アンチスパム、個人情報、保護者による管理、およびアップデート。これで、指摘されたセキュリティの問題の種類に応じて、BitDefender を簡単に管理できます。

設定コンソールの左側には、モジュールの選択肢が表示されます：

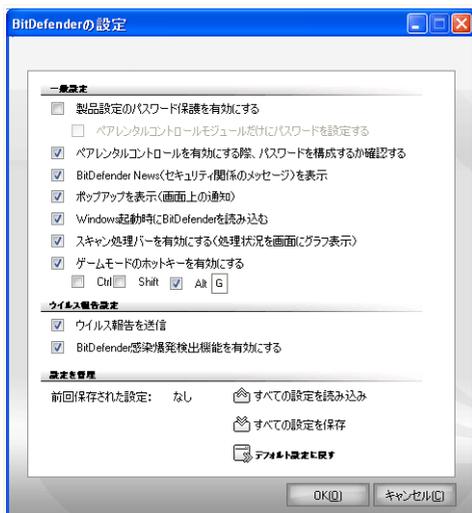
- **アンチウイルス** - ここからアンチウイルスモジュールを設定できます。
- **ファイアウォール** - この項では、ファイアウォールモジュールを設定できます。
- **アンチスパム** - この項では、アンチスパムモジュールを設定できます。
- **個人情報** - ここから個人情報コントロールモジュールを設定できます。
- **保護者による管理** - この項では、ペアレンタルコントロールモジュールを設定できます。
- **アップデート** - ここからアップデートモジュールを設定できます。

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

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

7.1. 一般設定

BitDefender Internet Security 2008の一般設定を行い、その設定を管理するには、詳細をクリックしてください。新しいウィンドウが開きます。



一般設定

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

7.1.1. 一般設定

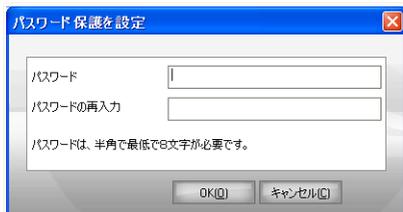
- 製品設定のパスワード保護を有効にする - BitDefender の設定を保護するため、パスワード保護を有効にします。



注意

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

このオプションを選ぶと、次のウィンドウが開きます：



パスワードを入力

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

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

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モジュールだけにパスワードを設定するをチェック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ら、BitDefender の設定を変更するために製品の修復が必要です。

- 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設定するか確認 - このオプションが有効で、パスワードが設定されていない場合、ペアレンタルコントロールを有効にする際パスワード設定を求められます。
- 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、ウイルスの発生に関するセキュリティ通知を時折表示します。
- ポップアップ（画面上の通知）を表示 - 製品の状態に関するポップアップウィンドウを表示します。
- Windows の起動時に BitDefender を読み込む - システム起動時に、自動で BitDefender を起動します。このオプションを選択しておくことをお勧めします。
- スキャン処理バーを有効にする（処理状況を画面にグラフ表示） - **スキャン処理**バーを有効/無効にします。スキャン処理バーを表示させたくない場合はこのチェックボックスのチェックを外してください。



注意

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

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

ホットキーを変更するには：

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

7.1.2. ウィルスレポートの設定

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

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

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

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

7.1.3. 設定を管理

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



重要項目

管理者権限を持つユーザだけが、設定の保存および読み込みを行えます。

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

8. アンチウイルス

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

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

BitDefenderが提供する保護は、2つのカテゴリに分類できます：

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

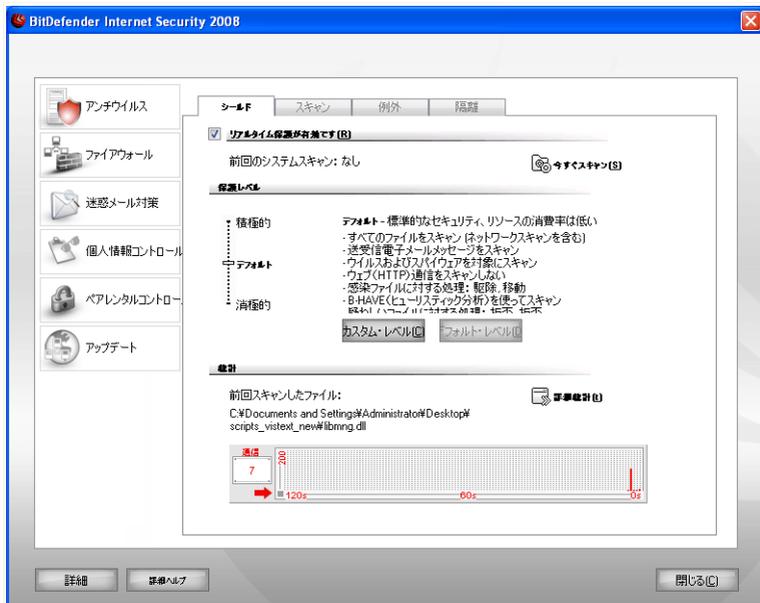
このガイドのアンチウイルスの項には、次のトピックが含まれています：

- **オンアクセススキャン**
- **オンデマンドスキャン**
- **スキャンから除外されるオブジェクト**
- **隔離領域**

8.1. オンアクセススキャン

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

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



リアルタイム保護



重要項目

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

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

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

8.1.1. 保護レベルを設定

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

3つの保護レベルがあります：

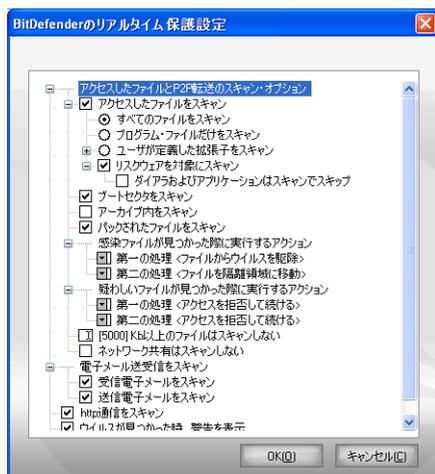
保護レベル	説明
消極的	<p>基本的に必要なセキュリティはカバーします。リソース消費レベルは低いです。</p> <p>ウイルスを対象にプログラムおよび受信メールメッセージだけスキャンします。従来のシグネチャ方式のスキャンに加え、ヒューリスティック分析も使用されます。感染ファイルに対するアクションは次の通りです：ファイルを感染除去/アクセス拒否。</p>
デフォルト	<p>標準的なセキュリティを提供します。リソース消費レベルは低いです。</p> <p>すべてのファイルと受信&送信メールメッセージが、ウイルスおよびスパイウェアを対象にスキャンされます。従来のシグネチャ方式のスキャンに加え、ヒュー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

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

8.1.2. カスタム保護レベル

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

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



シールド設定

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



注意

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

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

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

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

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

■電子メール通信をスキャン - 電子メール通信をスキャンします。

次のオプションが指定できます：

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

■http 通信をスキャン - http 通信をスキャンします。

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

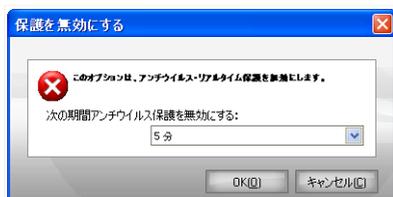
感染ファイルについては、警告ウィンドウにウイルス名、そのパス、BitDefender が実行したアクション、ウイルスに関する詳細情報を確認できる BitDefender サイトへのリンクが表示されます。感染電子メールについては、送信者と宛先の情報も警告ウィンドウで表示されます。

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

変更を保存してウィンドウを閉じるには、OKをクリックしてください。

8.1.3. リアルタイム保護を無効にする

リアルタイム保護を無効にしようとすると、警告ウインドウが開きます。



リアルタイム保護を無効にする

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



警告

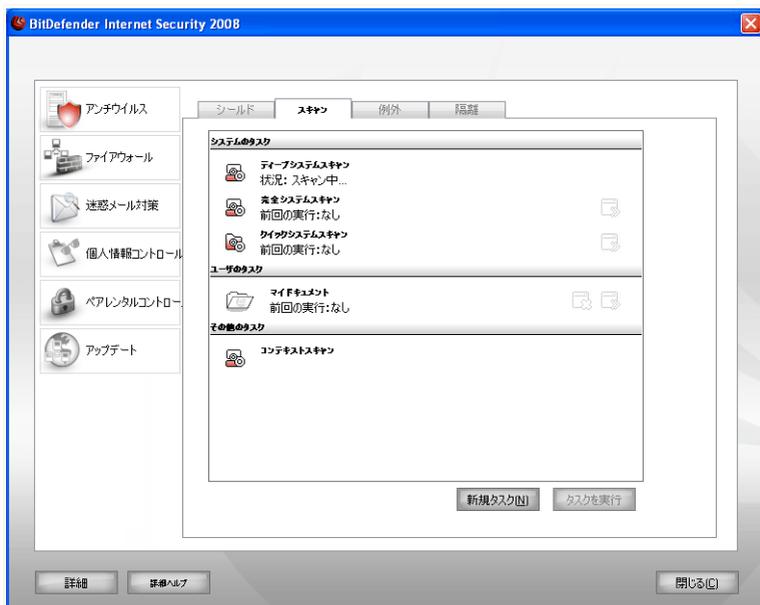
これはセキュリティ上の重要な判断を必要とします。リアルタイム保護を無効にする場合は、できるだけ短期間をすることをお勧めします。リアルタイム保護が無効だと、マルウェアの脅威から保護されません。

8.2. オンデマンドスキャン

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

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

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



スキャンタスク

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

8.2.1. スキャンタスク

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

各タスクには、タスクを設定し、スキャン結果を確認するプロパティウインドウがあります。詳細については、「[スキャンタスクを設定](#)」 (p. 61)をご参照ください。

スキャンタスクには3つのカテゴリがあります：

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

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



注意

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

- ユーザタスク - ユーザが指定したタスクを一覧できます。

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

- その他のタスク - その他のスキャンタスク一覧があります。これらのスキャンは、このウ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可能です。

各タスクの右には3つのボタンがあります：

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



注意

システムタスクには使えません。システムタスクを削除することはできません。

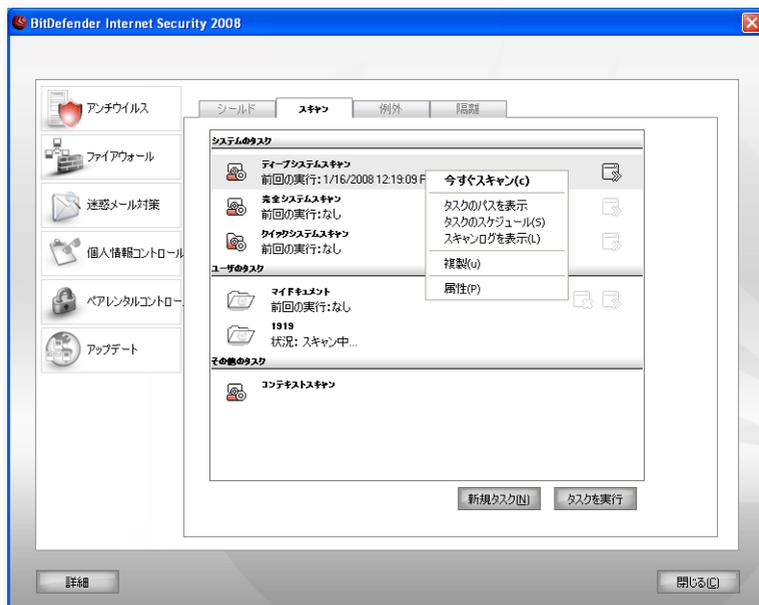
-  今すぐスキャン - 選択したタスクを実行して、**即座にスキャン**を開始します。

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

8.2.2. ショートカットメニューを使う

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

ショートカットメニューには、次のコマンドが用意されています：



ショートカットメニュー

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



注意

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

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

**注意**

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

- 削除 – 選択したタスクを削除します。

**注意**

システムタスクには使えません。システムタスクを削除することはできません。

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

**注意**

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

8.2.3. スキャンタスクを作成

スキャンタスクを作成するには、次のいずれかの方法を使えます：

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

8.2.4. スキャンタスクを設定

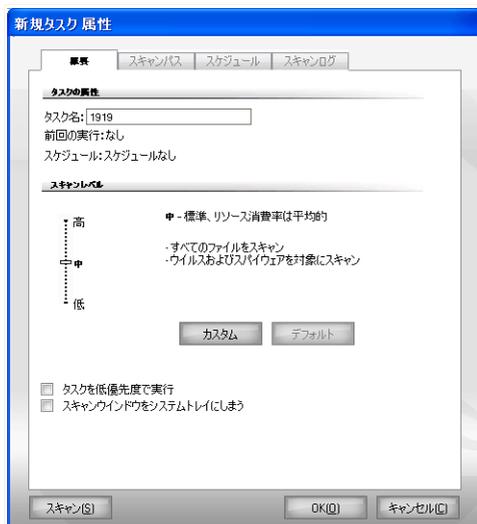
各スキャンタスクには、スキャンオプション設定、スキャン対象設定、タスクスケジュール、レポート表示をするためのプロパティウインドウがあります。このウインドウを開くには、タスクの右に表示される開くボタンをクリックしてください（あるいはタスクを右クリックし、開くをクリックしてください）。

**注意**

ログの表示およびログタブの詳細については、「**スキャンログを表示**」(p. 80)をご参照ください。

スキャン設定を行う

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



概要

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

スキャンレベルの選択

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

3つのスキャンレベルがあります：

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

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

スキャン処理に関する、一連の一般的なオプションも用意されています：

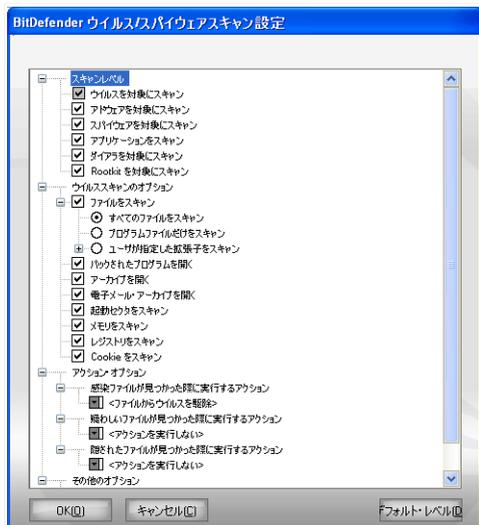
オプション	説明
タスクを低優先度で実行	スキャン処理の優先順位を下げます。他のプログラムがより高速で実行されますが、スキャン処理が完了するまでの時間が長くなります。
スキャンウィンドウをシステムトレイにしまう	スキャンウィンドウを システムトレイ にしまいます。BitDefender アイコンをダブルクリックすれば開きます。

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

スキャンレベルをカスタマイズ

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

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

スキャンオプションは、4つのカテゴリに分類されています：

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

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

次のオプションが指定できます：

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

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

次のオプションが指定できます：

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

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

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

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

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

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

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

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



注意

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

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

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

**注意**

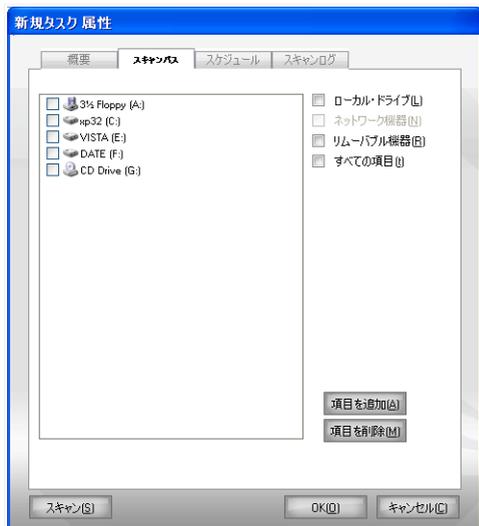
検出されたファイルが無視するように指定するか、選択したアクションが失敗したら、スキャンウィザードでアクションを選択しなければなりません。

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

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

スキャンの対象を設定

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



スキャンの対象

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

この画面には、次のボタンが表示されます：

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

**注意**

ファイル/フォルダをドラッグ&ドロップして一覧に追加することもできます。

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

**注意**

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

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

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

**注意**

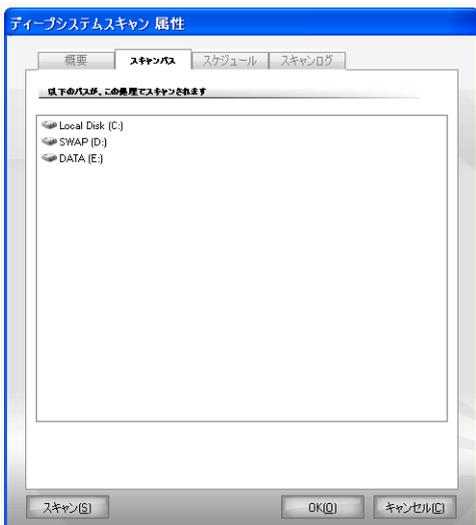
お使いのコンピュータ全体をスキャンするには、すべての項目チェックボックスを選択してください。

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

システムタスクのスキャン対象を表示

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

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

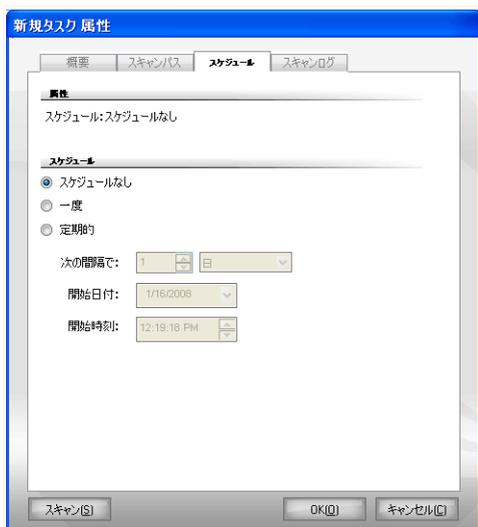
完全システムスキャンおよびディープシステムスキャンはすべてのローカルドライブをスキャンしますが、クイックシステムスキャンではWindowsおよびプログラムファイルフォルダだけをスキャンします。

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

スキャンタスクをスケジュール

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

特定のタスクのスケジュールを表示するか編集するには、タスクを右クリックして、タスクのスケジュールを選んでください。次のウ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、次のオプションのいずれかを選択してください：

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

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

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

8.2.5. スキャンするオブジェクト

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



注意

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

スキャン方式

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

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

即座にスキャン

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

スキャンタスクを実行するには、次の方法のいずれかを使ってください：

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

BitDefender スキャナが表示され、スキャンが開始されます。 詳細については、「**BitDefender Scanner**」 (p. 75) をご参照ください。

コンテキストスキャン

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



コンテキストスキャン

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

BitDefender スキャナが表示され、スキャンが開始されます。 詳細については、「**BitDefender Scanner**」 (p. 75) をご参照ください。

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

ドラッグ&ドロップスキャン

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



ファイルをドラッグ



ファイルをドロップ

BitDefender スキャナが表示され、スキャンが開始されます。 詳細については、「[BitDefender Scanner](#)」 (p. 75) をご参照ください。

手動スキャン

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



注意

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

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

次のウィンドウが開きます：



スキャンしたいオブジェクトを選び、OKをクリックしてください。

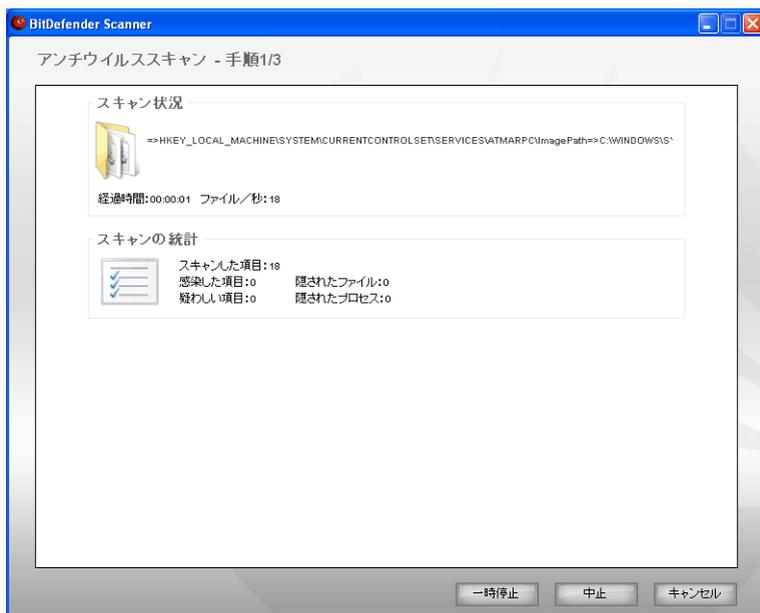
BitDefender スキャナが表示され、スキャンが開始されます。詳細については、「**BitDefender Scanner**」(p. 75)をご参照ください。

BitDefender Scanner

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

手順1/3 - スキャン

BitDefenderは、選択したオブジェクトのスキャンを開始します。



スキャン

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



注意

スキャンの内容によっては、スキャン処理に時間がかかる場合があります。

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

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

BitDefender がスキャンを完了するまでお待ちください。

手順2/3 - アクションを選択

スキャンが完了したら、スキャンの結果を表示するウィンドウが新たに開きます。



アクション

お使いのシステムに影響する問題の数を確認できます。

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

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

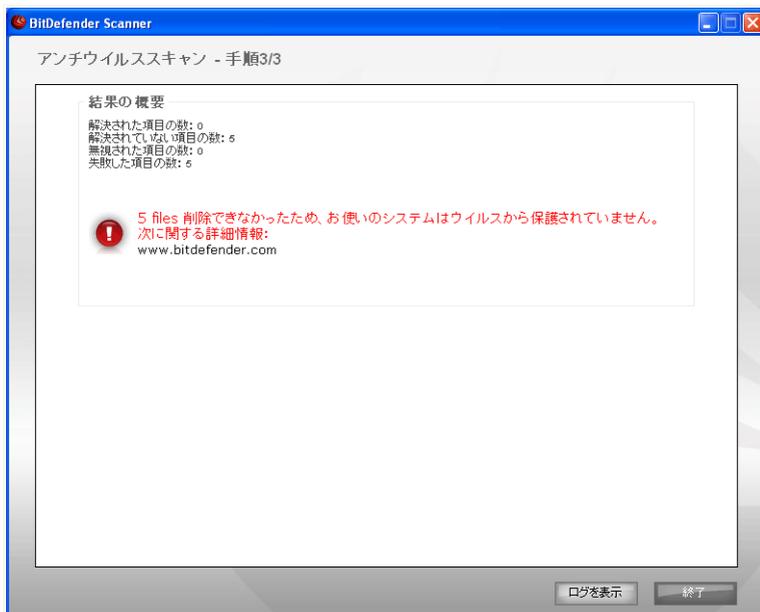
メニューには、次のオプションが表示されます：

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

指定したアクションを適用するには、続けるをクリックしてください。

手順3/3 - 結果を表示

BitDefender が問題の修正を完了したら、スキャンの結果が新しいウ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。レポートファイルは、対応するタスクのプロパティウインドウにある**ログ**画面に自動で保存されます。



重要項目

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

終了をクリックして、ウインドウを閉じてください。

BitDefender はいくつかの問題を解決できませんでした

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

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

BitDefender はパスワード保護された項目を検出しました

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

これらの項目が安全であることを確認するには：

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

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

BitDefender は疑わしいファイルを検出しました

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

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

8.2.6. スキャンログを表示

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

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

2つのボタンがあります：

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



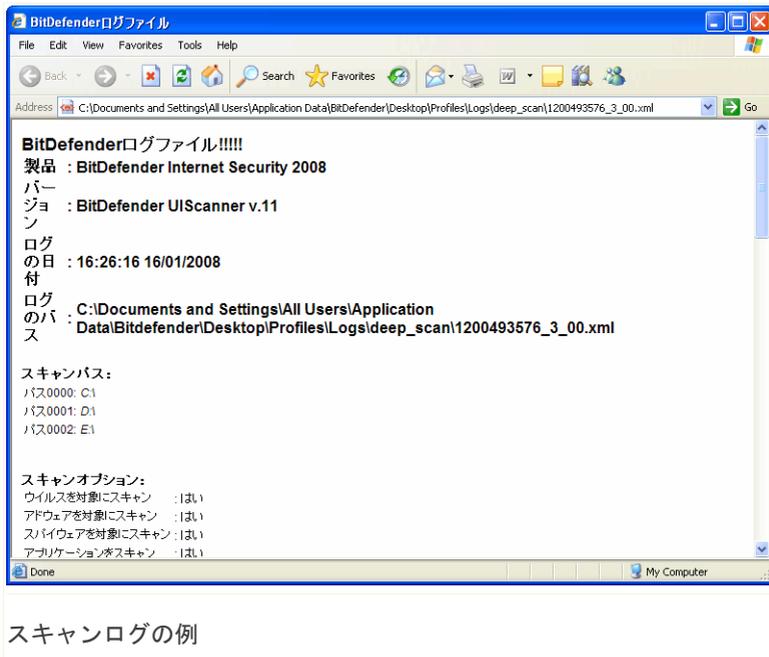
注意

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

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

スキャンログの例

次の図は、スキャンログの例です：



スキャンログの例

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

8.3. スキャンから除外されるオブジェクト

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

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

スキャンからは、2種類のオブジェクトが除外できます：

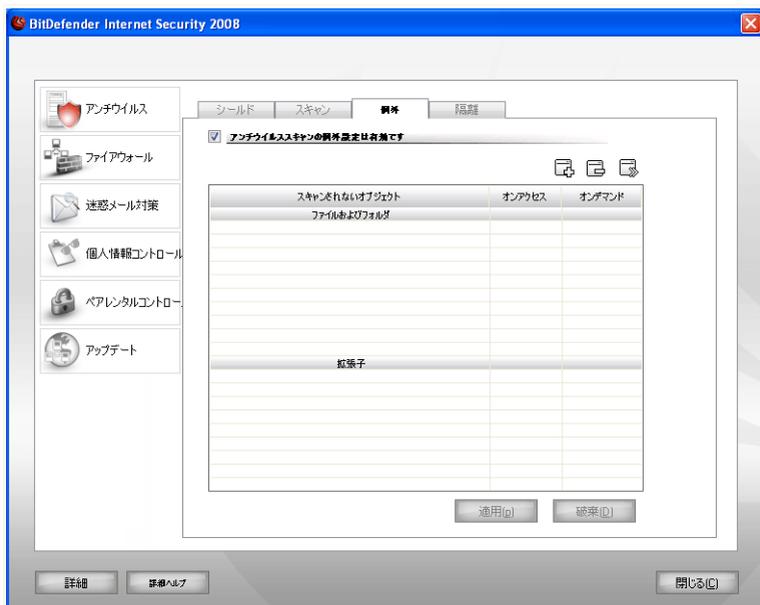
- パス - 指定したパスが示すファイルあるいはフォルダ（その中のすべてのオブジェクトを含む）がスキャンから除外されます。
- 拡張子 - 指定した拡張子を持つすべてのファイルがスキャンから除外されます。



注意

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

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



例外

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



注意

ここで指定された例外は、コンテキストスキャンには適用されません。

表から項目を削除するには、 削除ボタンをクリックしてください。

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

**注意**

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

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

8.3.1. スキャンからパスを除外

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

手順1/3 - オブジェクト形式を選択

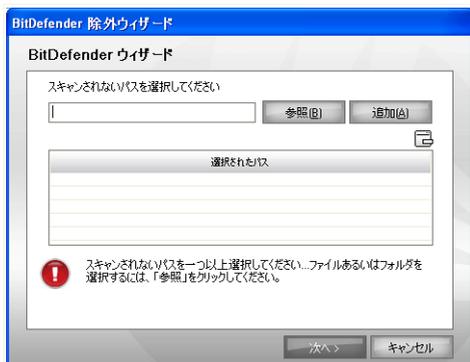


オブジェクト形式

スキャンからパスを除外するオプションを選択してください。

次へをクリックしてください。

手順2/3 - 除外するパスを指定



除外されるパス

スキャンから除外するパスを指定するには、次のいずれの方法を使ってください：

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



注意

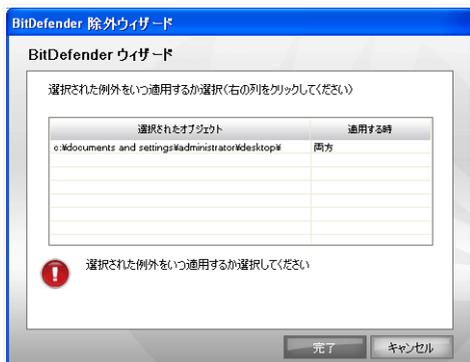
指定したパスが存在しないと、エラーメッセージが表示されます。OKをクリックし、パスが正しいかどうか確認してください。

パスを追加すると、一覧に表示されます。パスは好きな数だけ追加できます。

表から項目を削除するには、削除ボタンをクリックしてください。

次へをクリックしてください。

手順3/3 - スキャン方式を選択



スキャン方式

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

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

終了をクリックしてください。

適用をクリックして、変更を保存してください。

8.3.2. スキャンから拡張子を除外

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

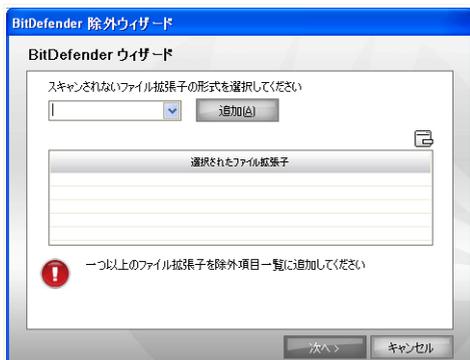
手順1/3 - オブジェクト形式を選択



オブジェクト形式

スキャンから拡張子を除外するオプションを選択してください。
次へをクリックしてください。

手順2/3 - 除外される拡張子を指定



除外される拡張子

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

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



注意

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

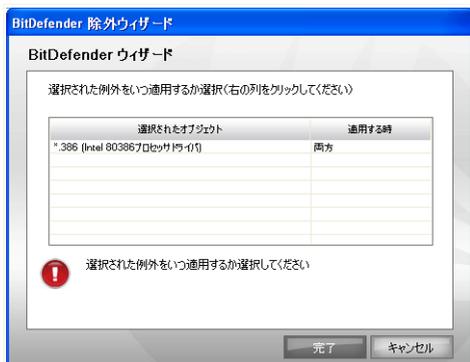
- スキャンから除外したい拡張子を編集欄に入力し、追加をクリックしてください。

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

表から項目を削除するには、 削除ボタンをクリックしてください。

次へをクリックしてください。

手順3/3 - スキャン方式を選択



スキャン方式

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

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

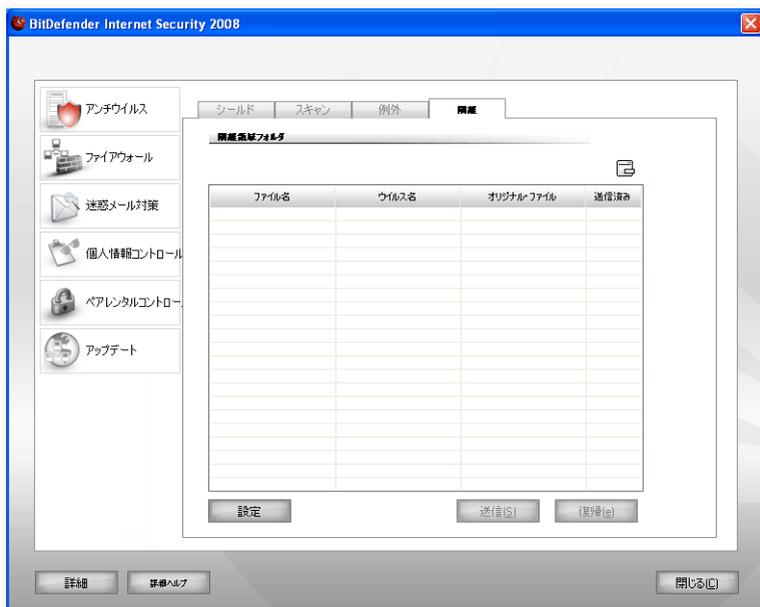
終了をクリックしてください。

適用をクリックして、変更を保存してください。

8.4. 隔離領域

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

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



隔離領域

8.4.1. 隔離されたファイルを管理

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



注意

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

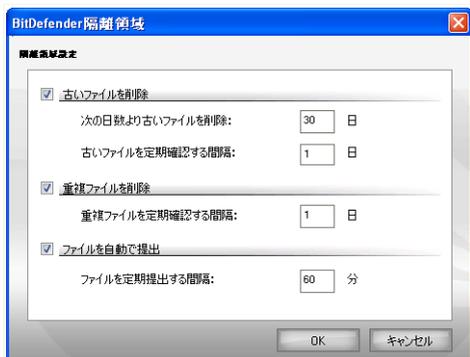
各領域から選択したファイルを削除するには、 削除ボタンをクリックしてください。選択したファイルを元の場所へ戻すには、復旧をクリックしてください。

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

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

8.4.2. 隔離領域設定を構成

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



隔離領域設定

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

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



注意

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

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



注意

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

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



注意

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

変更を保存してウィンドウを閉じるには、OKをクリックしてください。

9. ファイアウォール

ファイアウォールは、許可していない受信および発信接続からお使いのコンピュータを守ります。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、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お使いの場合は、特にファイアウォールが重要です。

ステルスモードでは、お使いの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）を自動で検出し保護することができます。

このユーザガイドのファイアウォールの項には、次の内容があります：

- **ファイアウォールの知識**
- **ファイアウォールの状態**
- **通信の保護**
- **詳細設定**
- **ファイアウォールのアクティビティ**
- **ネットワークゾーン**

9.1. ファイアウォールの知識

BitDefender のファイアウォールは、お客様が設定を行わなくても、お使いのネットワーク/インターネット接続に最高の保護を提供するように設計されています。直接インターネットに接続していても、単一のネットワークあるいは複数のネットワーク（Ethernet、ワイヤレス、VPN、あるいは他のネットワーク形式）に接続していても、接続先が信用できてもできなくても、対応する環境に合わせてファイアウォールが自ら設定を行います。

デフォルトでは、BitDefender は自動的にお使いのコンピュータのネットワーク設定を検出し、対応する基本的なファイアウォールプロフィールを作成します。また検出したネットワークをその設定に基づき、信頼できる/信頼できないネットワークゾーンとしてプロフィールに追加します。

9.1.1. ファイアウォールプロファイルの説明

ファイアウォールプロファイルは、アプリケーションのネットワーク/インターネット利用を制御するルールのセットです。

お使いのコンピュータのネットワーク設定により、BitDefender は自動的に特定の種類のプロファイルを作成します。基本的なプロファイルには、システムアプリケーションおよび BitDefender コンポーネントが必要とする、ネットワーク利用ルールあるいは最低限のインターネット利用ルールが含まれています。



注意

接続しているネットワークの数に関わらず、単一のファイアウォールプロファイルが作成されます。

基本的なプロファイルには3つの種類があります：

プロファイル	説明
直接接続	インターネットへの直接接続を可能とするネットワーク設定のために推奨される最低限のインターネット利用ルールを含みます。このルールでは、ネットワークユーザがお使いのコンピュータにアクセスすることも、お客様がネットワークを参照することもできません。
信頼できない	信頼できないネットワークを使うネットワーク設定のために推奨されるネットワーク利用ルールが含まれています。このルールでは、お客様がネットワークを参照することができますが、他のネットワーク利用者はお使いのコンピュータにアクセスできません。
信頼できる	信頼できるネットワークを使うネットワーク設定のために推奨されるネットワーク利用ルールが含まれています。ネットワークの利用に制限はありません。つまりお客様が、ネットワーク共有、ネットワークプリンタ、および他のネットワークリソースを利用できることを意味します。同時にネットワーク利用者もお使いのコンピュータに接続し、お使いの共有を利用できます。

アプリケーションがインターネットに接続しようとする時、プロフィールに対応するルールが追加されます。デフォルトでルールが設定されていないアプリケーションがインターネットを利用しようとした際に、許可するか拒否するか選択できます。あるいは、デフォルトでホワイトリストにあるアプリケーションだけを許可し、他のアプリケーションは許可を確認するように設定することもできます。



注意

インターネットに始めて接続しようとするアプリケーションのインターネット利用方針を指定するには、**状態**の項へ行き、保護レベルを設定してください。既存のプロフィールを編集するには、**通信**の項へ行き、プロフィールを編集をクリックしてください。

9.1.2. ネットワークゾーンの説明

ネットワークゾーンは、ネットワーク内のコンピュータ、あるいはお使いのコンピュータから完全に切り離されたネットワーク全体、あるいは逆にお使いのコンピュータを検出して接続できるネットワーク全体を意味します。現実的に言えば、ゾーンとは、お客様のコンピュータへの接続を許可された、あるいは拒否されたIPアドレスあるいはIPアドレスの範囲です。

デフォルトでは、BitDefender は特定のネットワーク設定にゾーンを自動で追加します。ネットワーク全体に適用される適切なネットワーク利用ルールを作成すると、ゾーンがプロフィールへ追加されます。

ゾーンには2種類あります：

ゾーンの種類	説明
信頼できるゾーン	<p>信頼できるゾーンからのコンピュータは、お使いのコンピュータと互いに接続可能です。</p> <p>そのようなゾーンからの接続試行およびお使いのコンピュータからそのようなゾーンへの接続試行は、許可されます。ネットワークが信頼できるゾーンに追加されると、そのネットワーク共有、ネットワークプリンタ、および他のネットワークリソースが無制限に利用可能となります。またネットワーク利用者は、お使いのコンピュータに接続し、お使いの共有を利用できます。</p>

ゾーンの種類	説明
信頼できないゾーン	<p>信頼できないゾーンからのコンピュータは、お使いのコンピュータとは互いに接続できません。</p> <p>そのようなゾーンからの接続試行およびお使いのコンピュータからそのようなゾーンへの接続試行は、ブロックされます。ICMP通信は拒否され、ステルスモードが有効のため、お使いのコンピュータは、そのゾーン内のコンピュータからは見えません。</p>



注意

ゾーンを編集するには、**ゾーン**の項を参照してください。特定のゾーンに対応したルールを編集するには、**通信**の項へ行き、プロフィールを編集をクリックしてください。

9.1.3. ファイアウォールの操作

インストール後にシステムを再起動すると、BitDefender は自動的にお使いのネットワーク設定を検出し、適切な基本的プロフィールを作成し、検出されたネットワークに基づいてゾーンを追加します。



注意

インターネットに直接接続している場合、対応するネットワーク設定にネットワークゾーンは作成されません。2つ以上のネットワークに接続されているなら、対応するネットワークにゾーンが追加されます。

他のネットワークに接続するかネットワーク接続を無効にすることでネットワーク設定が変更される度に、新しいファイアウォールプロフィールが作成されます。同時に、ネットワークゾーンがそれに応じて変更されます。

新しいファイアウォールプロフィールが作成されると、対応するネットワーク設定に戻った際に再度読み込めるよう、古いプロフィールは保存されます。

ネットワーク設定によって、BitDefender はそれに応じた設定をします。これが BitDefender ファイアウォールがデフォルトで設定される仕組みです：

- インターネットに直接接続している場合、他のネットワークにどのように接続されているかに関わらず、直接接続プロフィールが作成されます。あるいは、BitDefender は信頼できないファイアウォールプロフィールを作成します。



注意

セキュリティ上の判断で、デフォルトでは信頼できるプロフィールは作成されません。信頼できるプロフィールを作成するには、既存のプロフィールをリセットする必要があります。詳細については、「**プロフィールをリセット**」(p. 109)を参照してください。

- ゾーンは、ネットワーク設定に基づいて追加されます。

ゾーンの種類	ネットワーク設定
信頼できるゾーン	<p>ゲートウェイなしのプライベートIP - ローカルエリアネットワーク (LAN) の一部で、インターネットに接続しないコンピュータです。そのような状態の例には、家族でファイル、プリンタ、他のリソースを共有できるホームネットワークがあります。</p> <p>ドメイン制御が検出されたプライベートIP - LANの一部で、ドメインに接続されたコンピュータです。そのような状態の例には、ユーザが同一ドメイン内のファイルや他のリソースを共有できるオフィスネットワークがあります。ドメインは、利用者のコンピュータが従う一連の方針が存在することを暗示します。</p>
信頼できないゾーン	<p>公開 (セキュアでない) ワイヤレス - ワイヤレスのローカルエリアネットワーク (WLAN) の一部であるコンピュータです。このような状態の例には、公共の場でフリーアクセスポイントを使ってインターネットを利用する場合があります。</p>



注意

ゾーンは、次のようなネットワーク設定では作成されません：

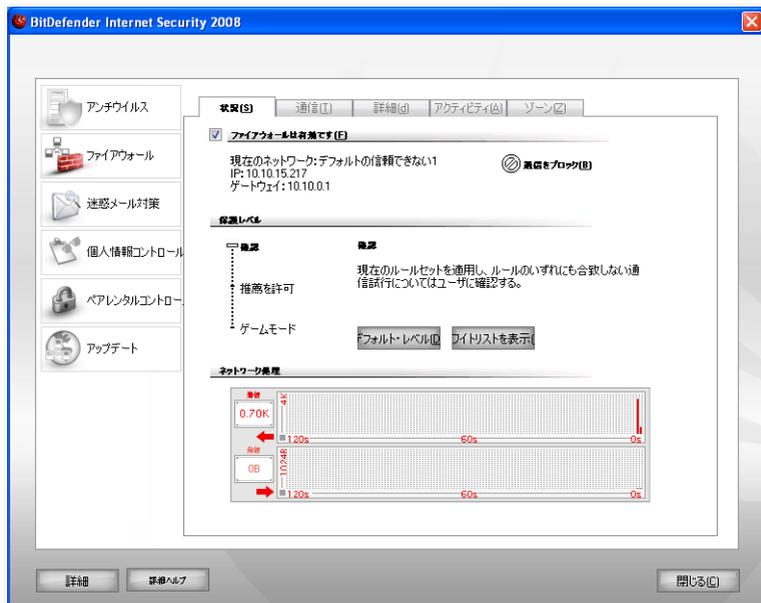
- ・ 公開 (ルート可能) IP - インターネットに直接接続されたコンピュータです。
- ・ ゲートウェアありのプライベートIP、ただしドメイン制御は検出されない - ドメインの一部でないまま、LANの一部ではあり、インターネットにはゲートウェ

イ経由で接続するコンピュータです。このような状態の例には、ユーザがファイアウォールや他のリソースを共有できる学校のネットワークがあります。

- ステルスモードは有効です。
- VPNおよびリモート接続は許可されます。
- インターネット接続共有は、信頼できないゾーンでは許可されません。
- ホワイトリスト内のアプリケーションは、自動的にアクセスを許可されますが、他のアプリケーションについては、それらが初めて接続しようとした際に、お客様に許可するか確認します。

9.2. ファイアウォールの状態

ファイアウォール保護を設定するには、設定コンソールでファイアウォール>状態をクリックしてください。次のウィンドウが開きます：



ファイアウォールの状態

この項では、ファイアウォールを有効／無効にし、すべてのネットワーク／インターネット通信をブロックし、新しいイベントに対するデフォルトの対応を設定できます。



重要項目

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

すべてのネットワーク／インターネット通信をブロックするには、 通信をブロックをクリックし、確認のためはいををクリックしてください。これでお使いのコンピュータはネットワーク上の他のすべてのコンピュータから隔離されます。

後で通信のブロックを解除するには、 通信をブロック解除をクリックしてください。

この項の下部には、送受信される通信に関する BitDefender 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を表示しています。



注意

グラフは、ファイアウォールが無効でも表示されます。

9.2.1. 保護レベルを設定

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

3つの保護レベルがあります：

保護レベル	説明
ゲームモード	現在のルールを適用し、さらに現在のルールに合致しないすべての通信要求を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およびゲーマーには便利かもしれません。
推奨を許可	現在のルールを適用し、BitDefender が信頼できると知っている（ホワイトリスト内の）プログラムによるすべての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

保護レベル	説明
	<p>認めます。作成された通信ルールは、通信の項で参照できます。</p> <p>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および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&ビデオプレイヤー、チャット、ファイル共有プログラムなどが含まれます。ホワイトリスト内のプログラムを確認するには、ホワイトリストをクリックしてください。</p>
確認	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お客様の指示を仰ぎます。

デフォルトの方針（推奨を許可）を設定するには、デフォルトをクリックしてください。

9.3. 通信コントロール

現在のプロフィールのファイアウォールルールを管理するには、設定コンソールでファイアウォール>通信をクリックしてください。次のウィンドウが開きます：



ファイアウォールの警告

フォルトで適用されます。



重要項目

信頼できるIPあるいはドメインからの受信接続は許可します。

9.3.2. ルールを手動で追加

- ☞ 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。 次のウィンドウが開きます：

次が表示されます：インターネットへ接続しようとす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およびアプリケーションが接続しようとする**ポート**。

このアプリケーションが生成する、関連するIPプロトコルと全ポートを使った、ローカルホストから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てください。ブロックをクリックすると、アプリケーションによるそのIPプロトコルを使ったインターネットの利用は完全に拒否されます。

お客様の回答により、ルールが作成および適用され、一覧に表示されます。次回このアプリケーションが接続しようとする、このルールがデ



ルールを追加

新しいファイアウォールルールを追加するには、次の手順で行ってください：

1. 新しいファイアウォールルールを作成するアプリケーションを選択してください。

アプリケーションを選択するには、参照をクリックし、場所を指定し、OKをクリックしてください。

全アプリケーション用のルールを作成するには、このルールをすべてのアプリケーションに適用をチェックしてください。

2. ルールが適用されるプロトコルを選択してください。

特定のプロトコルを選択できるように、最も一般的なプロトコルの一覧が用意されています。対応するドロップダウンメニューから（ルールを適用する）希望するプロトコルを選択するか、すべてを選択してすべてのプロトコルを指定してください。

次の表は、選択指定が可能な、簡単な説明付きのプロトコルの一覧です：

プロトコル	説明
ICMP	Internet Control Message Protocol - は、Internet Protocol (IP) の拡張版です。ICMPは、エラー、コントロール、情報を持ったメッセージを持つパケットに対応しています。例えば、PINGコマンドは、インターネット接続を試験するためにICMPを使っています。
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。ゲームおよびビデオを使った他のアプリケーションでは、UDPがよく使われます。

3. 対応するメニューからルールアクションを選択してください。

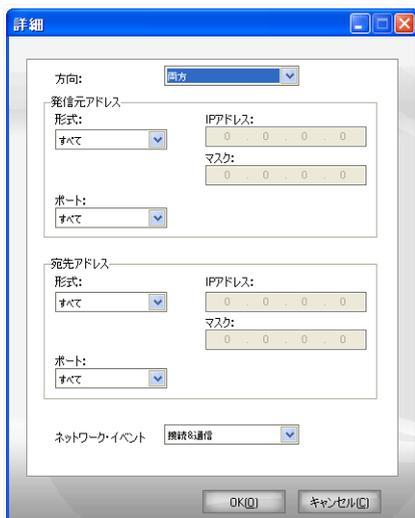
アクション	説明
許可	指定されたアプリケーションは、指定された環境での、ネットワーク/インターネットの使用が許可されます。
拒否	指定されたアプリケーションは、指定された環境での、ネットワーク/インターネットの使用が拒否されます。

4. この前で選択されたプロトコルがTCPまたはUDPの場合、アプリケーションがサーバとして動作するかどうかで、ルールを適用するかしないか指定できます。

アクションをすべてのネットワークイベントに適用するには、他のコンピュータによるこのアプリケーションへの接続を許可にチェックしてください。暗黙のうちに、このアプリケーションがポートを開く権利を許可あるいは拒否することになります。

アクションをUDPの通信およびTCPの通信&接続だけに適用するなら、対応するチェックボックスのチェックを外してください。

さらに詳細なルール設定を行うには、詳細をクリックしてください。新しいウィンドウが開きます：



詳細ルール設定

次の設定を行えます：

- 方向 - 通信方向を選択してください。

形式	説明
外向き	ルールは、発信通信にのみ適用されます。
内向き	ルールは、受信通信にのみ適用されます。
両方	ルールは、双方向に適用されます。

- 発信元アドレス - 発信元のアドレスを指定してください。

発信元のアドレスを指定するには、メニューからアドレス形式を選び、必要なデータを指定してください。次のオプションが指定できます：

形式	説明
すべて	ルールは、すべての発信元アドレスに適用されます。
ホスト	ルールは、発信元が特定のホストの場合にのみ適用されず。ホストのIPアドレスを入力する必要があります。
ネットワーク	ルールは、発信元が特定のネットワークの場合にのみ適用されます。IPアドレスおよびネットワークのマスクを入力する必要があります。
ローカルホスト	ルールは、発信元がローカルホストの場合にのみ適用されます。複数のネットワークインターフェースをお使いなら、ルールを適用するネットワークインターフェースをメニューから選択してください。ルールをすべてのローカルホストに適用するには、すべてを選択してください。
ローカルネットワーク	ルールは、発信元がローカルネットワークの場合にのみ適用されます。複数のネットワークに接続しているなら、ルールを適用するネットワークをメニューから選択してください。ルールをすべてのローカルネットワークに適用するには、すべてを選択してください。

プロトコルとしてTCPあるいはUDPを選択していると、特定のポートあるいは0から65535の範囲を設定できます。ルールをすべてのポートに適用するには、すべてを選択してください。

■宛先アドレス - 宛先のアドレスを指定してください。

宛先アドレスを指定するには、メニューからアドレス形式を選び、必要なデータを指定してください。次のオプションが指定できます：

形式	説明
すべて	ルールは、すべての宛先アドレスに適用されます。
ホスト	ルールは、宛先が特定のホストの場合にのみ適用されます。ホストのIPアドレスを入力する必要があります。
ネットワーク	ルールは、宛先が特定のネットワークの場合にのみ適用されます。IPアドレスおよびネットワークのマスクを入力する必要があります。

形式	説明
ローカルホスト	ルールは、宛先がローカルホストの場合にのみ適用されます。複数のネットワークインタフェースをお使いなら、ルールを適用するネットワークインタフェースをメニューから選択してください。ルールをすべてのローカルホストに適用するには、すべてを選択してください。
ローカルネットワーク	ルールは、宛先がローカルネットワークの場合にのみ適用されます。複数のネットワークに接続しているなら、ルールを適用するネットワークをメニューから選択してください。ルールをすべてのローカルネットワークに適用するには、すべてを選択してください。

プロトコルとしてTCPあるいはUDPを選択していると、特定のポートあるいは0から65535の範囲を設定できます。ルールをすべてのポートに適用するには、すべてを選択してください。

- ネットワークイベント - プロトコルとしてTCPあるいはUDPを選択した場合、ルールが適用されるネットワークイベントを選んでください。

詳細設定ウィンドウを閉じるには、OKをクリックしてください。

ファイアウォールルールを追加するには、追加をクリックしてください。

9.3.3. ルールを管理

これまでに現在のプロフィールで作成したルールが、表に表示されます。

システムあるいは BitDefender プロセスに関連したルールを隠すには、システムプロセスを隠すチェックボックスを選択してください。

ルールは、上から順に優先順位に基づいて並んでいます。つまり一番上のルールが最も高い優先順位を持っています。ルールを上下に移動して優先順位を変更できる詳細表示画面を表示するには、プロフィール編集をクリックしてください。

ルールを削除するには、対象を選択して  ルールを削除ボタンをクリックしてください。

ルールを編集するには、対象を選択して  ルールを編集ボタンをクリックするか、そのルールをダブルクリックしてください。

**注意**

利用できるコンテキストメニューの内容は次の通りです：ルールを追加、ルールを削除、ルールを編集。

9.3.4. プロフィール編集

プロフィール編集をクリックすれば、プロフィールが編集できます。次のウィンドウが開きます：

現在のルールセット 詳細表示

内向きのルール:

アプリケーション	プロ...	発信元のア...	発信元のポ...	宛先のアドレス	宛先のポート	接続を許可	アクション	パス
<input checked="" type="checkbox"/> すべて	す...	10.10.0.0	すべて	すべて	すべて	N/A	許可	
<input checked="" type="checkbox"/> svchost.exe	UDP	すべて	すべて	すべて	1024 - 65535	N/A	許可	c:\Windo...
<input checked="" type="checkbox"/> svchost.exe	UDP	すべて	DHCPサ...	すべて	DHCPライ...	N/A	許可	c:\Windo...
<input checked="" type="checkbox"/> seccenter.exe	TCP	すべて	HTTP (80)	すべて	すべて	はい	許可	c:\Windo...
<input checked="" type="checkbox"/> vserv.exe	TCP	すべて	HTTP (80)	すべて	すべて	はい	許可	c:\Windo...
<input checked="" type="checkbox"/> vserv.exe	TCP	すべて	SMTP (25)	すべて	すべて	はい	許可	c:\Windo...
<input checked="" type="checkbox"/> uiscan.exe	TCP	すべて	HTTP (80)	すべて	すべて	はい	許可	c:\Windo...
<input checked="" type="checkbox"/> bdagent.exe	TCP	すべて	HTTP (80)	すべて	すべて	はい	許可	c:\Windo...
<input checked="" type="checkbox"/> bdsbwiz.exe	TCP	すべて	HTTP (80)	すべて	すべて	はい	許可	c:\Windo...
<input checked="" type="checkbox"/> bdsbwiz.exe	TCP	すべて	HTTP (80)	すべて	すべて	はい	許可	c:\Windo...
<input checked="" type="checkbox"/> vserv.exe	TCP	すべて	HTTP (80)	すべて	すべて	はい	許可	c:\Windo...

外向きのルール:

アプリケーション	プロ...	発信元のア...	発信元のポ...	宛先のアドレス	宛先のポート	接続を許可	アクション	パス
<input checked="" type="checkbox"/> すべて	す...	すべて	すべて	10.10.0.0	すべて	N/A	許可	
<input checked="" type="checkbox"/> svchost.exe	UDP	すべて	1024 - 65535	すべて	DNS (53)	N/A	許可	c:\Windo...
<input checked="" type="checkbox"/> svchost.exe	UDP	すべて	DHCPライ...	すべて	DHCPサー...	N/A	許可	c:\Windo...
<input checked="" type="checkbox"/> seccenter.exe	TCP	すべて	すべて	すべて	HTTP (80)	はい	許可	c:\Windo...
<input checked="" type="checkbox"/> vserv.exe	TCP	すべて	すべて	すべて	HTTP (80)	はい	許可	c:\Windo...
<input checked="" type="checkbox"/> vserv.exe	TCP	すべて	すべて	すべて	SMTP (25)	はい	許可	c:\Windo...
<input checked="" type="checkbox"/> uiscan.exe	TCP	すべて	すべて	すべて	HTTP (80)	はい	許可	c:\Windo...
<input checked="" type="checkbox"/> bdagent.exe	TCP	すべて	すべて	すべて	HTTP (80)	はい	許可	c:\Windo...
<input checked="" type="checkbox"/> bdsbwiz.exe	TCP	すべて	すべて	すべて	HTTP (80)	はい	許可	c:\Windo...
<input checked="" type="checkbox"/> bdsbwiz.exe	TCP	すべて	すべて	すべて	HTTP (80)	はい	許可	c:\Windo...
<input checked="" type="checkbox"/> vserv.exe	TCP	すべて	すべて	すべて	HTTP (80)	はい	許可	c:\Windo...

OK [O]

詳細表示

ルールは、次の2つに分類されています：内向きルールおよび外向きルールです。各ルールのアプリケーションおよびルール属性（発信元アドレス、宛先アドレス、発信元ポート、宛先ポート、アクションなど）を確認できます。

ルールを削除するには、対象を選択し、 ルールを削除ボタンをクリックしてください。すべてのルールを削除するには、 一覧を削除ボタンをクリックしてください

い。ルールを編集するには、対象を選択して  ルールを編集ボタンをクリックするか、対象をダブルクリックしてください。ルールを削除せず、一時的に無効にするなら、対応するチェックボックスのチェックを外してください。

ルールの優先度を上げ下げできます。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てください。ルールに最も低い優先順位を与えるなら、 最後へ移動ボタンをクリックしてください。



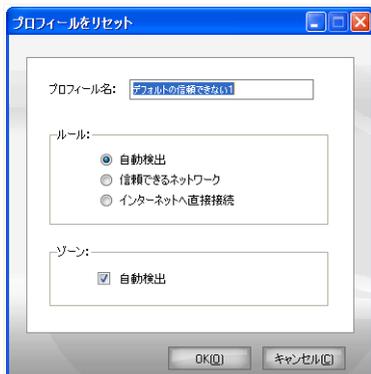
注意

次のオプションを持つコンテキストメニューも使えます：ルールを追加、ルールを編集、ルールを削除、上へ移動、下へ移動、最初へ移動、最後へ移動、一覧を削除。

OKをクリックして、ウィンドウを閉じてください。

9.3.5. プロフィールをリセット

経験豊富なユーザは、ファイアウォールの保護を最適化したり、必要に応じてカスタマイズしたりするために、ファイアウォールプロフィールを設定し直したいことがあるでしょう。ファイアウォールプロフィールをリセットするには、プロフィールをリセットをクリックしてください。次のウィンドウが開きます：



プロフィールをリセット

次の設定を行えます：

- プロフィール名 - 編集欄に新しい名前を入力してください。
- ルール - システムアプリケーションのために作成されるルールの形式を指定してください。

次のオプションが指定できます：

オプション	説明
自動検出	BitDefender にネットワーク設定を検出させ、基本的なルールの適切なセットを作成させます。
信頼できるネットワーク	信頼できるネットワークに適した基本的なルールのセットを作成します。
インターネットへ直接接続	インターネットへ直接接続するのに適した基本的なルールのセットを作成します。

- ゾーン - BitDefender に検出されたネットワークに適したゾーンを作成するには、自動検出をチェックしてください。

ウインドウを閉じて、プロフィールをリセットするには、OKをクリックしてください。

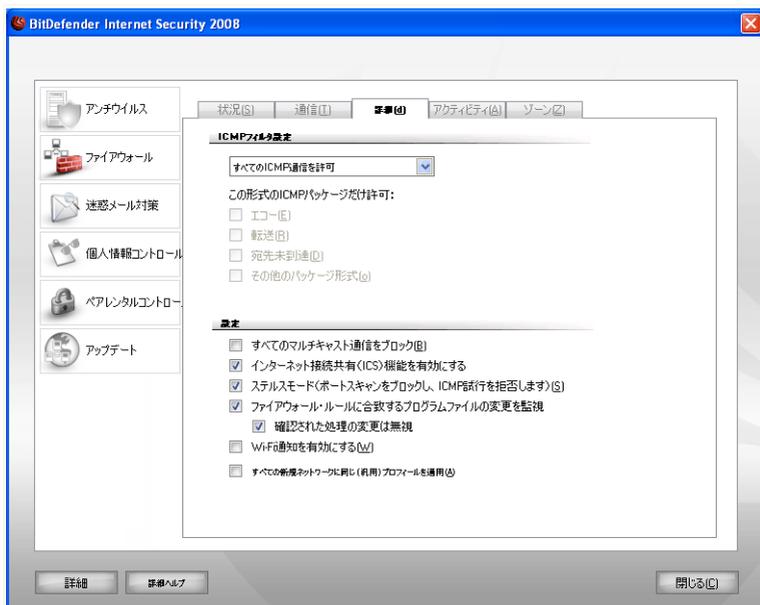


重要項目

ファイアウォールプロフィールを設定し直すと、この項で追加したすべてのルールは失われます。

9.4. 詳細設定

BitDefender ファイアウォールの詳細設定を行うには、設定コンソールでファイアウォール>詳細をクリックしてください。次のウインドウが開きます：



詳細設定

この項では、BitDefender のファイアウォールの詳細設定を行えます。詳細設定では、ICMP通信（**ICMP フィルタ設定**）のフィルタルールを指定し、マルチキャスト通信をブロックし、インターネット接続を共有し、お使いのコンピュータを悪意のあるソフトウェアやハッカーから隠すことができます（**設定**）。

9.4.1. ICMP フィルタ設定

メニューから、ICMP 通信をフィルタするための方針として次から1つを選択できます：

- すべての ICMP 通信を許可 - すべての ICMP 通信を許可します。
- すべての ICMP 通信をブロック - すべての ICMP 通信をブロックします。
- カスタム ICMP フィルタ - ICMP 通信をフィルタする方法をカスタマイズします。許可する ICMP パッケージの形式を選ぶことができます。

次のオプションが指定できます：

オプション	説明
Echo	このオプションは、Echo Reply および Echo Request メッセージを有効にします。Echo Request は、ホストにデータのペケットを送り、そのデータが Echo Reply で戻ってくることを期待する ICMP メッセージです。ホストは、すべての Echo Requests に、要求メッセージで受け取ったものと同じデータを含む Echo Reply で回答しなければなりません。Echo Reply は、ICMP Echo Request メッセージの回答として生成された ICMP メッセージで、すべてのホストとルータで必須です。
Redirect	これは、（ペケットを別のルートへ送るために）そのルーティング情報の宛先変更をホストに通知する ICMP メッセージです。ホストがデータをルータ（R1）経由で送ろうとした時、別のルータ（R2）がホストに到達すると、ホストからR2への直接経路が使えるようになり、Redirect がそのような経路をホストに通知します。それでもルータは、元々の宛先に元のデータグラムを送ります。しかし、データグラムにルーティング情報が含まれていると、より適した経路が使えても、このメッセージは送られません。
宛先に到達不能	これは、データグラムがマルチキャストアドレスを持っていない限り、宛先ホストが到達不能であることをクライアントに通知するために、ルータが生成するICMPメッセージです。このメッセージの原因には、ホストへの物理的接続が存在しない（距離が無限）、指定されたプロトコルあるいはポートがアクティブでない、またはデータが分裂しているが'分裂なし'フラグがオンになっている、場合などがあります。

オプション	説明
その他のパッケージ形式	このオプションが有効だと、Echo、宛先に到達不能、Redirect以外のすべてのパッケージは通過します。

9.4.2. 詳細ファイアウォール設定

次の詳細ファイアウォール設定が使えます：

- すべてのマルチキャスト通信をブロック - 受け取ったあらゆるマルチキャストパッケージを破棄します。

マルチキャスト通信は、ネットワーク内の特別なグループに宛てたある種の通信です。パッケージは、マルチキャストクライアントが同意すれば受け取ることができる特別なアドレスから送られます。

例えば、TVチューナーを持つネットワークのメンバーは、ビデオストリームをブロードキャスト（ネットワークの各メンバーへ送信）あるいはマルチキャスト（特別なアドレスへ送信）することができます。マルチキャストアドレスを聴取しているコンピュータは、パッケージを許可または拒否できます。許可すると、ビデオストリームをマルチキャストクライアントで視聴できます。

膨大な量のマルチキャスト通信は、帯域幅とリソースを消費します。このオプションが有効だと、受信したすべてのマルチキャストパッケージは破棄されます。ただし、このオプションを選択することはお勧めできません。

- 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、お使いのシステムのICSを自動的に有効にするわけではなく、お使いの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、お使いの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、それをお使いの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。またお使いの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）。

- ステルスモード - 悪意のあるソフトウェアやハッカーからお使いのコンピュータを隠します。

お使いのコンピュータが脆弱かどうか知る最も簡単な方法は、ポートに接続して反応があるか調べることです。これはポートスキャンと呼ばれる手法です。

悪意のある個人あるいはソフトウェアプログラムにお使いのコンピュータがネットワークに接続されていることはもちろん、存在していることさえ知らせる必要はありません。ステルスモードオプションは、どのポートが開いているか調べ、その正確な場所を知ろうとする試みに、お使いのコンピュータが反応しないようにします。

- ファイアウォールに合致するプログラムファイルの変更を監視 - 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。しかしお使い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おいて、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。

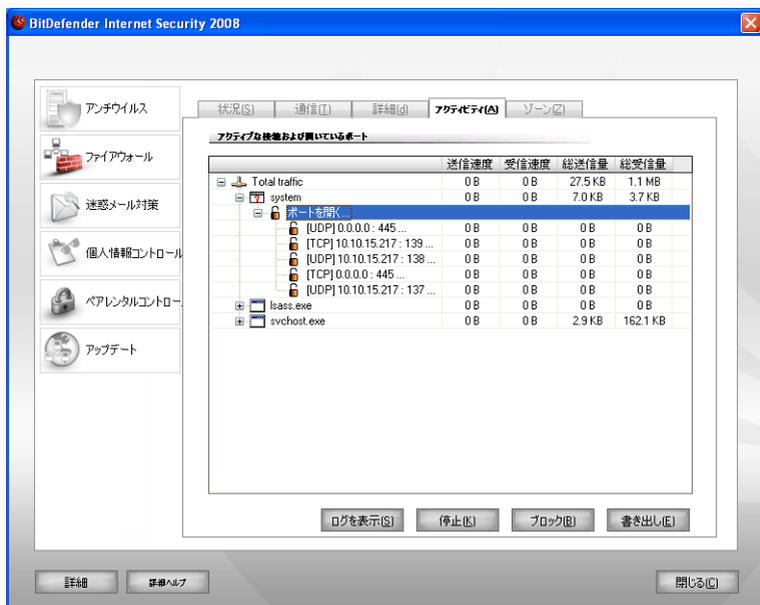
署名されたアプリケーションは、信頼でき、高いセキュリティレベルを持つと考えられます。このイベントについて、署名付きアプリケーションが変更されても、警告せずにインターネットへの接続を許可するなら、署名付きアプリケーションの変更は無視をチェックしてください。

- Wi-Fi 通知を有効にする - Wi-Fi 通知を有効にします。
- 同じ（一般の）プロフィールをすべての新規ネットワークに適用 - Generic Networkという名前のデフォルト（一般）の **ファイアウォールプロフィール**を作成し、新規のネットワーク設定を検出すると常にそれを適用します。ファイアウォールプロフィールが存在する古いネットワーク設定に戻る場合、デフォルト

のプロフィールではなく対応するファイアウォールプロフィールが読み込まれます。

9.5. 接続コントロール

アプリケーション別に並んだ現在の（TCPおよびUDPを介した）ネットワークインターネットアクティビティを監視し、BitDefender ファイアウォールログを開くには、設定コンソールでファイアウォール>アクティビティをクリックしてください。次のウィンドウが開きます：



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。

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お客様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。

選択したアプリケーション、ポート、あるいは接続による通信を制限するルールを作成するには、ブロックをクリックしてください。その選択の確認表示が表示されます。さらに調整するには、**通信**の項でルールを編集できます。



注意

アプリケーション、ポート、接続をブロックするには、それを右クリックして、ブロックを選択することもできます。

選択したプロセスのすべてのインスタンスを終了するには、停止をクリックしてください。選択肢の確認を促されます。



注意

プロセスを停止するには、それを右クリックして停止を選択することもできます。

一覧を .txt ファイルに書き出すには、書き出しをクリックしてください。

ファイアウォールモジュールの動作（ファイアウォールの開始／停止、通信のブロック、ステルスモードの有効化、設定の編集、プロフィールの適用）に関するイベント一覧、あるいはファイアウォールモジュールによって検出されたアクティビティ（ポートのスキャン、ルールによる接続試行あるいは通信のブロック）によって生成されたイベント一覧を表示するには、ログを表示をクリックすると表示される BitDefender ファイアウォールログファイルをご確認ください。このファイルは、現在の Windows ユーザ の Common Files フォルダにあります（次のパス内）：
...BitDefender¥BitDefender Firewall¥bdfirewall.txt。

9.6. ネットワークゾーン

ゾーンとは、プロフィール内で作成された特別なルールのための IP アドレスあるいは IP アドレスの範囲です。ルールは、ネットワークのメンバーによるお使いのコンピュータへの無制限なアクセスを許可するか（信頼できるゾーン）、逆にネットワーク上のコンピュータからお使いのコンピュータを完全に切り離す（信頼できないゾーン）か、どちらかになります。

デフォルトでは、BitDefender はお客様が接続されたネットワークを自動検出し、ネットワークの設定に応じてゾーンを追加します。

**注意**

複数のネットワークに接続されている場合は、それらの設定により、2つ以上のゾーンが追加される場合があります。

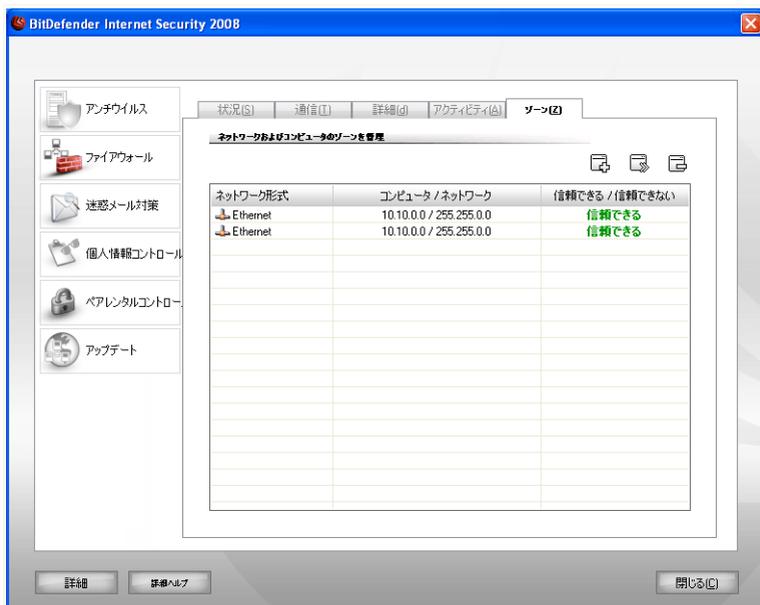
次のネットワーク設定では、デフォルトで信頼できるゾーンが追加されます：

- ゲートウェイなしのプライベートIP - コンピュータは、ローカルエリアネットワーク（LAN）の一部で、インターネットには接続されていません。
- ドメイン制御が検出されたプライベートIP - LANの一部で、ドメインに接続されたコンピュータです。

次のネットワーク設定では、デフォルトで信頼できないゾーンが追加されます：

- 公開（セキュアでない）ワイヤレス - ワイヤレスのローカルエリアネットワーク（WLAN）の一部であるコンピュータです。

ネットワークゾーンを管理するには、設定コンソールでファイアウォール>ゾーンをクリックしてください。 次のウィンドウが開きます：



ネットワークゾーン

表に記載された現在のプロフィールに対応するネットワークゾーンを確認できます。各ゾーン毎に、ネットワーク形式（Ethernet、ワイヤレス、PPPなど）、そのゾーンに関連したコンピュータあるいはネットワーク、およびゾーンが信頼できるかできないかが確認できます。

ゾーンを編集するには、 ゾーンを編集ボタンをクリックするか、ダブルクリックしてください。



注意

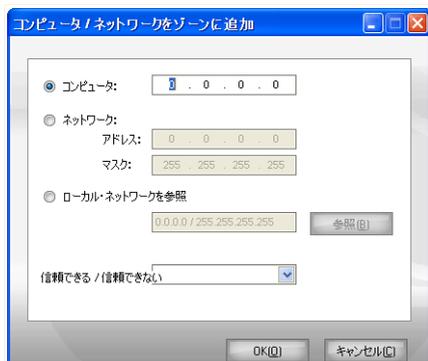
デフォルトでは、BitDefender は公開されたワイヤレスネットワークを信頼できないゾーンとして追加します。オープンな ad-hoc ワイヤレスネットワークに信頼できるコンピュータ（家、あるいは数人の友人）と接続しているなら、関連するゾーンを編集した方がよいかもしれません。ネットワークの他のメンバーとリソースを共有するには、ネットワークを信頼するゾーンに設定しなければなりません。

ゾーンを削除するには、選択して  ゾーンを削除ボタンをクリックしてください。

9.6.1. ゾーンを追加

ゾーンは手動で追加できます。これで、例えば公開されたワイヤレスネットワークの内側で（彼らのコンピュータを信頼できるゾーンに追加することで）友人とだけファイルを共有することができます。あるいは、コンピュータを信頼できないゾーンに追加することで、信頼できるネットワークからはブロックすることができます。

新しいゾーンを追加するには、 ゾーンを追加ボタンをクリックしてください。次のウィンドウが開きます：



ゾーンを追加

ゾーンを追加するには、次の手順に従ってください：

1. ゾーンとして追加したいローカルネットワーク内のコンピュータあるいはローカルエリアネットワーク全体を指定してください。 次の方法のいずれかを使えます：
 - 特定のコンピュータを追加するには、コンピュータを選択し、そのIPアドレスを提供してください。
 - 特定のネットワークを追加するには、ネットワークを選択し、そのIPアドレスとマスクを提供してください。
 - コンピュータあるいはネットワークを見つけて追加するには、ローカルネットワークを参照してください。

ローカルネットワークを参照するには、ローカルネットワークを参照を選択し、参照をクリックしてください。接続されているすべてのネットワークおよび各ネットワークのメンバーが表示される新しいウィンドウが開きます。

ゾーンとして追加したいコンピュータあるいはネットワークを一覧から選択し、OKをクリックしてください。

2. 作成したいゾーンの形式（信頼できる、あるいは信頼できない）をメニューから選択してください。
3. OKをクリックすると、ゾーンが追加されます。

10. アンチスパム

BitDefender Antispam は、迷惑メールがお使いの受信ボックスに到達する前に除去するため、目を見張る技術的革新と業界標準のアンチスパムフィルタを採用しています。

このユーザガイドのアンチスパムの項には、次の内容が記載されています：

- **アンチスパムの知識**
- **アンチスパムの統計**
- **アンチスパムの設定**
- **メールクライアントとの連携**

10.1. アンチスパムの知識

迷惑メール（スパム）は、個人および組織にとって、日々増大する頭痛の種です。決して子供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。

10.1.1. アンチスパムフィルタ

BitDefender Antispam Engine は、お使いの受信ボックスから迷惑メールを一掃するために7種類の異なるフィルタを搭載しています：**ホワイトリスト**、**ブラックリスト**、**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。

ホワイトリスト／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しており、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。友人あるいは迷惑メール送信

者一覧を使えば、その内容に関わらず電子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）を簡単に区別することができます。



注意

ホワイトリスト／ブラックリストは、それぞれ友人一覧／迷惑メール送信者一覧とも呼ばれます。

友人／迷惑メール送信者一覧は、**設定コンソール**、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**から管理できます。



注意

友人の名前および電子メールアドレスは友人一覧に追加することをお勧めします。BitDefender は、その一覧上の人からのメッセージはブロックしません；ですから友人を追加することは、信頼できるメッセージが届く精度を向上させるのに役立つのです。

Charset 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）charset（文字セット）で書かれています。Charset 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検出をすり抜けるのが難しいため、最近では受信ボックスが不要な内容の画像だけしか持たないメッセージが多く来るようになっていきます。これに対処するため、BitDefender は電子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。合致したら、SPAMタグを付加します。

URL フィルタ

ほぼすべて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。これらの場所の多くは、さらに広告や商品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。合致すると、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）に一連の試験を行い、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、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、（お客様自身あるい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内に登場す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。

これは、例えば、迷惑メールに特定の4文字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は高まることを意味します。メッセージ内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。

このモジュールは、もう1つの興味深い特徴を持っています：学習可能なのです。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

アンチスパムツールバーの 迷惑メールおよび 非迷惑メールボタンを使ってベイジアンモジュールを修正できます。



注意

アップデートを実行する度：

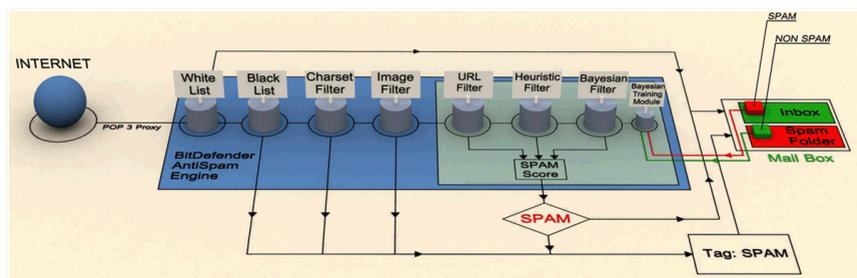
- 新しいイメージグネチャがイメージフィルタに追加されます。
- 新しいリンクがURL フィルタに追加されます。
- 新しいルールがNeuNet (ヒューリスティック) フィルタに追加されます。

これはアンチスパムエンジンの精度を向上させます。

迷惑メール送信者からお客様を守るために、BitDefender は自動アップデートを実行できます。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。

10.1.2. アンチスパム操作

次の仕組みは、BitDefender の動作を表します。



アンチスパム操作

上に図解されたアンチスパムフィルタ (ホワイトリスト、ブラックリスト、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)は、メールがお使いの受信ボックスへ届けられるべきかどうか判断するため、BitDefender によって連携して使用されます。

インターネットから届く電子メールは、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れば、電子メールはお使いの受信ボックスへそのまま移動されます。

それ以外の場合、ブラックリストフィルタが電子メールを引き継ぎ、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、電子メールにSPAMタグが付加され、(Microsoft Outlook内の) Spamフォルダに移動されます。

それ以外の場合、Charset フィルタが電子メールが 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、電子メールにSPAMタグが付加され、Spamフォルダへ移動されます。

電子メールが 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電子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、電子メールにSPAMスコアを追加します。

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



注意

電子メールの件名に SEXUALLY EXPLICIT 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、（お客様あるい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を比較して、登場す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。電子メールには、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ら、メッセージは迷惑メールと判定されます。

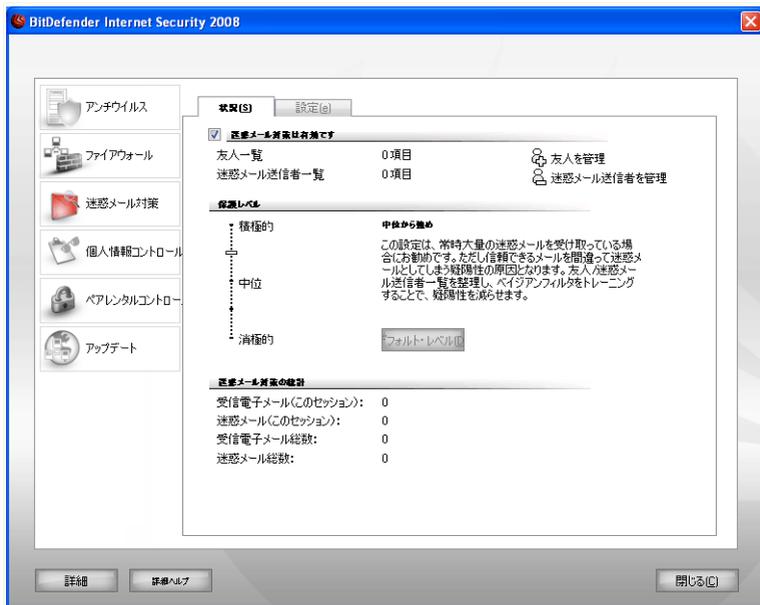


重要項目

Microsoft Outlook あるいは Microsoft Outlook Express 以外のメールクライアントをお使いなら、BitDefender によってSPAMとタグされた電子メールメッセージをカスタムの隔離フォルダへ移動するルールを作成してください。BitDefender は、迷惑メールと判定されたメッセージの件名の最初に[SPAM]を追加します。

10.2. アンチスパムの状態

アンチスパム保護を設定するには、設定コンソールでアンチスパム>状態をクリックしてください。次のウィンドウが開きます：



アンチスパムの状態

この項では、アンチスパムモジュールを設定し、その動作に関する情報を確認できます。



重要項目

迷惑メールがお使いの受信ボックスに届かないように、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、アンチスパムアクティビティの結果を（お使いの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。

アンチスパムモジュールを設定するには、次の手順が必要です：

10.2.1. 手順1/2 - しきい値レベルを設定

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。

5種類のしきい値レベルがあります：

しきい値レベル	説明
消極的	<p>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。</p> <p>フィルタは多くの電子メールを通過させますが、擬陰性（迷惑メールを通常メールと判定）の可能性があります。</p>
弱めから中位	<p>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。</p> <p>フィルタは多くの電子メールを通過させますが、擬陰性（迷惑メールを通常メールと判定）の可能性があります。</p>
中位	<p>一般的なアカウントを保護します。</p> <p>フィルタは、擬陽性を避けながら、ほとんどの迷惑メールをブロックします。</p>
中位から積極的	<p>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。</p> <p>フィルタは迷惑メールをほとんど通過させませんが、擬陽性（通常のメールを間違っ迷惑メールと判定する）の可能性があります。</p> <p>擬陽性の数を減らすには、友人/迷惑メール送信者一覧を作成し、学習エンジン（ベイジアン）を学習させてください。</p>
積極的	<p>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。</p>

しきい値レベル	説明
	<p>フィルタは迷惑メールをほとんど通過させませんが、擬陽性（通常のメールを間違えて迷惑メールと判定する）の可能性があります。</p> <p>擬陽性の数を減らすためには、お使いのアドレス帳を友人一覧に追加してください。</p>

保護レベルをデフォルトの（中位から積極的）に設定するには、デフォルトレベルをクリックしてください。

10.2.2. 手順2/2 – アドレス一覧に登録

通常の電子メールメッセージあるいは迷惑メールを送ってくる電子メールアドレスの情報を持つアドレスの一覧です。

友人一覧

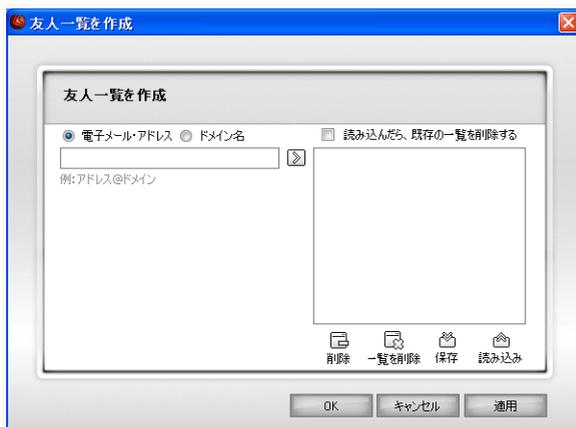
友人一覧は、その内容に関わらず、常にメッセージを受け取りたいすべての電子メールアドレスの一覧です。友人からのメッセージは、内容が迷惑メールのように見えても迷惑メールと判定されません。



注意

友人一覧内のアドレスから届いたすべてのメールは、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。

友人一覧を管理するには、（友人一覧に対応）をクリックするか、 **アンチスパムツールバー**の友人ボタンをクリックしてください。



友人一覧

ここで友人一覧の項目を追加あるいは削除できます。

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、をクリックしてください。アドレスが友人一覧に表示されます。



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、をクリックしてください。ドメインが友人一覧に表示されます。



重要項目

構文：

- @domain.com、*domain.com、domain.com - domain.comから来たすべての受信電子メールメッセージは、その内容に関わらず、お使いの受信ボックスに届きます；
- *domain* - domainから来たすべての受信電子メールメッセージは、（その末尾が何であれ）その内容に関わらず、お使いの受信ボックスに届きます；
- *com - comというドメイン末尾を持つすべての受信電子メールメッセージは、その内容に関わらず、お使いの受信ボックスに届きます；

一覧から項目を削除するには、対象を選択し、 削除ボタンをクリックしてください。 一覧を削除ボタンをクリックすると、一覧内のすべての項目が削除されます。注意：一度削除すると復旧は不可能です。

友人一覧を希望する場所に保存／読み込みするには、 保存/  読み込みボタンを使用します。ファイルには、拡張子 .bwl が付きます。

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、読み込んだら、現在の一覧を削除するを選択してください。



注意

友人の名前および電子メールアドレスは友人一覧に追加することをお勧めします。BitDefender は、その一覧上の人からのメッセージはブロックしません；ですから友人を追加することは、信頼できるメッセージが届く精度を向上させるのに役立つのです。

友人一覧を保存して閉じるには、適用およびOKをクリックしてください。

迷惑メール送信者一覧

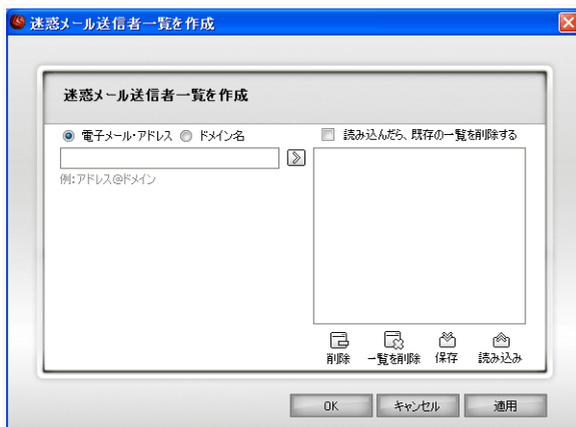
迷惑メール送信者一覧は、その内容に関わらず、お客様がメッセージを一切受け取りたくないすべての電子メールアドレスの一覧です。



注意

迷惑メール送信者一覧内のアドレスから受け取ったすべての電子メールは、それ以降の処理なしに自動的にSPAMとマークされます。

迷惑メール送信者一覧を管理するには、 (迷惑メール送信者一覧に対応) をクリックするか、 アンチスパムツールバーで迷惑メール送信者ボタンをクリックしてください。



迷惑メール送信者一覧

ここで、迷惑メール送信者一覧の項目を追加したり削除したりできます。

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、をクリックしてください。アドレスは迷惑メール送信者一覧に表示されます。



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、をクリックしてください。ドメインは迷惑メール送信者一覧に表示されます。



重要項目

構文：

- @domain.com、*domain.com、domain.com - domain.comから来たすべての受信電子メールメッセージは、SPAMタグを付加されます；
- *domain* - domainから来たすべての受信電子メールメッセージは、（ドメイン末尾に関わらず）SPAMタグを付加されます；
- *com - ドメイン末尾がcomのすべての受信電子メールメッセージは、SPAMタグを付加されます；

一覧から項目を削除するには、対象を選択し、 削除ボタンをクリックしてください。 一覧を削除ボタンをクリックすると、一覧内のすべての項目が削除されます。注意：一度削除すると復旧は不可能です。

迷惑メール送信者一覧を希望する場所に保存／読み込みするには、 保存 /  読み込み ボタンを使用します。ファイルには、拡張子.bwlが付きます。

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、読み込んだら、現在の一覧を削除するを選択してください。

迷惑メール送信者一覧を保存して閉じるには、適用およびOKをクリックしてください。

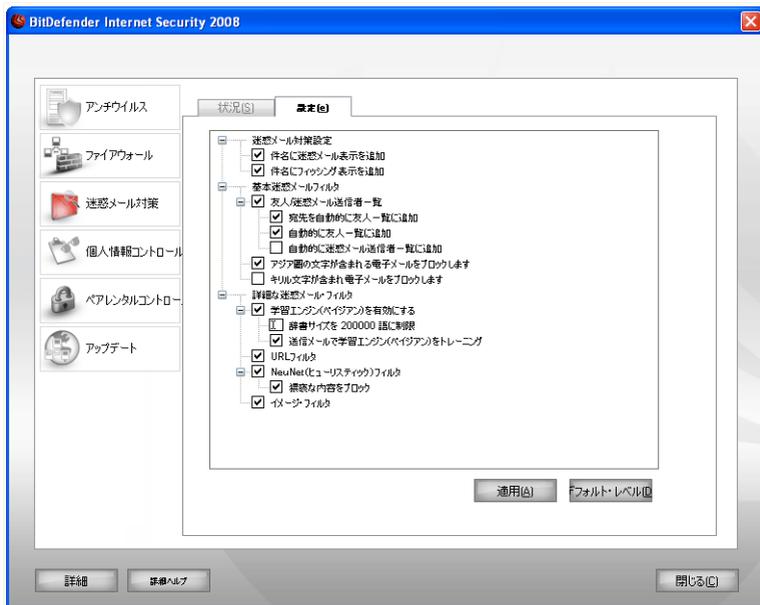


重要項目

BitDefender を再インストールする場合、その前に友人 / 迷惑メール送信者一覧を保存しておき、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。

10.3. アンチスパム設定

アンチスパム設定を設定するには、設定コンソールで迷惑メール対策>設定をクリックしてください。次のウィンドウが開きます：



アンチスパム設定

ここで、各アンチスパムフィルタを有効/無効にでき、アンチスパムモジュールに関する他の設定も指定できます。

Windows で使わ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。

10.3.1. 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電子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電子メールメッセージは、件名にSPAMタグが付加されます。

10.3.2. 基本迷惑メールフィルタ

- 友人／迷惑メール送信者一覧 - **友人／迷惑メール送信者一覧**をオン／オフにします。
 - ・宛先を自動的に友人一覧に追加 - 送信メールの受信者を自動で友人一覧に追加します。
 - ・自動的に友人一覧に追加 - 次回**アンチスパムツールバー**で  非迷惑メールボタンをクリックすると、送信者は自動的に友人一覧に追加されます。
 - ・自動的に迷惑メール送信者一覧に追加 - 次回**アンチスパムツールバー**で  迷惑メール ボタンをクリックすると、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 - **アジア文字セット**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) 文字セット**で書かれたメッセージはブロックします。

10.3.3. 詳細な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)** をオン／オフにします。
 - ・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 - 小さいほど早いですが、大きいほど正確です。



注意

推奨サイズ：200,000 語

- ・送信電子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) を送信電子メールでも学習させます。

- URL フィルタ - URL フィルタをオン/オフにします。
- NeuNet (ヒューリスティック) フィルタ - NeuNet (ヒューリスティック) フィルタをオン/オフにします。
 - ・ 猥褻な内容をブロック - 件名に SEXUALLY EXPLICIT と書かれたメッセージの検出をオン/オフにします。
- イメージフィルタ - イメージフィルタをオン/オフにします。



注意

オプションをオン/オフにするには、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。

変更を保存するには適用をクリックし、デフォルト設定を読み込むにはデフォルトをクリックしてください。

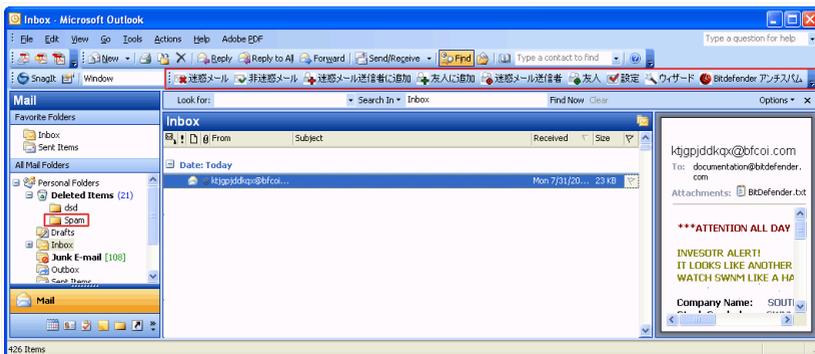
10.4. メールクライアントとの連携

BitDefender は、分かりやすく使いやすいツールバーから次のメールクライアントに直接統合します：

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

10.4.1. 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



重要項目

Microsoft Outlook と Outlook Express / Windows Mailでの BitDefender Antispam の違いは、Microsoft Outlook ではSPAMメッセージがSpamフォルダへ移動するのに対し、Outlook Express / Windows Mail では削除された項目フォルダへ移動する点です。どちらの場合も、メッセージの件名にはSPAMタグが付加されます。

Microsoft Outlook のSpamフォルダは、BitDefender が自動で作成し、フォルダー一覧（カレンダーやコンタクトリストなど）と同じ階層に表示されます。

BitDefender ツールバーの各ボタンの説明は、以下の通りです：

-  迷惑メール - メッセージをペイジアンモジュールへ送り、選択された電子メールが迷惑メールであることを伝えます。電子メールは、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電子メールは、SPAMとタグされます。



注意

電子メールメッセージは、1つあるいは好きな数だけ選択できます。

-  非迷惑メール - メッセージをペイジアンモジュールに送り、選択された電子メールは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、Spamフォルダから受信ボックスディレクトリへ移動されます。

今後受け取る同じパターンを持つ電子メールは、もうSPAMとはタグされません。



注意

電子メールメッセージは、1つあるいは好きな数だけ選択できます。



重要項目

BitDefender によってSPAMとマークされたメッセージ（通常、Spamフォルダ内にあります）を選ぶと、 非迷惑メールボタンが有効になります。

-  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一覧に追加します。



迷惑メール送信者のアドレスを一覧に追加する際、この確認を表示し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てください。

OKをクリックして、ウィンドウを閉じてください。

迷惑メール送信者を追加

今後このアドレスから届く電子メールメッセージは、SPAMとタグされます。



注意

送信者は、1人あるいは好きな数だけ選択できます。

-  友人を追加 - 選択した電子メールの送信者を友人一覧に追加します。



友人を追加

友人のアドレスを一覧に追加する際、この確認を表示し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てください。

OKをクリックして、ウインドウを閉じてください。

このアドレスから届く電子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

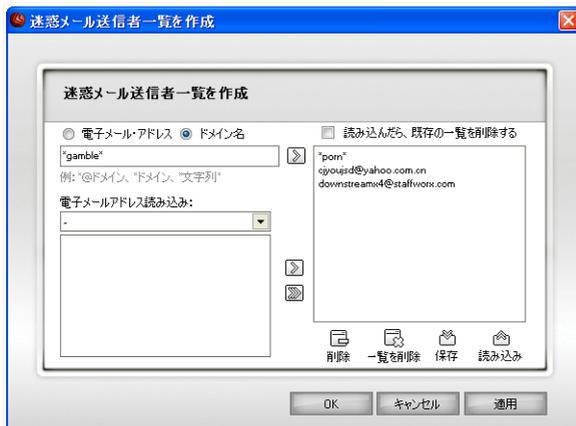
送信者は、1人あるいは好きな数だけ選択できます。

-  迷惑メール送信者 - 内容に関わらずメッセージを受け取りたくない電子メールアドレスが保管された迷惑メール送信者一覧を開きます。



注意

迷惑メール送信者一覧内のアドレスから受け取ったすべての電子メールは、それ以降の処理なしに自動的にSPAMとマークされます。



迷惑メール送信者一覧

ここで、迷惑メール送信者一覧の項目を追加したり削除したりできます。

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、 ボタンをクリックしてください。アドレスが迷惑メール送信者一覧に表示されます。



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てください。ドメインが迷惑メール送信者一覧に表示されます。



重要項目

構文：

- ・ @domain.com、*domain.com、domain.com - domain.com から来たすべての受信電子メールメッセージは、SPAM タグを付加されます；
- ・ *domain* - domain から来たすべての受信電子メールメッセージは、(ドメイン末尾に関わらず) SPAM タグを付加されます；
- ・ *com - ドメイン末尾が com のすべての受信電子メールメッセージは、SPAM タグを付加されます；

電子メールアドレスを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、電子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てください。

Microsoft Outlook Express / Windows Mailでは、迷惑メール送信者一覧に追加したい電子メールアドレスが保存されたフォルダを選択するための新しいウィンドウが開きます。選んだら、選択をクリックしてください。

どちらの場合も、電子メールアドレスは、読み込みリストに表示されます。希望する項目を選び、をクリックして迷惑メール送信者一覧に追加してください。をクリックすると、すべての電子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、対象を選択し、削除ボタンをクリックしてください。一覧を削除ボタンをクリックすると、一覧内のすべての項目が削除されます。注意：一度削除すると復旧は不可能です。

迷惑メール送信者一覧を希望する場所に保存／読み込みするには、 保存/  読み込み ボタンを使用します。ファイルには、拡張子.bwlが付きます。

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、読み込んだら、現在の一覧を削除するを選択してください。

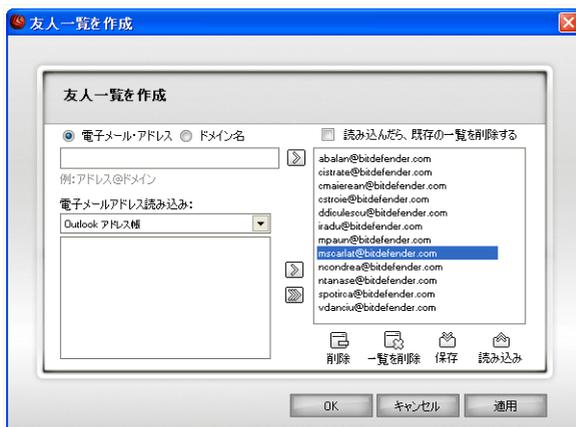
迷惑メール送信者一覧を保存して閉じるには、適用およびOKをクリックしてください。

-  友人 - 内容に関わらず常に受け取りたい電子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一覧を開きます。



注意

友人一覧内のアドレスから届いたすべてのメールは、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。



友人一覧

ここで友人一覧の項目を追加あるいは削除できます。

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、ボタンをクリックしてください。アドレスが友人一覧に表示されます。



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てください。ドメインが友人一覧に表示されます。



重要項目

構文：

- ・ @domain.com、*domain.com、domain.com - domain.comから来たすべての受信電子メールメッセージは、その内容に関わらず、お使いの受信ボックスに届きます；
- ・ *domain* - domainから来たすべての受信電子メールメッセージは、（その末尾が何であれ）その内容に関わらず、お使いの受信ボックスに届きます；
- ・ *com - comというドメイン末尾を持つすべての受信電子メールメッセージは、その内容に関わらず、お使いの受信ボックスに届きます；

電子メールアドレスを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、電子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てください。

Microsoft Outlook Express / Windows Mailの場合、友人一覧に追加したい電子メールアドレスが保存されたフォルダを選択できる新しいウインドウが開きます。対象を選び、選択をクリックしてください。

どちらの場合も、電子メールアドレスは読み込みリストに表示されます。希望する項目を選んで をクリックし、友人一覧に追加してください。 をクリックすると、すべての電子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、対象を選択し、 削除ボタンをクリックしてください。 一覧を削除ボタンをクリックすると、一覧内のすべての項目が削除されます。注意：一度削除すると復旧は不可能です。

友人一覧を希望する場所に保存／読み込みするには、 保存 / 読み込みボタンを使用します。ファイルには、拡張子 .bwl が付きます。

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、読み込んだら、現在の一覧を削除するを選択してください。

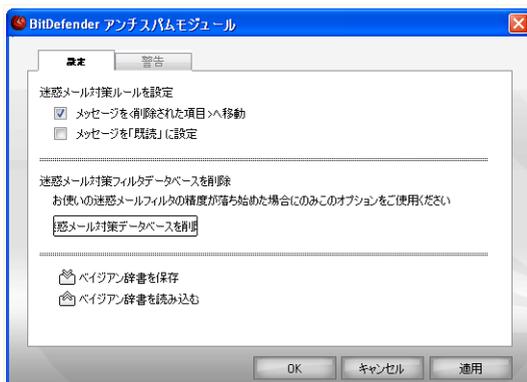


注意

友人の名前および電子メールアドレスは友人一覧に追加することをお勧めします。BitDefender は、その一覧上の人からのメッセージはブロックしません；ですから友人を追加することは、信頼できるメッセージが届く精度を向上させるのに役立つのです。

友人一覧を保存して閉じるには、適用およびOKをクリックしてください。

- 設定 - アンチスパムに対してオプションを指定できる設定ウインドウが開きます。



設定

次のオプションが指定できます：

- ・ 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、**ベイズアンチスパム**を再度学習させた方がよいかもかもしれません。**ベイズアンチスパムデータベース**をリセットするには、アンチスパムデータベースを消去を選択してください。

ベイズアンチスパムデータベースを希望する場所に保存あるいは読み込みするには、 ベイズアンチスパムを保存 /  ベイズアンチスパムを読み込みボタンを使用します。ファイルには、.dat拡張子が付きます。

 迷惑メール送信者を追加および  友人を追加ボタンについて、確認ウインドウが表示されるのを無効にする設定は、警告タブをクリックすると使えます。



注意

警告ウインドウでは、電子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。電子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 - BitDefender アンチスパムの効果をさらに高めるため、**ページアンフィルタ**学習を手順を追って手引きする**ウィザード**を開きます。また、お使いのアドレス帳内のアドレスを**友人一覧** / **迷惑メール送信者一覧**に追加できます。
- 🖱️ BitDefender Antispam - **マネージメントコンソール**を開きます。

10.4.2. アンチスパム設定ウィザード

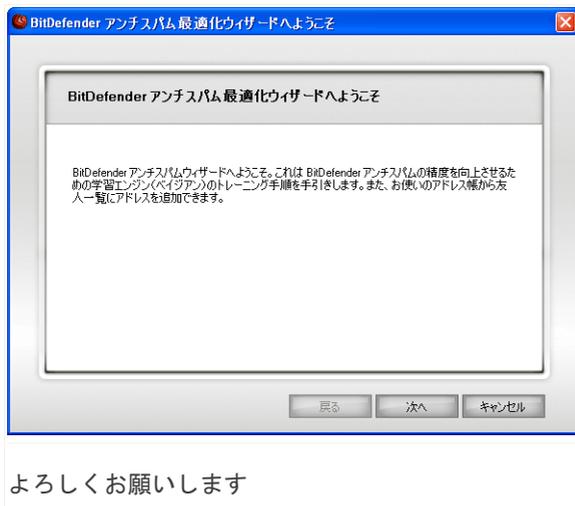
BitDefender をインストール後初めてメールクライアントを起動する際、迷惑メール対策フィルタの効率を上げるため、**友人一覧**および**迷惑メール送信者一覧**の作成と**ページアンフィルタ**トレーニングを手引きするウィザードが表示されます。



注意

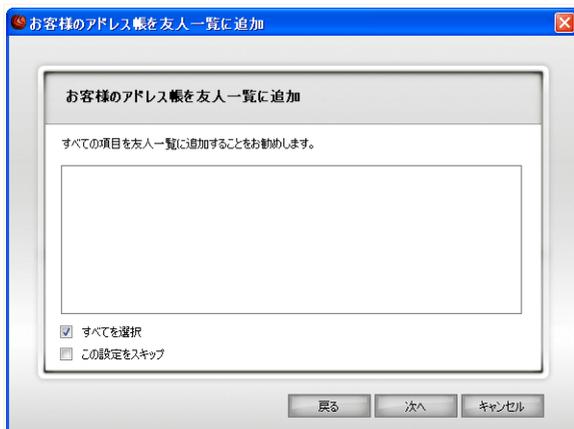
ウィザードは、**アンチスパムツールバー**で🖱️ ウィザードボタンをクリックすれば、いつでも起動できます。

手順1/6 - ご挨拶



次へをクリックしてください。

手順2/6 - 友人一覧に登録



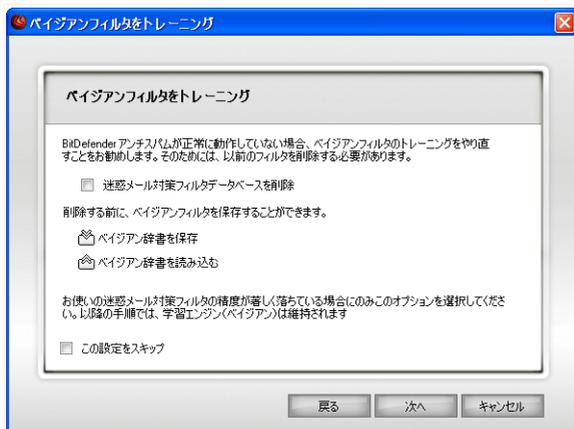
友人一覧に登録します。

ここでは、お使いのアドレス帳内のすべてのアドレスが確認できます。友人一覧に追加したい項目を選んでください（すべてを選択することをお勧めします）。それらのアドレスからは、内容に関わらずすべての電子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一覧へ追加するには、すべてを選択にチェックしてください。

この手順を省略する場合、スキップを選択してください。前の手順へ戻るには戻るをクリックし、ウィザードを続けるには次へをクリックしてください。

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

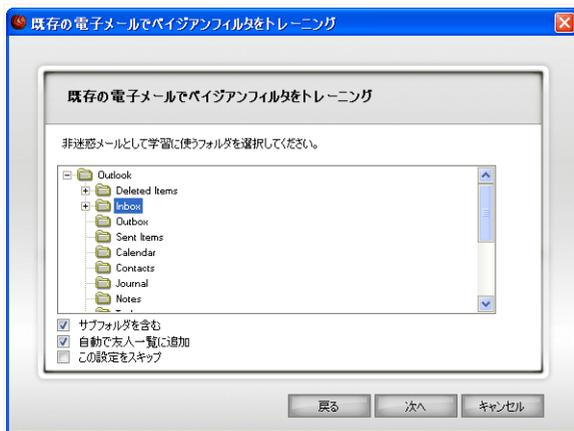
お使いの迷惑メール対策フィルタの効果が下がってくる場合があるかもしれません。これは不適当な学習が原因です（つまり多くの通常メールメッセージを迷惑メールとしたり、その逆を行ったということです）。フィルタの精度が下がったら、フィルタデータベースを削除し、このウィザードの次の手順に沿って再度学習させてください。

ベイジアンデータベースをリセットするには、アンチスパムフィルタを消去を選択してください。

ベイジアンデータベース一覧を希望する場所に保存／読み込みするには、 ベイジアンを保存/ ベイジアンを読み込みボタンを使用します。ファイルには、.dat拡張子が付きます。

この手順を省略する場合、スキップを選択してください。前の手順へ戻るには戻るをクリックし、ウィザードを続けるには次へをクリックしてください。

手順4/6 - 通常メールでベイジアンフィルタを学習



ベイジアンフィルタを通常メールで学習

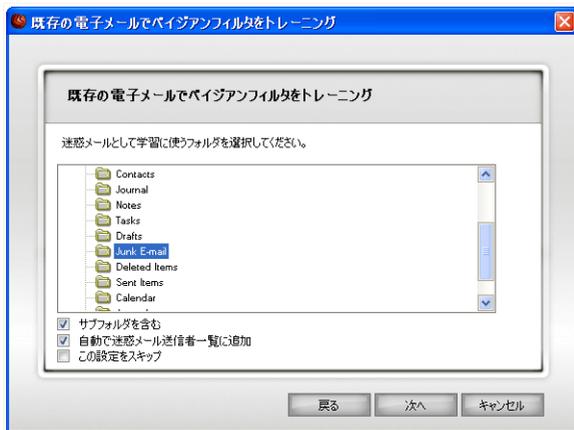
通常の電子メールメッセージが保存されたフォルダを選択してください。これらのメッセージが、アンチスパムフィルタの学習に使われます。

ディレクトリー一覧の下に2つの詳細オプションがあります：

- 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。
- 友人一覧に自動で追加 - 送信者を友人一覧に追加します。

この手順を省略する場合、スキップを選択してください。前の手順へ戻るには戻るをクリックし、ウィザードを続けるには次へをクリックしてください。

手順5/6 - ベイジアンフィルタを迷惑メールで学習



ベイジアンフィルタを迷惑メールで学習

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で使われます。



重要項目

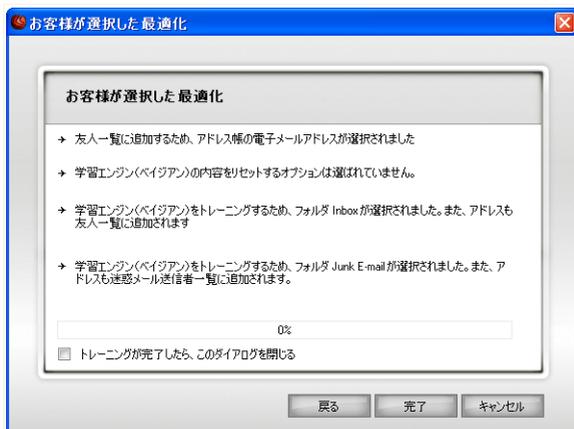
選んだフォルダには、通常メールがまったく含まれていないことを確認してください。でないと、アンチスパムの効果は目に見えて低下します。

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：

- 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。
- 迷惑メール送信者一覧に自動で追加 - 送信者を迷惑メール送信者一覧に追加します。

この手順を省略する場合、スキップを選択してください。前の手順へ戻るには戻るをクリックし、ウィザードを続けるには次へをクリックしてください。

手順6/6 - まとめ



概要

ここでは設定ウィザードのすべての設定を確認できます。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。

11. 個人情報コントロール

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

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

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

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

11.1. 個人情報コントロールの状態

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



個人情報コントロールの状態

11.1.1. 個人情報コントロール



重要項目

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

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

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

**注意**

画面の下には、個人識別情報コントロールの統計が表示されます。

- **レジストリをコントロール** - プログラムが Windows 起動時に実行できるようにレジストリ項目を変更しようとする度に、お客様の許可を要求します。
- **Cookie をコントロール** - 新しいウェブサイトが Cookie を設定しようとする度に、お客様の許可を要求します。
- **スクリプトをコントロール** - ウェブサイトがスクリプトあるいは他のアクティブなコンテンツを実行しようとする度に、お客様の許可を要求します。

これらのコントロールの設定を行うには、 **詳細設定**をクリックしてください。

保護レベルを設定

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

3つの保護レベルがあります：

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

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

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

11.1.2. アンチフィッシング保護

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

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

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

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

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

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

Internet Explorer に統合された BitDefender アンチフィッシングツールバーを使って、アンチフィッシング保護およびホワイトリストを簡単に管理することもできます。詳細については、「[アンチフィッシングツールバー](#)」（p. 170）を参照してください。

11.2. 詳細設定 - 個人識別情報コントロール

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

お使いの電子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、お客様に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知れません。

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

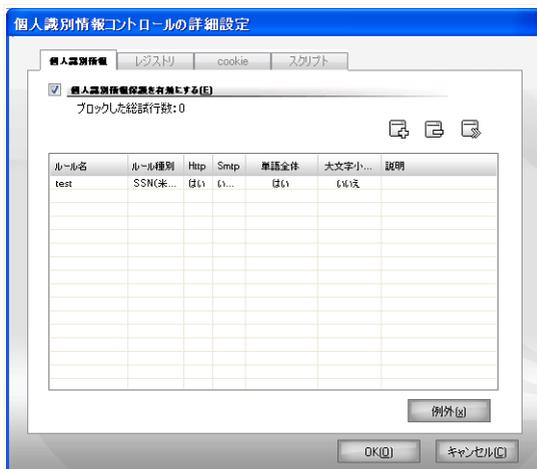
システムを使う他のユーザに、お客様が設定したルールを見られないよう、マルチユーザに対応しています。

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



注意

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



個人識別情報コントロール

11.2.1. 個人識別情報のルール

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

設定ウィザードには、3つの手順があります。

手順1/3 - ルールの形式とデータを設定

ルールの形式およびデータを設定

ルール名を編集フィールドに入力してください。

次の内容を設定する必要があります：

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



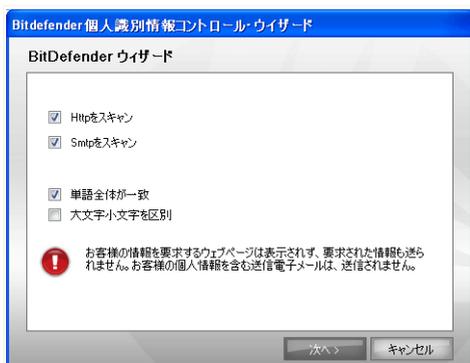
注意

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

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

次へをクリックしてください。

手順2/3 - 通信を選択



通信を選択

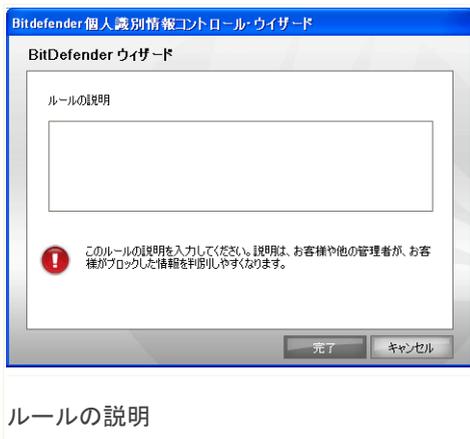
BitDefender にスキャンさせたい通信形式を選択してください。次のオプションが指定できます：

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

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

次へをクリックしてください。

手順3/3 - ルールの説明



ルールの簡単な説明を編集フィールドに入力してください。
終了をクリックしてください。

11.2.2. 例外を指定

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

例外を管理するためのウィンドウを開くには、例外をクリックしてください。

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

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



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

ルールを編集

変更を保存してウィンドウを閉じるには、OKをクリックしてください。

11.3. 詳細設定 - レジストリコントロール

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

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

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



レジストリ警告

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

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



注意

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

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



注意

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

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

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



Cookie 警告

Cookie を送信しようとしているアプリケーション名を確認できます。

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

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



注意

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

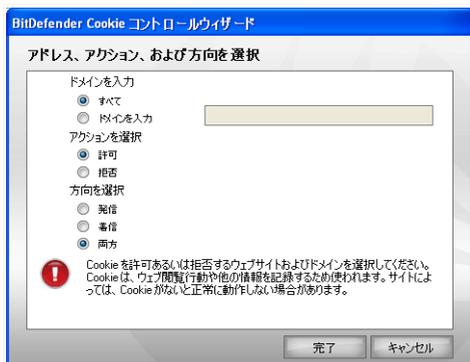
記憶されたすべてのルールは、Cookie画面でさらに調整できます。この画面を開くには、個人情報コントロールの詳細設定ウィンドウを開き、Cookieタブをクリックしてください。



注意

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

手順1/1 - アドレス、アクション、および方向を選択



アドレス、アクション、および方向を選択

内容を設定できます：

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

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

- 方向 - 通信方向を選択してください。

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

終了をクリックしてください。



注意

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

変更を保存してウィンドウを閉じるには、OKをクリックしてください。

11.5. 詳細設定 - スクリプトコントロール

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

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



スクリプト警告

リソース名を確認できます。

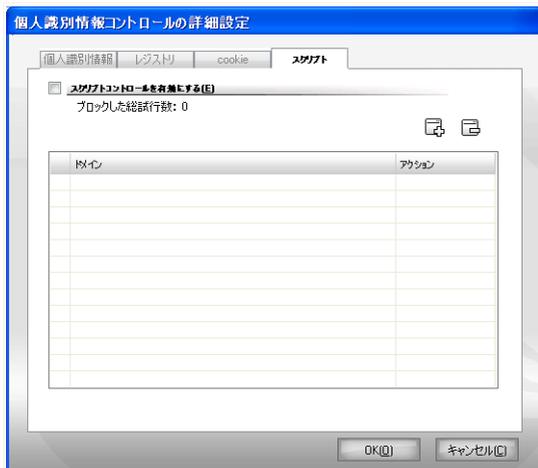
回答を記憶オプションをチェックして、はいあるいはいいえをクリックすると、ルールが作成、適用され、ルール表示に記載されます。同じサイトがアクティブコンテンツを送ってきても、今後は通知されません。

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



注意

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



スクリプトコントロール

これまでに作成したルールが表に記載されます。



重要項目

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

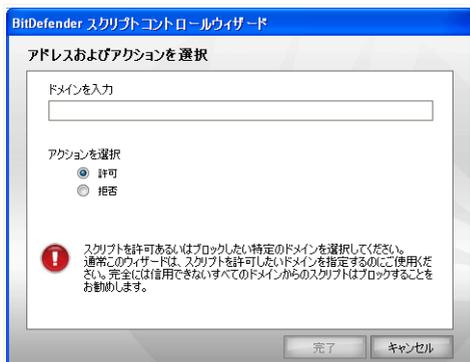
ルールを削除するには、それを選択し、 削除ボタンをクリックしてください。ルールの内容を変更するには、その入力欄をダブルクリックし、必要な変更を加えてください。ルールを削除せず、一時的に無効とするには、対応するチェックボックスのチェックを外してください。

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

11.5.1. 設定ウィザード

設定ウィザードの手順は1つだけです。

手順1/1 - アドレスおよびアクションを選択



アドレスおよびアクションを選択

内容を設定できます：

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

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

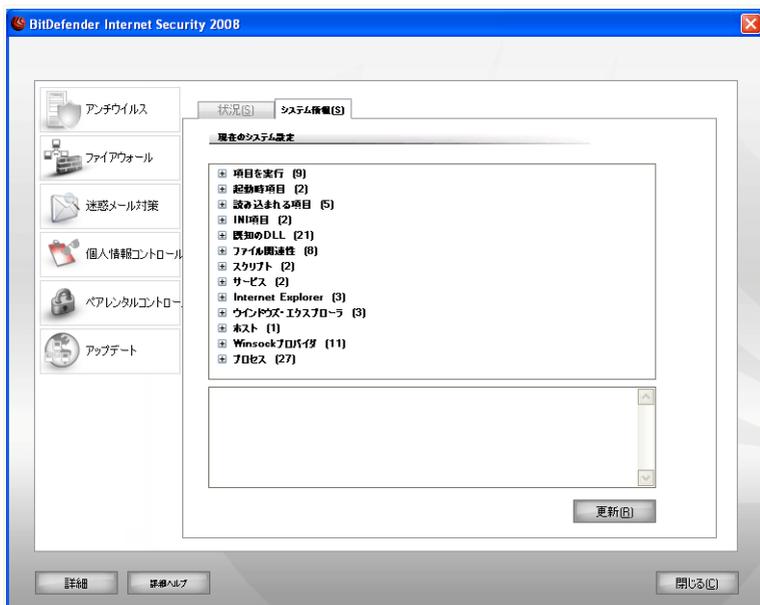
終了をクリックしてください。

変更を保存してウィンドウを閉じるには、OKをクリックしてください。

11.6. システム情報

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

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



システム情報

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

3つのボタンがあります：

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



注意

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

- 表示 - 選択した項目が保管された場所を開きます（例えばレジストリ）。

■更新 - システム情報画面を開き直します。



注意

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

11.7. アンチフィッシングツールバー

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

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

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



注意

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



アンチフィッシングツールバー

ツールバーメニューでは、次のコマンドが使えます：

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



注意

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

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

次のオプションが指定できます：

- ・ スキャンを有効 - アンチフィッシングのスキャンを有効にします。
- ・ ホワイトリストに追加する前に確認 - ウェブサイトをホワイトリストに追加する前にお客様に確認します。

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

**注意**

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

- ホワイトリストを表示 - ホワイトリストを開きます。

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

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

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

- ヘルプ - ヘルプファイルを開きます。
- 説明 - BitDefender および何か問題が起きた際の連絡先について情報を確認できるウィンドウが開きます。

12. 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、次に対するアクセスをブロックできます：

- 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および電子メールメッセージ。
- 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。



重要項目

このモジュールは、管理者権限を持つユーザ（システム管理者）だけが開いて設定することができます。設定がパスワード保護されていれば、パスワードを入力した場合にだけ変更が可能です。他の管理者によってすでにルールが定義されたユーザのルールを、管理者が無理矢理変更することはできません。

このガイドの保護者による管理の項には、以下の内容があります：

- **ペアレンタルコントロール設定の保護**
- **ペアレンタルコントロールの状態**
- **ウェブコントロール**
- **アプリケーションコントロール**
- **キーワードフィルタ**
- **ウェブ時間制限**

12.1. ペアレンタルコントロール設定の保護

お客様以外の人もこのコンピュータを使う管理者権限を持っているなら、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するには、次を実行してください：

1. パスワードをパスワード欄に入力します。
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. パスワード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。

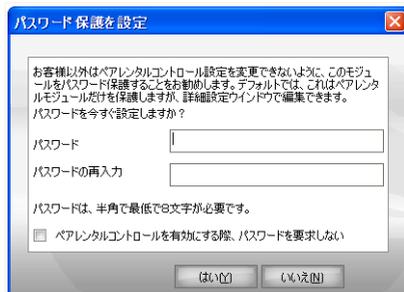
パスワードが設定されると、ペアレンタルコントロール設定を変更しようとする度に、パスワードの入力を求められます。他のシステム管理者（もしあれば）もペアレンタルコントロール設定を変更する際には、パスワードの入力を求められます。



注意

このパスワードは、他の BitDefender 設定は保護しません。

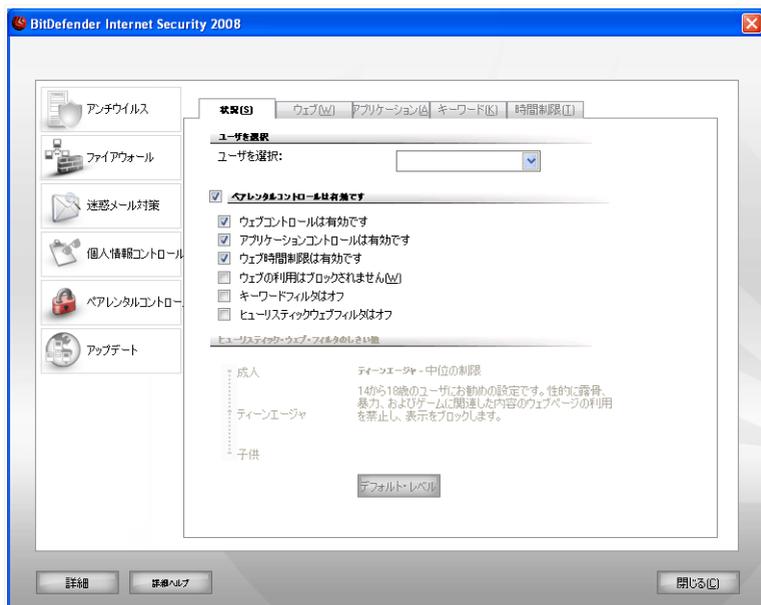
パスワードを設定せず、このウィンドウが表示されないようにするには、ペアレンタルコントロールを有効にする際、パスワードを要求しないにチェックしてください。



パスワード保護を設定

12.2. ペアレンタルコントロールの状態

選択したユーザのペアレンタルコントロールを設定するには、設定コンソールで「保護者による管理」状態をクリックしてください。次のウィンドウが開きます：



ペアレンタルコントロールの状態



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ください。

12.2.1. ペアレンタルコントロールを選択

保護レベルを設定するには、まずその設定を適用したいユーザを選択してください。次に以下のコントロールを使って保護レベルを設定してください：

- **ウェブコントロール** - **ウェブ**の項でお客様が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、ウェブコントロールを有効にしてください。
- **アプリケーションコントロール** - **アプリケーション**の項でお客様が設定したルールに従ってアプリケーションの利用をブロックするには、アプリケーションコントロールを有効にしてください。

- ウェブ時間制限 - **時間制限**の項でお客様が設定した時間表に従ってウェブ閲覧を許可するには、ウェブ時間制限を有効にしてください。
- ウェブ閲覧 - すべてのウェブサイト（**ウェブ**の項にあるもの以外も）の利用をブロックするには、このオプションを有効にしてください。
- キーワードフィルタ - **キーワード**の項でお客様が設定したルールに従って、ウェブおよびメールをフィルタリングするには、キーワードフィルタを有効にしてください。
- ヒューリスティック・ウェブフィルタ - 年齢カテゴリを基に設定されたルールに沿ってウェブアクセスをフィルタリングするには、このオプションを有効にしてください。



注意

ペアレンタルコントロールが提供する機能を最大限有効利用するには、選択したコントロールを設定しなければなりません。その設定方法については、この章の次のトピックを参照してください。

12.2.2. ヒューリスティック・ウェブフィルタを設定

ヒューリスティック・ウェブフィルタは、ウェブページを分析し、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、特定の保護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切と思われる保護レベルに設定できます。

3種類の保護レベルがあります：

しきい値レベル	説明
子供	14歳以下のユーザ用の推奨設定に従って、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、子供に害を与える可能性のあるコンテンツのウェブページはブロックされます。
ティーンエイジャ	14から18歳のユーザ用の推奨設定に従って、ウェブの利用を制限できます。

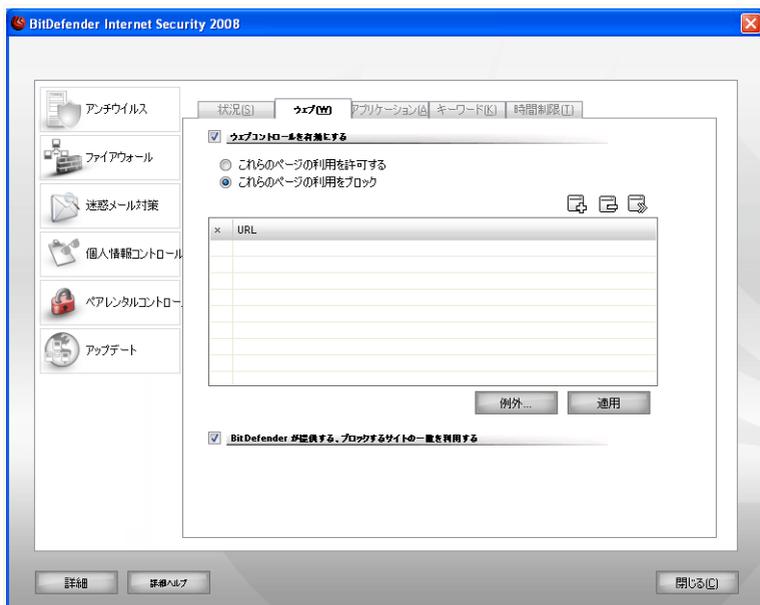
しきい値レベル	説明
	性的、ポルノ、あるいは成年向けコンテンツのウェブページはブロックされます。
成人	そのコンテンツに関わらず、すべてのウェブページの利用を無制限に許可します。

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てください。

12.3. 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のブロックに貢献します。ブロックしたいサイトおよびその部分の候補一覧が BitDefender によって提供され、通常のアップデート処理の一環としてアップデートされます。

ウェブコントロールを設定するには、設定コンソールで保護者による管理>ウェブをクリックしてください。次のウィンドウが開きます：



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。

許可/ブロックされたサイトの一覧を表示するには、これらのページの利用を許可/これらのページの利用をブロックを選択してください。例外... をクリックすると、他の一覧を表示します。

ルールは手動で入力する必要があります。まず、ウェブサイトを許可/ブロックするため、これらのページの利用を許可/これらのページの利用をブロックを選択します。次に、 追加... ボタンをクリックして設定ウィザードを開始します。

12.3.1. 設定ウィザード

設定ウィザードの手順は1つだけです。

手順 1/1 - ウェブサイトを指定



ウェブサイトを指定

ルールが適用されるウェブサイトを入力し、完了をクリックします。



重要項目

構文：

- *. xxx. com - ルールのアクションは、. xxx. comで終わるすべてのウェブサイトに応用されます；
- *porn* - ルールのアクションは、ウェブサイトのアドレスにpornを持つすべてのウェブサイトに応用されます；
- www. *. com - ルールのアクションは、ドメインの最後にcomを持つすべてのウェブサイトに応用されます；
- www. xxx. * - ルールのアクションは、ドメインの末尾に関わらず、www. xxx. で始まるすべてのウェブサイトに応用されます。

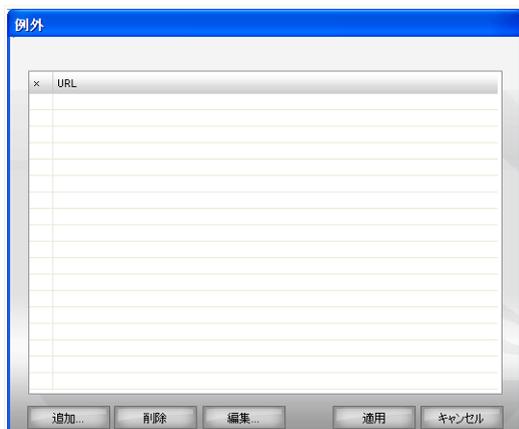
適用をクリックして、変更を保存してください。

ルールを削除するには、対象を選択し、 削除ボタンをクリックしてください。ルールの編集は、対象を選択し、 編集... ボタンをクリックするか、ダブルクリックしてください。ルールを削除せず、一時的に無効にするには、対応するチェックボックスのチェックを外します。

12.3.2. 例外を指定

場合によっては、特定のルールに例外を指定する必要があります。例えば、アドレスに“killer”が含まれるサイトをブロックするルール（構文：*killer*）を設定したとします。同時に、オンラインで音楽を聴けるkiller-musicというサイトの存在も知っているとして。作成したルールに例外として指定するには、例外ウィンドウを開き、ルールの例外を指定してください。

例外... をクリックしてください。次のウィンドウが開きます：



例外を指定

例外を指定するには、追加... をクリックしてください。設定ウィザードが表示されます。ウィザードを完了すると例外が設定されます。

適用をクリックして、変更を保存してください。

ルールを削除するには、対象を選択し、削除をクリックしてください。ルールを編集するには、編集... をクリックするか、項目をダブルクリックしてください。ルールを削除せず、一時的に無効にするには、対応するチェックボックスのチェックを外してください。

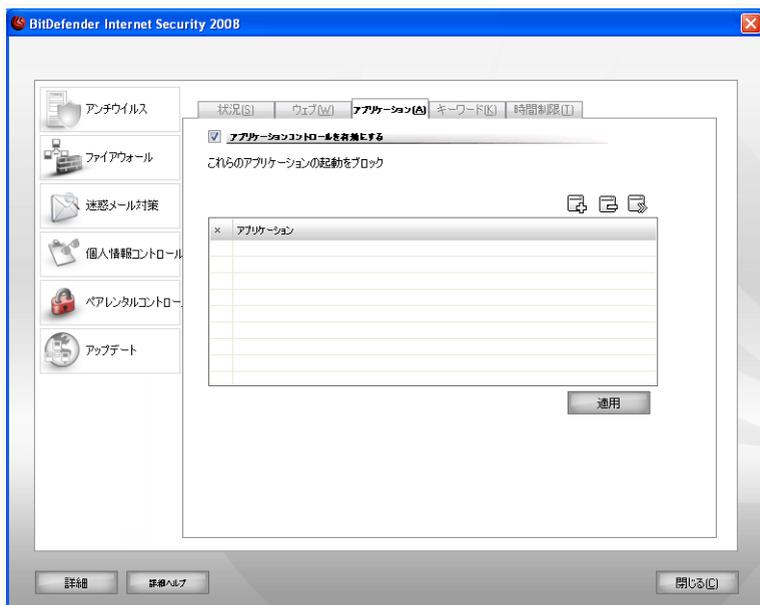
12.3.3. BitDefender のウェブブラックリスト

子供を守るために、BitDefender は不適切あるいは害がある可能性のあるコンテンツのウェブサイトのブラックリストを持っています。この一覧に記載されたサイトをブロックするには、BitDefender が提供する、ブロックするサイトの一覧を利用するを選択してください。

12.4. 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。

アプリケーションコントロールを設定するには、設定コンソールで保護者による管理>アプリケーションをクリックしてください。 次のウィンドウが開きます：



アプリケーションコントロール

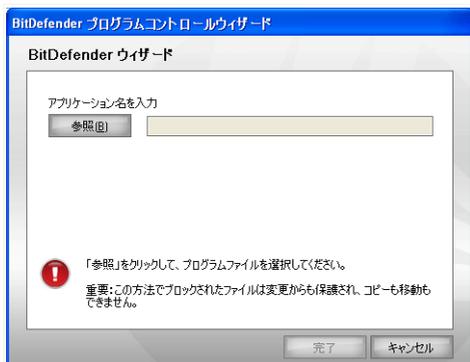
この保護を有効にするには、アプリケーションコントロールを有効にするチェックボックスを選択してください。

ルールは手動で入力しなければなりません。追加... ボタンをクリックして、設定ウィザードを開始してください。

12.4.1. 設定ウィザード

設定ウィザードの手順は1つだけです。

手順1/1 - ブロックするアプリケーションを選択



ブロックするアプリケーションを選択

参照をクリックし、ブロックしたいアプリケーションを選択して、完了をクリックしてください。

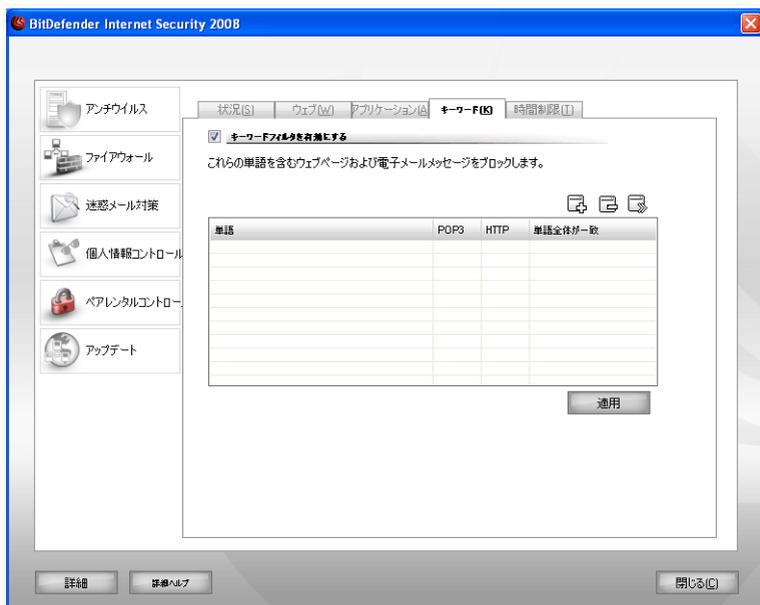
適用をクリックして、変更を保存してください。

ルールを削除するには、対象を選択し、 削除ボタンをクリックしてください。ルールの編集は、対象を選択し、 編集... ボタンをクリックするか、ダブルクリックしてください。ルールを削除せず、一時的に無効にするには、対応するチェックボックスのチェックを外します。

12.5. キーワードフィルタ

キーワードフィルタは、特定の単語を持つ電子メールメッセージあるいはウェブページのブロックを手助けします。この方法で、ユーザが不適切な単語や文章を見ないようにします。

キーワードフィルタを設定するには、設定コンソールで保護者による管理>キーワードをクリックしてください。次のウィンドウが開きます：



キーワードフィルタ

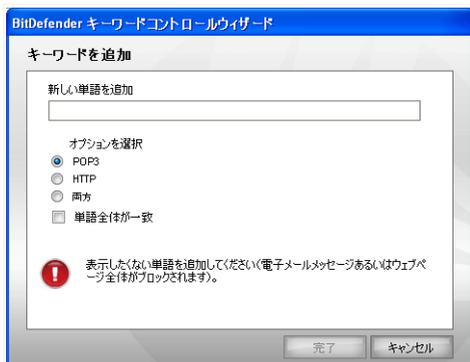
この保護を有効にするには、キーワードフィルタを有効にするチェックボックスを選択してください。

ルールは手動で入力しなければなりません。追加... ボタンをクリックして、設定ウィザードを開始してください。

12.5.1. 設定ウィザード

設定ウィザードの手順は1つだけです。

手順1/1 - キーワードを入力



キーワードを入力

次の内容を設定する必要があります：

- キーワード - ブロックしたい単語あるいは文章を編集欄に入力してください。
- プロトコル - BitDefender が特定の単語をスキャンするプロトコルを選んでください。

次のオプションが指定できます：

オプション	説明
POP3	キーワードを含む電子メールメッセージはブロックされます。
HTTP	キーワードを含むウェブページはブロックされます。
両方	キーワードを含む電子メールメッセージおよびウェブページは、両方ともブロックされます。

適用をクリックして、変更を保存してください。

ルールを削除するには、対象を選択し、 削除ボタンをクリックしてください。ルールの編集は、対象を選択し  編集... ボタンをクリックするか、ダブルクリッ

クしてください。ルールを削除せず、一時的に無効にするには、対応するチェックボックスのチェックを外します。

12.6. ウェブ時間制限

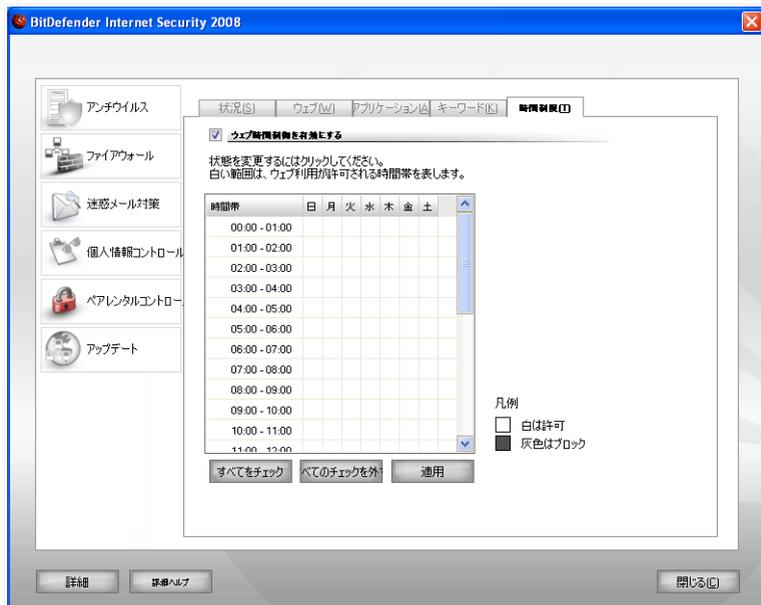
ウェブ時間制限は、指定した時間、ユーザあるいはアプリケーションによるウェブの利用を許可あるいはブロックするようにします。



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。

ウェブ時間制限を設定するには、設定コンソールで保護者による管理>時間制限をクリックしてください。次のウィンドウが開きます：



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てください。

すべてのインターネット接続がブロックされる時間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して長い期間を指定できます。またすべてをチェックをクリックしてすべてのセルを選択し、すべてのウェブアクセスをブロックすることもできます。チェックを外すをクリックすると、インターネット接続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。

適用をクリックして、変更を保存してください。

13. アップデート

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

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

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

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

アップデートは、次の方法で実行されます：

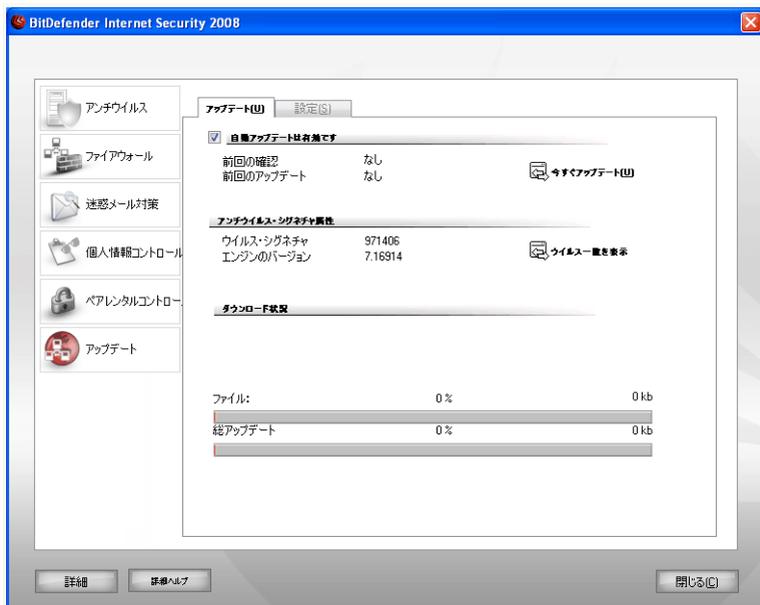
- **アンチウイルスエンジン用アップデート** - 新しい脅威が現れた際に、今後もそのウイルスから保護するためにはウイルスシグネチャを含むファイルをアップデートしなければなりません。このアップデート形式は、ウイルス定義のアップデートとも呼ばれます。
- **アンチスパムエンジン用アップデート** - ヒューリスティックおよびURLフィルタには新しいルールが追加され、イメージフィルタには新しいイメージが追加されます。これでお使いのアンチスパムエンジンの効率を向上させます。このアップデート形式は、アンチスパム用アップデートとも呼ばれます。
- **アンチスパイウェアエンジン用アップデート** - 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。

このユーザガイドのアップデートの項では、次の内容を取り上げます：

- **自動アップデート**
- **アップデートの設定**

13.1. 自動アップデート

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



自動アップデート

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

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

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

アップデート中にこの画面を開くと、ダウンロード状況が表示されます。



重要項目

最新の脅威から保護されるには、自動アップデートを有効にしておいてください。

13.1.1. アップデートを請求

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

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



重要項目

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

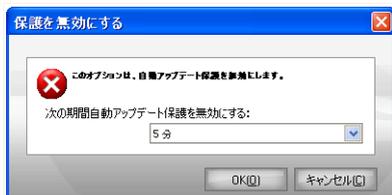


注意

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

13.1.2. 自動アップデートを無効にする

自動アップデートを無効にすると、警告ウインドウが開きます。



自動アップデートを無効にする

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



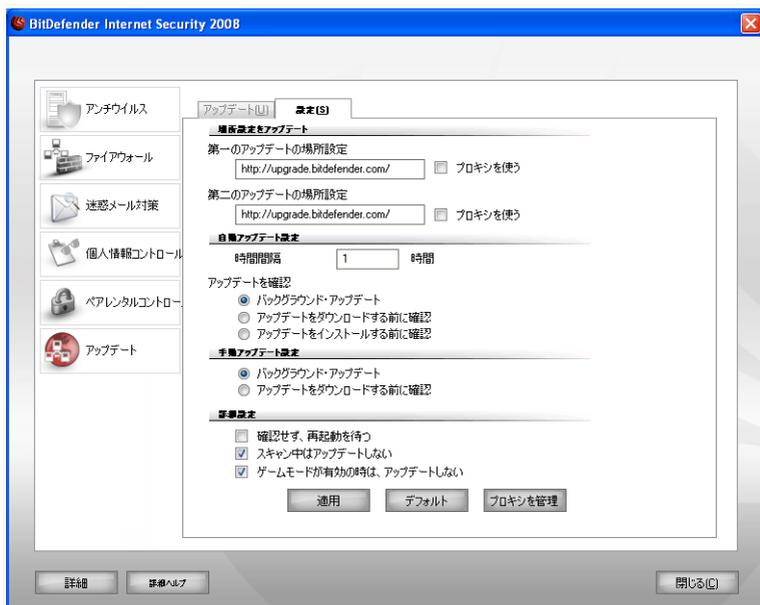
警告

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

13.2. アップデート設定

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

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



アップデート設定

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

13.2.1. アップデートの場所を設定

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



注意

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

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

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



注意

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

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



注意

詳細については、「[プロキシを管理](#)」(p. 195)を参照してください。

13.2.2. 自動アップデート設定

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

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

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

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



注意

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

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

**注意**

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

13.2.3. 手動アップデート設定

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

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

**注意**

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

13.2.4. 詳細設定

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

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

**注意**

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

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

13.2.5. プロキシを管理

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



注意

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

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

プロキシマネージャ

プロキシ設定

管理者プロキシ設定 (インストール時に輸出されました)

アドレス: ポート: ユーザ名:
 パスワード:

現在のユーザのプロキシ設定 (デフォルトブラウザから)

アドレス: ポート: ユーザ名:
 パスワード:

お客様独自のプロキシ設定を指定してください

アドレス: ポート: ユーザ名:
 パスワード:

OK キャンセル

プロキシマネージャ

プロキシ設定には、3つのセットがあります：

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



注意

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

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

次の設定を指定してください：

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

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

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

変更を保存してウィンドウを閉じるには、OKをクリックしてください。

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

BitDefender Rescue CD

14. 概要

BitDefender Internet Security 2008には、お使いのオペレーティングシステムが起動する前に、既存のすべてのハードディスクをスキャンおよびウイルス駆除できる、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イルス感染のせいで正常に動作していない時は、すぐに BitDefender Rescue CD を使ってください。アンチウイルス製品をインストールしていないとき、そのような状態になる可能性があります。

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

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



注意

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

14.1. システム要項

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

プロセッサ形式

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

メモリ

最小512 MBのRAMメモリ (1 GB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。

14.2. 同梱されるソフトウェア

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

Xedit

これはテキストファイルエディタです。

Vim

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

Xcalc

これは計算機です。

RoxFiler

RoxFiler は、高速で強力な、グラフィカルなファイルマネージャです。

詳細については、[RoxFiler のホームページ](#)をご参照ください。

MidnightCommander

GNU Midnight Commander (mc) は、テキストモードのファイルマネージャです。

詳細については、[MC のホームページ](#)をご参照ください。

Pstree

Pstree は、実行中のプロセスを表示します。

Top

Top は、Linux タスクを表示します。

Xkill

Xkill は、クライアントをその X リソースで「キル」します。

Partition Image

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

詳細については、[Partimageのホームページ](#)をご参照ください。

GtkRecover

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

詳細については、[GtkRecoverのホームページ](#)をご参照ください。

ChkRootKit

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

詳細については、[ChkRootKit のホームページ](#)をご参照ください。

Nessus Network Scanner

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

詳細については、[Nessus のホームページ](#)をご参照ください。

lptraf

lptrafは、IP Network Monitoring Softwareです。

詳細については、[lptraf のホームページ](#)をご参照ください。

lftop

lftop 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、[lftop のホームページ](#)をご参照ください。

MTR

MTR は、ネットワーク分析ツールです。

詳細については、[MTR のホームページ](#)をご参照ください。

PPPStatus

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

詳細については、[PPPStatus のホームページ](#)をご参照ください。

Wavemon

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

詳細については、[Wavemon のホームページ](#)をご参照ください。

USBView

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

詳細については、[USBView のホームページ](#)をご参照ください。

Pppconfig

Pppconfig は、ダイヤルアップ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。

15. 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。

15.1. BitDefender Rescue CD を起動

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

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



起動画面

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

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



デスクトップ

15.2. 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。

```
X Window session terminated without errors.
Shutting down.
INIT: Sending processes the KILL signal
Killing processes with signal 15: (init) (aufsd) (aufsd) (aufsd) (aufsd)
(ald) (hald-addon-acpi) (hald-addon-keyb) (ksoftirqd/0) (logsave) (inetd)
(s/0) (khelper) (kthread) (ata/0) (ata_aux) (kseriod) (kpsmoused) (ksuspent)
(aio/0) Done.
Waiting for processes to finish.....
Killing processes with signal 9: (init) (aufsd) (aufsd) (aufsd) (aufsd)
(kblockd/0) (kacpid) (knoppix-halt) (events/0) (khelper) (kthread) (ata/0)
(d) (khapsbpkt) (pdflush) (pdflush) (kswapd0) (aio/0) Done.
Waiting for processes to finish.....
Syncing/Unmounting filesystems: /sys/fs/fuse/connections /UNIONFS/lib/in
Turning off swap... Done.
Unmounting remaining file systems.
rootfs unmounted

KNOPPIX halted.
Please remove CD, close cdrom drive and hit return [auto 2 minutes].
```

終了する場合は、このメッセージを待ってください。

15.3. どうやってアンチウイルススキャンを実行するのですか？

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



注意

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

次の3つの手順に従って、スキャン処理を完了させてください。

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



注意

スキャンの内容によっては、スキャン処理に時間がかかる場合があります。

2. お使いのシステムに影響する問題の数を確認できます。

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

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

3. 結果の概要を確認できます。

特定のディレクトリのみをスキャンしたい場合は、次の手順を実行してください：

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

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

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

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

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

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

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

15.5. データをどうやって保存するのですか？

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

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

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

2. BitDefender Rescue CD が起動するのを待ってください。次のウ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。

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。

問い合わせ先

16. サポート

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

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

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

16.1. BitDefender Knowledge Base

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

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

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

16.2. ヘルプを依頼

16.2.1. Web Self Service を開いてください

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

次のリンクを参照してください：

English

<http://www.bitdefender.com/site/KnowledgeBase/browseProducts/2195/>

German

<http://www.bitdefender.com/de/KnowledgeBase/browseProducts/2195/>

French

<http://www.bitdefender.com/fr/KnowledgeBase/browseProducts/2195/>

Romanian

<http://www.bitdefender.com/ro/KnowledgeBase/browseProducts/2195/>

Spanish

<http://www.bitdefender.com/es/KnowledgeBase/browseProducts/2195/>

16.2.2. サポートチケットを開く

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

English: <http://www.bitdefender.com/site/Main/contact/1/>

German: <http://www.bitdefender.de/site/Main/contact/1/>

French: <http://www.bitdefender.fr/site/Main/contact/1/>

Romanian: <http://www.bitdefender.ro/site/Main/contact/1/>

Spanish: <http://www.bitdefender.es/site/Main/contact/1/>

16.3. 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。

16.3.1. ウェブアドレス

営業: sales@bitdefender.com

技術サポート: support@bitdefender.com

図書制作: documentation@bitdefender.com

パートナープログラム: partners@bitdefender.com

マーケティング: marketing@bitdefender.com

広報: pr@bitdefender.com

求人: jobs@bitdefender.com

ウイルスの提出: virus_submission@bitdefender.com

迷惑メールの提出: spam_submission@bitdefender.com

悪用の報告: abuse@bitdefender.com

製品のウェブサイト: <http://www.bitdefender.com>

製品のFTPアーカイブ: <ftp://ftp.bitdefender.com/pub>

各地の代理店: http://www.bitdefender.com/partner_list

BitDefender Knowledge Base: <http://kb.bitdefender.com>

16.3.2. 支店

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

U. S. A

BitDefender, LLC

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

■E-mail: support@bitdefender.com

■Phone:

- 1-888-868-1873 (Registered Users Only; accessible in United States only)
- 1-954-776-6262 (Registered Users Only)

Customer Service:

■E-mail: customerservice@bitdefender.com

■Phone:

- 1-888-868-1873 (Registered Users Only; accessible in United States only)
- 1-954-776-6262 (Registered Users Only)

Germany

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

UK and Ireland

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

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

Spain

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

Romania

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

用語集

ActiveX

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

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

アドウェア

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

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

アーカイブ

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

1つ以上のファイルを圧縮された状態で保管しているファイルです。

バックドア

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

起動セクター

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

ブートウイルス

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

ブラウザ

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

コマンドライン

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

Cookie（クッキー）

インターネットの世界では、Cookie は、お客様のオンライン上での興味や嗜好を知るために広告主が分析、利用する、個々のコンピュータに関する情報を保管した小さなファイルを意味します。その目的は、お客様が興味を持っているものを直接宣伝することですが、Cookie 技術はまだ発展途上でもあります。お客様が興味を持つ広告だけが届くので、ある意味では効率がよく理想的な技術ですが、そのためにお客様が訪問してクリックしたものを“監視”し“記録”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、多くの人々は“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方でもあります。

ディスクドライブ

ディスクにデータを読み書きする機械です。

ハードディスクドライブは、ハードディスクを読み書きします。

フロッピードライブは、フロッピーディスクを読み書きします。

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

ダウンロード

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

電子メール

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

イベント

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

擬陽性

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

ファイル名拡張子

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

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

ヒューリスティック

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

IP

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

Java アプレット

ウェブページ上だけで実行されるように設計された Java プログラムです。ウェブページでアプレットを使うには、アプレットが利用できるアプレットの名前とサイズ（ピクセル単位の長さや幅）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（クライアント）上で実行します。アプレットは、厳密なセキュリティプロトコルで管理されている点で、アプリケーションと異なります。

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

マクロウイルス

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

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

メールクライアント

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

メモリ

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

非ヒューリスティック

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

バックされたプログラム

圧縮形式のファイルです。多くのオペレーティングシステムおよびアプリケーションは、ファイルサイズを小さくするためにファイルをバ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。

しかしファイルをバ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。これはバック技術の1例で、世の中には多くの技術が存在します。

パス

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

2台のコンピュータ間の通信チャンネルのような、2点間をつなぐルートです。

フィッシング

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

多形性ウイルス

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

ポート

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

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

レポートファイル

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

Rootkit

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

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

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

スクリプト

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

迷惑メール

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

スパイウェア

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

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

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

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

起動項目

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

システムトレイ

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

TCP/IP

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

トロイの木馬

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

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

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

アップデート

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

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

ウイルス

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

ウイルス定義

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

ワーム

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