Bitdefender TOTAL SECURITY

ユーザーガイド

Bitdefender Total Security
ユーザーガイド

Publication date 07/26/2018

免責事項

Bitdefender

目次

このガイドについて

1. 目的および対象ユーザー

お客様の Bitdefender Total Security サブスクリプションは、Windows PC、Mac、iOS、Android スマートフォンおよびタブレットを保護できます。保護しているデバイスの管理は、 Bitdefender アカウントを使って行うことができます。アカウントは、アクティブなサブスクリプションと紐付けされている必要があります。

このガイドは、サブスクリプションに含まれる以下の製品のセットアップおよび使用方法をご案内します: Bitdefender Total Security (Windows)、 Bitdefender Antivirus for Mac (macOS)、Bitdefender Mobile Security (Android)、および Bitdefender Mobile Security for iOS。

あらゆる脅威から各デバイスを保護するための Bitdefender の設定方法を学ぶことができます。

2. このガイドの使い方

このガイドは、 Bitdefender Total Security に含まれる 4 つの製品で構成されています:

- 「PC 用のトータルセキュリティ」 (p. 1)

  この製品を Windows PC で使用する方法を学びましょう。

- 「Antivirus for Mac」 (p. 214)

  この製品を Mac で利用するには

- 「Mobile Security for iOS」 (p. 257)

  この製品を iOS スマートフォンおよびタブレットで使用する方法を学びましょう。

- 「Mobile Security for Android」 (p. 274)

  この製品を Android スマートフォンおよびタブレットで使用する方法を学びましょう。

- 「お問い合わせ」 (p. 316)

  予期しない事態が発生した際の、ヘルプの参照方法を確認しましょう。

PC 用のトータルセキュリティ

1. インストール

1.1. インストールの準備

Bitdefender Total Securityのインストールを開始する前に、以下の準備を行なってください：

- Bitdefenderをインストールするパソコンが、最低限のシステム要件を満たしているかご確認ください。 パソコンがシステム要件をすべて満たしていない場合、 Bitdefender は、インストールに失敗するか、またはインストールできたとしても正しく動作せず、システムが遅くなったり不安定になる可能性があります。 システム要件の一覧を確認するには、「システム要件」 (p. 215) を参照してください。
- 管理者アカウントで、パソコンにログインしてください。
- パソコンから他のセキュリティ対策ソフトを削除してください。 Bitdefender のインストール中に別のアプリケーションが検出された場合、アンインストールを促すメッセージが表示されます。 2つのセキュリティソフトを併用すると、ソフトの動作に影響を与え、システムに重大な問題を引き起こす可能性があります。 インストール中、Windows Defenderは無効になります。
- パソコンで使用しているファイアウォールを無効にするか、削除してください。 2つのファイアウォールを併用すると、各ソフトの動作に影響を与え、システムでも重度な問題を引き起こしてしまう可能性があります。 インストール中、Windowsファイアウォールは無効にされます。
- 製品は（CD/DVDからインストールする場合も含め）、パソコンをインターネットに接続した状態でインストールすることをおすすめします。 インストールに必要な、より新しいバージョンのファイルがある場合は、Bitdefenderがダウンロードしてインストールします。

1.2. システム要件

Bitdefender Total Securityは以下のオペレーティング システムでのみ動作します：

- Windows 7 Service Pack 1 (SP1)
- Windows 8
- Windows 8.1
- Windows 10

インストールを開始する前に、お使いのパソコンが最低動作条件を満たしているかご確認ください。

注記
お使いのコンピュータの Windows オペレーティングシステムおよびハードウェア情報を確認するには:

- Windows 7 デスクトップ上のマイ コンピュータ を右クリックし、メニューから プロパティ を選択します。
- Windows 8の場合、Windowsスタート画面から「コンピュータ」を探して（またはスタート画面で「コンピュータ」と入力して）、アイコンを右クリックしてください。 Windows 8.1 で この PC を参照します。

  メニュー下部のプロパティを選択してください。 システムエリアで、システムのタイプに関する情報を確認します。
- Windows 10 のタスクバーの検索ボックスに「システム」と入力し、アイコンをクリックします。 システムエリアで、システムのタイプに関する情報を確認します。

最低動作条件

- ハードディスク空き容量： 2 GB 以上
- デュアルコア 1.6 GHz プロセッサ
- 1 GB のメモリ（RAM）

推奨動作環境

- 2.5 GB 以上のハードディスク空き容量（システムドライブ上に 800MB 以上の空き容量）
- Intel CORE Duo（2 GHz）、または、それに相当するプロセッサ
- 2 GB のメモリ（RAM）

動作環境

お使いのパソコンで、 Bitdefender のすべての機能を使用するには、パソコンが以下の条件を満たす必要があります：

- Microsoft Edge 40 以上
- Internet Explorer バージョン 10 以上
- Mozilla Firefox 51 以上
- Google Chrome 34 以上

1.3. Bitdefenderをインストール

Bitdefender はインストールディスクから、あるいは Bitdefender Central を使ってコンピュータにダウンロードしたウェブインストーラからインストールできます。

複数台のコンピュータをカバーするサブスクリプションを購入した場合、それぞれのコンピュータに製品をインストールし、同じアカウントですべての製品を有効化します。 Bitdefender の有効なサブスクリプションが含まれているアカウントを使用する必要があります。

Bitdefender Centralからインストール

購入したサブスクリプションに応じたインストールキットを、 Bitdefender Central からダウンロードすることができます。 インストール処理が完了すると Bitdefender Total Security が有効化されます。

Bitdefender Total Security を Bitdefender Central からダウンロードするには:

1. Bitdefender Centralにアクセスします。
2. マイデバイス パネルを選択し、保護をインストール をクリックします。
3. 以下のいずれかのオプションを選択します:

   - このデバイスを保護

     このオプションを選択するとインストールファイルを保存できます。

   - 他のデバイスを保護

     このオプションを選択してから、ダウンロードリンクを送信 をクリックします。 当該フィールドにメールアドレスを入力してメールを送信をクリックします。 ダウンロードリンクは、以後 24 時間のみ有効です。 リンクの有効期限が切れた場合は、同じ手順を実行して新しいリンクを生成する必要があります。

     Bitdefender 製品をインストールしたいデバイス上で、登録したメールアドレスの受信トレイを開き、届いたメールに記載されているダウンロードボタンをクリックしてください。

4. ダウンロードが完了するまでお待ちください。ダウンロードが完了したら、インストーラーを実行します。

インストール前の確認

Bitdefender は、まず最初にお使いのパソコンのインストール検証を行います。

パソコンがBitdefenderをインストールするために必要な最低動作条件を満たしていない場合は、条件を満たしていない項目が表示されます。

併用できないセキュリティソリューション、または Bitdefender の古いバージョンが検出された場合は、パソコンから削除するように案内されます。 今後のトラブルを回避するために、手順に従ってソフトウェアをシステムから削除してください。 検知したセキュリティソリューションを削除するには、パソコンの再起動が必要になる場合があります。

Bitdefender Total Security のインストールパッケージは、随時更新されています。

注記
低速回線をご利用の場合、最新インストールファイルのダウンロードに時間がかかる場合があります。

インストール前の確認が終わると、セットアップ・ウィザードが起動されます。 手順に従って、 Bitdefender Total Security のインストールを行なってください。

ステップ 1 - Bitdefender のインストール

インストールを続行する前に、サブスクリプション契約に同意する必要があります。 サブスクリプション契約には、 Bitdefender Total Security を使用する上で守っていただく条件が記載されていますので、必ずよくお読みください。

使用許諾書の条件に同意されない場合は、ウィンドウを閉じてください。 インストールは中断され、セットアップは終了します。

このステップでは、さらに 2 つのタスクを実行できます:

- 製品レポートを送信 オプションは有効のままにしてください。 このオプションを許可すると、製品の使用状況を含むレポートが Bitdefender のサーバーに送信されます。 この情報は製品の改良のために重要であり、より良い製品のご提供に役立てられます。 なお、これらのレポートにはお客様の個人データ（お名前や IP アドレスなど）は一切含まれておりませんので、これらのデータが商業目的に利用されることもありません。

- 製品をインストールする言語を選択してください。

インストール ボタンをクリックすると、 Bitdefender 製品のインストールが開始されます。

ステップ2 - インストール中

インストールが完了するまでお待ちください。 進捗に関する詳細情報が表示されます。

システムの重要な領域の脅威検査を行い、最新のアプリケーションファイルをダウンロード・インストールし、 Bitdefender のサービスを開始します。 この手順は数分で完了します。 システムを後でスキャンする場合はスキャンをスキップをクリックします。 システムスキャンの実行についての詳細は 「パソコン全体の検査を実行する」 (p. 87) を参照してください。

ステップ 3 - インストール完了

Bitdefenderのインストールが正しく完了しました。

インストールの概要が表示されます。 インストール中に脅威を検知した場合は、パソコンの再起動が必要になる場合があります。 Bitdefender を使用開始 をクリックして続行します。

ステップ 4 - 開始する

始める ウィンドウには、現在アクティブなサブスクリプションの情報が表示されます。

Bitdefender Total Security のインターフェイスにアクセスするには 完了 をクリックします。

インストールディスクからインストール

Bitdefenderをインストールディスクからインストールするには、まずディスクを光学ドライブ（CD/DVDドライブ）へ挿入します。

しばらくするとインストール画面が表示されます。 指示に従って、インストールを開始してください。

インストール画面が表示されない場合は、Windows エクスプローラーを使ってディスクのルートディレクトリにアクセスし、autorun.exe ファイルをダブルクリックしてください。

インターネット速度が遅い、またはシステムがインターネットに接続されていない場合は、CD/DVD からインストール ボタンをクリックします。 この場合、ディスク上の Bitdefender 製品がインストールされ、製品アップデート時に Bitdefender サーバから最新バージョンが ダウンロードされます。

インストール前の確認

Bitdefender は、まず最初にお使いのパソコンのインストール検証を行います。

パソコンがBitdefenderをインストールするために必要な最低動作条件を満たしていない場合は、条件を満たしていない項目が表示されます。

併用できないセキュリティソリューション、または Bitdefender の古いバージョンが検出された場合は、パソコンから削除するように案内されます。 今後のトラブルを回避するために、手順に従ってソフトウェアをシステムから削除してください。 検知したセキュリティソリューションを削除するには、パソコンの再起動が必要になる場合があります。

注記
低速回線をご利用の場合、最新インストールファイルのダウンロードに時間がかかる場合があります。

インストール前の確認が終わると、セットアップ・ウィザードが起動されます。 手順に従って、 Bitdefender Total Security のインストールを行なってください。

ステップ 1 -Bitdefender のインストール

インストールを続行する前に、サブスクリプション契約に同意する必要があります。 サブスクリプション契約には、 Bitdefender Total Security を使用する上で守っていただく条件が記載されていますので、必ずよくお読みください。

使用許諾書の条件に同意されない場合は、ウィンドウを閉じてください。 インストールは中断され、セットアップは終了します。

このステップでは、さらに 2 つのタスクを実行できます:

- 製品レポートを送信 オプションは有効のままにしてください。 このオプションを許可すると、製品の使用状況を含むレポートが Bitdefender のサーバーに送信されます。 この情報は製品の改良のために重要であ

り、より良い製品のご提供に役立てられます。 なお、これらのレポートにはお客様の個人データ（お名前や IP アドレスなど）は一切含まれておりませんので、これらのデータが商業目的に利用されることもありません。

- 製品をインストールする言語を選択してください。

インストール ボタンをクリックすると、 Bitdefender 製品のインストールが開始されます。

ステップ2 - インストール中

インストールが完了するまでお待ちください。 進捗に関する詳細情報が表示されます。

システムの重要部分の脅威チェックを実行後、 Bitdefender のサービスを開始します。 この手順は数分で完了します。 システムを後でスキャンする場合は スキャンをスキップをクリックします。 システムスキャンの実行についての詳細は 「パソコン全体の検査を実行する」 (p. 87) を参照してください。

ステップ 3 - インストール完了

インストールの概要が表示されます。 インストール中に脅威を検知した場合は、パソコンの再起動が必要になる場合があります。 Bitdefender を使用開始 をクリックして続行します。

ステップ 4 - Bitdefender アカウント

初期セットアップが完了すると、 Bitdefender アカウントのウィンドウが表示されます。 製品のライセンスを有効化し、オンライン機能を使用するには Bitdefender アカウントが必要です。 詳細については、「Bitdefender Central」 (p. 31)をご参照ください。

アカウントをお持ちの場合、作成が必要な場合の手順については、下記をご参照ください。

- Bitdefenderアカウントを作成する

1. 該当する欄に必要な情報を入力してください。 入力いただいたデータは機密情報として扱われます。 パスワードは最低 8 文字で、数字を含める必要があります。

2. 続行する前に、使用条件に同意する必要があります。　サブスクリプション契約には、 Bitdefender を使用する上で守っていただく条件が記載されているため、必ずよくお読みください。

   また、プライバシーポリシーにアクセスして参照することもできます。

3. アカウント作成をクリックします。

> **注記**
> アカウントの作成が完了したら、メールアドレスとパスワードを使用して https://central.bitdefender.com または Android/iOS デバイスにインストールされた Bitdefender Central アプリからアカウントにログインできるようになります。 Android で Bitdefender Central アプリをインストールするには、Google Play にアクセスして Bitdefender Central を検索してインストールする必要があります。 iOS で Bitdefender Central アプリをインストールするには、App Store にアクセスして Bitdefender Central を検索してインストールする必要があります。

- 既に Bitdefender アカウントを取得済みの場合

1. サインイン をクリックし、入力欄に Bitdefender アカウントのメールアドレスとパスワードを入力します。

   サインイン をクリックして続行します。

2. アカウントのパスワードを忘れた場合や、設定したパスワードを変更したい場合は、「パスワードのリセット」リンクをクリックします。メールアドレスを入力し、「パスワードを忘れた場合」をクリックします。　メールアカウントを確認し、記載されている手順に従って Bitdefender アカウントに新しいシステムパスワードを設定します。

> **注記**
> MyBitdefender　アカウントをすでにお持ちの場合は、同じ認証情報を使って Bitdefender アカウントにログインできます。 パスワードを忘れた場合は、まず https://my.bitdefender.com にアクセスしてリセットする必要があります。 次に、新しい認証情報を使って Bitdefender アカウントにログインします。

- Microsoft、FacebookまたはGoogleアカウントを利用してログインする

Microsoft、Facebook、Googleアカウントを利用してログインするには

1. 利用するサービスを選択してください。 サービスのログイン画面へリダイレクトされます。

2. 選択したサービスの手順に従ってアカウントをBitdefenderへリンクさせてください。

> **注記**
> Bitdefenderはお客様のアカウントのパスワードや、お友達の連絡先など、機密情報へアクセスすることはできません。

ステップ 5 - 製品をアクティベートする

> **注記**
> このステップは、直前のステップで新規 Bitdefenderアカウントを作成することを選択した場合、またはサブスクリプションの有効期限が切れたアカウントでログインした場合に表示されます。

製品のアクティベーションを完了するにはインターネット接続が必要です。

ご利用状況に応じて以下の手順を進めてください。

- ライセンスキーを持っています。

  この場合、以下の手順で製品をアクティベートします:

  1. アクティベーションコードを持っています フィールドにアクティベーションコードを入力し、続ける をクリックします。

     > **注記**
     > アクティベーションコードの確認方法:
     > - CD/DVDのラベルに記載
     > - 製品登録カード
     > - オンラインストアからのメール

  2. Bitdefenderを体験版として使用する。

     この場合、製品は30日間使用することができます。 トライアルを開始するには、サブスクリプションは持っていないが製品を無料で試用してみたい を選択して 続行 をクリックします。

ステップ 6 - 開始する

始める ウィンドウには、現在アクティブなサブスクリプションの情報が表示されます。

Bitdefender Total Security のインターフェイスにアクセスするには 完了 をクリックします。

2. 開始

2.1. 基本

Bitdefender Total Security をインストールすると、コンピュータはあらゆる種類の脅威 （マルウェア、スパイウェア、ランサムウェア、エクスプロイト、ボットネット、トロイの木馬など） およびインターネットの脅威（ハッカー、フィッシング、スパムなど）から保護されます。

このアプリケーションは、Photon テクノロジーを使用し、脅威のスキャン処理の速度とパフォーマンスを向上します。 この機能は、システムアプリケーションの使用パターンを分析し、最適なスキャン対象およびスキャン日時を設定することで、システムパフォーマンスへの影響を最小限に抑えます。

空港、ショッピングセンター、カフェ、ホテルなどの公衆ワイヤレスネットワークに、適切なセキュリティ保護なしで接続すると、お使いのデバイスやデータに危険が及ぶ恐れがあります。 サイバー犯罪者たちは、このようなユーザーのオンラインアクティビティを監視して、個人情報を盗む出す最高のタイミングを伺っている可能性があります。また、IP アドレスが丸見えになってしまうため、お使いのマシンが第三者によるサイバー犯罪の犠牲になり得る危険が存在します。 このような不幸な状況を回避するには、「VPN」 (p. 144) アプリをインストールして使用することをお勧めします。

パスワードとオンラインアカウントは、ウォレットに 「認証情報をパスワードマネージャーで保護」 (p. 137) で保管して管理することができます。 1 つのマスターパスワードで、お客様からお金を盗もうと試みる侵入者からプライバシーを守ることができます。

「webカメラ保護」 (p. 125)信頼できないアプリがウェブカメラにアクセスしないようにして、ハッキングによる被害を未然に防ぎます。 Bitdefender ユーザーの設定に基づいて、人気アプリによるウェブカメラへのアクセスが許可またはブロックされます。

保護されていないワイヤレスネットワークへの接続時にお客様のデバイスの安全を守るため、 Bitdefender はネットワークのセキュリティレベルを診断し、必要に応じてオンラインアクティビティの安全性を高めるための推奨事項を提案します。 個人データを安全に保護する方法については「WiFiアドバイザー」 (p. 122)を参照してください。

ドキュメント、写真、ムービーなど、ローカルおよびクラウド上に保存された個人データは、昨今の最も危険な脅威からしっかりと守られます。 個

人ファイルをシェルターに退避する方法の詳細については 「Safe Files」 (p. 127) を参照してください。

ランサムウェアで暗号化されたファイルを、要求された身代金を支払うことなく復元できるようになりました。 暗号化されたファイルを復元する方法の詳細については 「ランサムウェア防御」 (p. 130) を参照してください。

Bitdefender は、システムのメンテナンスタスクを遅らせることができるので、仕事やゲーム中、映画を見ている間の動作の邪魔をせず、システムビジュアル効果の調整を行って快適な環境を維持できます。 「プロファイル」 (p. 175) を有効にして設定することで、これらを活用することができます。

セキュリティに関する難しい選択はBitdefenderが行うため、ポップアップなどの警告はほとんど表示されることはありません。 実行されたアクションの詳細と、プログラム操作に関する情報は通知画面で確認できます。 詳細については、「通知」 (p. 14) をご参照ください。

定期的に Bitdefender を開き、問題を修復するようにしてください。 また必要に応じて、Bitdefenderの設定を行ない、コンピュータとデータを守ってください。

Bitdefender Total Security のオンライン機能を利用したり、サブスクリプションおよびデバイスを管理したりするには Bitdefender アカウントにアクセスしてください。 詳細については、「Bitdefender Central」 (p. 31) をご参照ください。

「操作手順」 (p. 42) では、普段よく行うタスクの詳細手順が記載されています。 Bitdefenderのご利用中に問題があった場合は、「一般的な問題を解決する」 (p. 182) をご確認いただき、よくある問題の解決策をご確認ください。

Bitdefenderウィンドウを開く

Bitdefender Total Securityのメイン画面を開くには以下の手順を行なってください：

● Windows 7の場合：

1. Windows スタートボタンをクリックして、すべてのプログラムを選択してください。
2. Bitdefenderをクリックしてください。

3. Bitdefender Total Security をクリックするか、もしくはシステムトレイの Bitdefender アイコンをダブルクリックします。

- Windows 8 および Windows 8.1:

  Windowsスタート画面のBitdefenderを探して、アイコンをクリックしてください。（スタート画面で「 "Bitdefender"」の名前を入力することで直接開くこともできます） あるいはデスクトップアプリを開き、システムトレイの Bitdefender アイコンをダブルクリックします。

- Windows 10の場合 :

  タスクバーの検索ボックスに "Bitdefender" と入力し、アイコンをクリックします。 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します。

Bitdefender画面や、タスクトレイのアイコンに関するより詳しい情報については、「Bitdefender 管理画面」 (p. 18)をご参照ください。

2.1.1. 通知

Bitdefenderは、パソコン上で行なった操作や、各種イベントの詳細ログを作成します。 システムまたはデータのセキュリティに影響を与えるイベントが発生すると、新しいメールが受信箱に届くのと同じように Bitdefender の通知画面に新しいメッセージが追加されます。

通知は Bitdefender の保護を監視・管理するために非常に重要なツールです。 たとえば、アップデートが正しく実行されたか、コンピュータ上で脅威や脆弱性が見つかったかを簡単に確認できます。 また、必要に応じて追加で処理を行ったり、 Bitdefenderが行なった処理を変更することもできます。

通知ログにアクセスするには、Bitdefender インターフェイスのナビゲーションメニューにある 通知 をクリックします。 重大なイベントが発生するたびに、  アイコンにカウンターが表示されます。

通知はその種類と重要度に応じて、以下のグループに分けられます:

- 緊急イベントは、重大な問題があることを表します。 これらはすぐにご確認ください。
- 警告イベントは、重大ではないが確認が必要な問題があることを表します。 お時間があるときに、内容を確認して修復してください。
- 情報のイベントは、正常に実行された操作を示します。

各タブをクリックすると、生成されたイベントの詳細を確認できます。 各イベントのタイトルを一度クリックすると、次のような詳細情報が表示されます: イベントの簡単な説明、イベント発生時に Bitdefender が実行したアクション、および発生した日時。 ※必要に応じて追加の処理を行うことができます。

通知画面には、セクション内のすべてのイベントを削除したり、既読にしたりするためのオプションが用意されており、イベントのログを簡単に管理できます。

2.1.2. プロファイル

オンラインゲームやビデオ再生などの処理には、高速なレスポンスや高い性能がコンピュータに求められます。 お使いのノートPCがバッテリで動作している場合、電力を多く消費する不要な操作は、実行しないようにするのがベストです。

Bitdefender のプロファイルは、一時的に保護設定およびシステム構成を変更し、実行中のアプリケーションに対してより多くのシステムリソースを割り当てます。 その結果、システムに及ぼす影響を最小化します。

Bitdefender には、異なるアクティビティに対応した複数のプロファイルが用意されています:

仕事プロファイル
: 製品およびシステムの設定を識別し、調整することで作業効率を最適化します。

動画プロファイル
: 視覚効果を向上し、動画視聴時に中断が起こるのを回避します。

ゲームプロファイル
: 視覚効果を向上し、ゲームプレイ時に中断が発生するのを回避します。

公共Wi-Fiのプロファイル
: 安全でないワイヤレスネットワークへの接続時に、最適なセキュリティ保護を実現するための製品設定を適用します。

バッテリーモード･プロファイル
: 製品設定を適用し、バックグラウンドのアクティビティを抑制してバッテリー消費を抑えます。

プロファイルの自動アクティベーションを設定する

Bitdefender を設定してプロファイルを自動管理させると、より快適なユーザーエクスペリエンスを体験できます。 この場合、 Bitdefender はユーザーのアクティビティを自動的に検知し、最適な設定をシステムおよび製品に適用します。

Bitdefender によるプロファイルの有効化を許可するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. プロファイル タブを選択します。
3. 対応するスイッチをクリックして、プロファイルを自動的に有効にするをオンにします。

プロファイルを自動的に有効にしたくない場合はスイッチをオフにします。

プロファイルを手動で有効にするには、対応するスイッチをオンにします。一度に 1 つのプロファイルしか手動で有効にできません。

プロファイルの詳細については以下を参照してください:「プロファイル」(p. 175)

2.1.3. Bitdefenderの設定変更をパスワードで保護する

パソコンの管理者権限を持つユーザーが複数いる場合は、Bitdefenderの設定をパスワードで保護することをおすすめします。

Bitdefender 設定に対するパスワード保護を設定するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. 一般 ウィンドウで パスワード保護 をオンにします。
3. つのフィールドにパスワードを入力し、OK をクリックします。 パスワードは最低 8 文字必要です。

一度パスワードを設定したら、 Bitdefender の設定を変更するにはパスワードの入力が必要です。

重要項目

パスワードはメモして、紛失しないように大切に保管してください。 パスワードを忘れてしまった場合は、プログラムを再インストールするか、Bitdefender サポートページをご覧ください。

パスワード保護の削除：

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. 一般 ウィンドウで パスワード保護 をオフにします。
3. パスワードを入力し、 OKをクリックします。

注記
製品のパスワードを変更するには、パスワード変更リンクをクリックします。 現在のパスワードを入力し、OK をクリックします。 表示される新しいウィンドウで、 Bitdefender の設定へのアクセスを制限するために使用したい新しいパスワードを入力します。

2.1.4. 製品レポート

製品レポートには、インストールした Bitdefender 製品の使用方法に関する情報が含まれています。 この情報は製品の改良に重要で、より良い製品を提供するために役立てられます。

なお、これらのレポートにはお客様の個人データ （お名前や IP アドレスなど） は一切含まれておりませんので、これらのデータが商業目的に利用されることもありません。

インストール時に Bitdefender サーバーにレポートを送信するように設定したが、レポートの送信を止めたい場合:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. 詳細設定 タブを選択します。
3. 製品レポート をオフにします。

2.1.5. 特別キャンペーン通知

特別キャンペーンが実施されると、 Bitdefender 製品はポップアップウィンドウでその詳細を表示します。 よりお得な価格で、デバイスをより長期間保護できるチャンスをご提供します。

特別キャンペーンおよの通知をオン/オフにするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. 一般 ウィンドウで、対応するスイッチをオン/オフにします。

デフォルトでは、特別キャンペーンおよび製品に関するお知らせオプションは有効になっています。

2.1.6. アンチマルウェアスキャンインタフェース

Bitdefender は Microsoft アンチマルウェアスキャン インターフェイス (AMSI) を搭載しており、動的スクリプトベースのマルウェアや、未知のサイバー攻撃などからもシステムをしっかりと保護します。 AMSI は、アプリケーションやサービスを Bitdefender 製品と統合することを可能にする汎用インターフェイスです。

アンチマルウェアスキャンのインターフェースとの統合をオン/オフにするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. 一般 ウィンドウで、対応するスイッチをオン/オフにします。

Microsoft アンチマルウェアスキャン インターフェイス (AMSI) のオプションはデフォルトで有効になっており、Windows 10 でのみ利用できます。

2.2. Bitdefender 管理画面

Bitdefender Total Securityはパソコン初心者の方にも、パソコン熟練者の方にも、あらゆるレベルのユーザーのご要望へお応えします。 また、製品の画面や各ユーザー管理画面は、あらゆるユーザーの要望に適合するようデザインされています。

Bitdefender のインターフェイスの使い方や各種設定方法を学ぶには、左上部に表示されている製品紹介ウィザードを活用してください。 チュートリアルを続ける場合は右山括弧を選択し、ウィザードを閉じるには ツアーをスキップ を選択します。

Bitdefender のシステムトレイアイコンにはいつでもアクセスでき、メインウィンドウを開いたり、製品アップデートを実行したり、バージョンを確認したりといった作業をすばやく行えます。

メイン画面には、現在のセキュリティの状態に関する情報が表示されます。デバイスの使用状況やニーズに基づき、自動操作機能はデバイスのセキュリティとパフォーマンスを改善するためのさまざまな推奨事項を表示します。 さらに、最も頻繁に使用するクイックアクションを追加することで、必要な機能にいつでもすばやくアクセスできます。

左のナビゲーションメニューから Bitdefender アカウント、設定エリア、通知設定、および詳細な設定や管理タスクを実行するための Bitdefender の各セクション にアクセスできます。 また、ご質問がおありの場合や、画面に予期しない内容が表示された場合などは弊社サポートまでご連絡いただくこともできます。

重要なセキュリティ情報を常に監視し、各種設定へ簡単にアクセスしたい場合はウィジェットをデスクトップ上に表示するようにしてください。

2.2.1. タスクトレイアイコン

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

注記
Bitdefender アイコンは非表示になっている場合があります。 アイコンを常に表示するには:

- Windows 7、Windows 8、および Windows 8.1:
  1. 画面の右下に表示される矢印 をクリックしてください。
  2. カスタマイズ...をクリックして、通知領域アイコンのウィンドウを開いてください。
  3. Bitdefenderエージェントの隣のプルダウンメニューからアイコンと通知を表示を選択してください。
- Windows 10の場合 :
  1. タスクバーを右クリックし、プロパティ を選択します。
  2. 「タスクバー」ウィンドウの カスタマイズ をクリックします。
  3. 通知・アクション ウィンドウで、タスク バーに表示するアイコンを選択する リンクをクリックします。
  4. Bitdefender エージェント の横にあるスイッチを有効にします。

アイコンをダブルクリックすると、Bitdefenderのメイン画面が表示されます。 また、アイコンを右クリックすると、コンテキストメニューを使用して Bitdefender製品を素早く管理できます。

タスクトレイアイコン

- パネル表示 - Bitdefenderのメイン画面を開きます。
- この製品について - Bitdefender 製品に関する情報、問題が発生した際の連絡先情報、サブスクリプション契約の内容、サードパーティコンポーネント、およびプライバシーポリシーが記載された画面が開きます。
- ウィジェットを表示 / 非表示 - ウィジェットの有効 / 無効を切り替えます。
- 今すぐアップデート - すぐにアップデートを開始します。 アップデートの状態は、Bitdefender メインウィンドウ のアップデートパネルで確認できます。

Bitdefenderのタスクトレイアイコンは、パソコンに問題がある場合、以下のように表わします：

システムのセキュリティに影響を及ぼしている問題はありません。
システムのセキュリティに影響を与える重大な問題が発生しています。即時対応と修復が必要です。

Bitdefenderが正常に動作していない場合、タスクトレイのアイコンはグレーで表示されます：これは通常、サブスクリプションの有効期限が切れた際に発生します。 また、Bitdefenderのサービスが応答しない場合や、その他エラーがBitdefenderの通常動作に影響を及ぼしている場合に表示されます。

2.2.2. ナビゲーションメニュー

Bitdefender インターフェイスの左側にはナビゲーションメニューがあり、Bitdefender の各種機能やツールにすばやくアクセスできるようになっています。 このエリアで利用できるタブは以下の通りです：

- ダッシュボード。 ここから、セキュリティの問題をすばやく修正したり、システムのニーズや使用パターンなどに基づく推奨事項を確認したり、クイックアクションを実行したり、他のデバイスに Bitdefender をインストールしたりできます。
- 保護。 ここから、アンチウイルススキャンを実行したり、ファイアウォールの設定にアクセスしたり、ファイルやアプリをランサムウェアの攻撃から防御したり、ランサムウェアによって暗号化されたデータを復旧したり、ブラウジング時の保護を設定したりできます。

- プライバシー。 ここでは、オンラインアカウント用にパスワード管理ウォレットを作成したり、ウェブカメラへの不正なアクセスを防止したり、安全に保護された環境でオンラインバンキングを行ったり、VPN アプリを利用したり、お子様のオンラインアクティビティの監視と制限を行ったりできます。
- ユーティリティ。 ここでは、システム速度を向上させたり、各デバイスの盗難対策機能を設定したりできます。
- 通知。 ここから、生成された通知にアクセスできます。
- マイアカウント. ここから Bitdefender アカウントにアクセスし、サブスクリプションを確認したり、管理しているデバイスに対してセキュリティタスクを実行したりできます。 Bitdefender アカウントおよびサブスクリプションの詳細も確認できます。
- 設定。 ここから一般設定にアクセスできます。
- サポート。 Bitdefender Total Security で発生した問題の解決にヘルプが必要な際には、ここから Bitdefender のテクニカルサポートに連絡することができます。 ▪

2.2.3. ダッシュボード

ダッシュボード ウィンドウでは、共通のタスクを実行、セキュリティの問題をすばやく修復、製品の動作に関する情報を確認、製品の設定を変更できるパネルにアクセスなどを行うことができます。

すべての操作を、わずか数クリックで行うことができます。

このモードの画面は、以下の主要なセクションで構成されています：

セキュリティの状態エリア
: ここで、コンピュータのセキュリティ状態を確認できます。

Autopilot
: ここで自動操作機能による推奨事項を確認し、システムの動作を最適化することができます。

クイックアクション
: ここからシステムを保護して最適な動作を維持するための様々なタスクを実行したりできます。 ここから、 Bitdefender 製品を他のデバイスにも簡単にインストールすることもできます（サブスクリプションにスロットが残っていることが条件です）。

セキュリティの状態エリア

Bitdefender はトラッキングシステムを利用して、パソコンのセキュリティに影響を及ぼす可能性のある問題を検出し、報告します。 検出される問題は、パソコンの保護に必要な重要機能が無効になっているなど、重大なセキュリティリスクが存在する場合などです。

コンピュータの安全を脅かす恐れのある問題が発生すると、 Bitdefender インターフェイスの上部にあるステータス表示が赤に変わります。 表示されるステータスは、システムに影響を与えている問題のタイプを示しています。 また、システムトレイのアイコンが に変わり、アイコン上にマウス カーソルを移動すると、未解決の問題が記載されたポップアップ画面が表示されます。

検出された問題によって Bitdefender がシステムを脅威から保護できなくなったり、その他のセキュリティリスクが生じる可能性があるため、問題はできるだけ迅速に解決することをお勧めします。 問題を修正するには、検出された問題の横にあるボタンをクリックします。

Autopilot

Bitdefender 自動操作機能は、色々な作業やアクティビティをより効率的かつ安全に行うための、パーソナルセキュリティアドバイザーとして役立ちます。 Bitdefender の自動操作は、仕事、オンラインバンキング、映画鑑賞、ゲームなど、デバイス上で実行しているアクティビティの種類に応じて、各種設定を最適化します。 提案される推奨事項は、お使いの製品を最適な状態でお使いいただくために必要なアクションに関するものである場合もあります。

推奨された機能を起動したり、製品性能を向上するには、それぞれ該当するボタンをクリックします。

自動操作の通知をオフにする

自動操作機能による推奨事項を通知するため、 Bitdefender 製品はポップアップウィンドウで通知を表示するように設定されています。

自動操作の通知をオフにするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. 一般 ウィンドウで 推奨事項の通知 をオフにします。

クイックアクション

クイックアクションを活用することで、システムを保護したり、システム速度を最適化するために役立つ思うタスクをすばやく簡単に実行できます。

Bitdefender にはデフォルトでいくつかのクイックアクションが設定されていますが、これらは各ユーザーが使いやすいように入れ替えることができます。 クイックアクションを変更するには:

1. 削除したいカードの右上隅にある「＋」アイコンをクリックします。
2. メインインターフェイスに追加したいタスクを選び、追加 をクリックします。

メインインターフェイスに追加できるタスクは以下の通りです:

- クイック検査. クイックスキャンを実行すると、コンピュータ上に脅威が存在しないかどうかすばやくチェックできます。
- システムスキャン。 パソコン全体の検査を実行することで、コンピュータ上に脅威が存在していないかどうかを確認できます。
- 脆弱性検査. コンピュータの脆弱性をスキャンし、オペレーティングシステムおよびすべてのインストール済みアプリケーションが最新の状態で、正しく動作しているかをチェックします。
- Wi-Fi の安全性をチェック。 Wi-Fi セキュリティアドバイザーを開いて、接続しているワイヤレスホームネットワークが安全かどうか、および脆弱性があるかどうかをチェックします。
- パスワード管理。 パスワード管理を表示・管理します。
- 決済ブラウザを起動. Bitdefender Safepay™を開くことで、オンラインバンキングなどの際に重要なデータを保護できます。
- 決済ブラウザを開くを開く. Bitdefender VPN を開いて、インターネット接続時にセキュリティ保護をさらに強化できます。
- ファイル シュレッダー. ファイルシュレッダーを起動して、デバイス上のすべてのプライバシーデータの痕跡を削除します。
- ファイル金庫. 重要な個人データや文書を安全に保管するためのファイル金庫を作成します。
- ワンクリック最適化ツールを開く. シングルクリック操作のみで、ディスクの空き容量を増やしたり、レジストリエラーを修復したり、不要なファイルをすべて削除してプライバシーを保護したりできます。
- スタートアップ最適化ツールを開く. 起動時に不要なアプリが起動しないようにすることで、システムの起動時間を短縮できます。
- デバイスをクリーンアップ. 不要なファイルを削除して、新しいデータのためのスペースを確保します。

Bitdefender で追加のデバイスの保護を開始するには:

1. 「別のデバイスにインストールする」 のリンクをクリックします。

   Bitdefender アカウントの Web ページにリダイレクトされます。 ご自身の認証情報を使ってログインしていることを確認してください。

2. 表示されるウィンドウで、ダウンロードリンクを送信をクリックします。

3. 当該フィールドにメールアドレスを入力してメールを送信 をクリックします。 ダウンロードリンクは、以後 24 時間のみ有効です。 リンクの有効期限が切れた場合は、同じ手順を実行して新しいリンクを生成する必要があります。

   Bitdefender をインストールしたいデバイス上で、登録したメールアドレスの受信トレイを開き、届いたメールに記載されているダウンロードボタンを押してください。

選択内容に応じて、以下の Bitdefender 製品がインストールされます:

- Windows ベースのデバイス上の Bitdefender Total Security。
- macOS デバイス上の Bitdefender Antivirus for Mac。
- Android ベースのデバイス上の Bitdefender Mobile Security。
- iOS ベースのデバイス上の Bitdefender Mobile Security。
- macOS、iOS、Android ベースのデバイス上の Bitdefender ペアレンタルコントロール。

2.2.4. Bitdefender セクション

Bitdefender 製品には、仕事やネットサーフィン、ゲーム、オンラインショッピング中にしっかりとシステムを保護したり、システム速度を向上したりしてくれる便利な機能群が 3 つのセクションに分かれて提供されています。

特定のセクションにある機能にアクセスしたい場合や、製品の設定を開始したい場合は、Bitdefender インターフェース のナビゲーションメニューにある以下のアイコンに使用します:

- 保護
- プライバシー
- ユーティリティ

保護

保護セクションでは、高度なセキュリティ設定を構成したり、友達やスパマーを管理したり、接続設定を表示・編集したり、セーフファイルおよびオンライン脅威対策機能をセットアップしたり、システムの脆弱性を確認・修正したり、接続しているワイヤレスネットワークの安全性をチェックしたりできます。

保護セクションで管理できる機能は以下の通りです:

ウイルス対策
ウイルス対策は、パソコンのセキュリティの基本です。 Bitdefenderは、パソコンをマルウェアやトロイの木馬、スパイウェア、アドウェアなど、あらゆる脅威から脅威自動検知・手動スキャンを使って保護します。

アンチウイルス機能からは、以下のスキャンタスクに簡単にアクセスできます:
- クイックスキャン
- パソコン全体の検査
- 検査タスクを管理
- レスキューモード (Windows 10 のレスキュー環境)

検査タスクに関するより詳しい情報や、ウイルス対策の設定方法については「ウイルス対策」 (p. 80)を参照してください。

オンライン脅威対策
オンライン脅威対策機能は、ブラウジング時におけるフィッシング攻撃、詐欺サイト、個人データの漏洩などのオンライン脅威に対する保護を提供します。

Bitdefender でオンラインアクティビティを保護するための設定方法については 「オンライン脅威対策」 (p. 102) を参照してください。

ファイアウォール
ファイアウォールはパソコンがネットワークに接続している間にすべての通信を監視し、パソコンを守ります。

ファイアウォールの設定に関する詳しい情報は、「ファイアウォール」 (p. 112)をご参照ください。

世界最高レベルの防御
アクティブ脅威防御は、インストールされているすべてのアプリケーションの動作を分析することで、ランサムウェア、スパイウェア、トロ

イの木馬などの脅威からシステムをアクティブに保護します。 不審なプロセスが特定され、必要に応じてブロックされます。

システムを脅威から保護する方法の詳細については 「高度な防御」（p. 100）を参照してください。

迷惑メール対策

Bitdefender の迷惑メール対策機能は、POP3 のメールトラフィックをフィルタリングすることで、受信トレイに不要なスパムメールが届かないようにします。

アンチスパム保護の詳細については 「迷惑メール対策」（p. 104）を参照してください。

脆弱性

脆弱性診断機能は、オペレーティングシステムおよびよく使用するアプリケーションを最新の状態に保ち、また、安全でないネットワーク接続を検出する役割を持ちます。

「脆弱性診断」配下の 脆弱性スキャン をクリックすると、Windows や各アプリケーションの重要なアップデートを確認したり、パスワードが脆弱な Windows アカウントを検出したり、安全でないワイヤレスネットワークを検出したりできます。

Wi-Fi セキュリティアドバイザー をクリックすると、通常接続するワイヤレスネットワークの一覧が、セキュリティ評価とともに表示され、ネットワークを脅威から保護するための対策を確認できます。

脆弱性保護の設定については 「脆弱性」（p. 118）を参照してください。

安全なファイル

セーフファイル機能は、お客様の重要なドキュメントやその他のファイルをランサムウェアによる脅威から守ります。

個人ファイルをランサムウェアの攻撃から守るためのセーフファイル機能を設定する方法の詳細については、「Safe Files」（p. 127）を参照してください。

ランサムウェア修復

ランサムウェア修復機能は、ファイルがランサムウェアによって暗号化された場合に、ファイルを復元して取り戻すことができます。

暗号化されたファイルを復元する方法の詳細については 「ランサムウェア防御」（p. 130）を参照してください。

プライバシー

「プライバシー」セクションでは、 Bitdefender VNP アプリを開いて個人データの暗号化、オンライン決済処理の保護、Web カメラの保護、セキュアなブラウジング、およびお子様のオンラインアクティビティのモニタリングや制限などを行えます。

プライバシーセクションで管理できる機能は以下の通りです:

VPN
: VPN を使用すると、空港、ショッピングセンター、カフェ、ホテルなどの安全でないワイヤレスネットワークに接続する際に、IP アドレスを隠して個人データを安全に保護できます。 さらに、通常は特定の地域でしかアクセスできないコンテンツも楽しむことができます。

  この機能の詳細については 「VPN」 (p. 144) を参照してください。

ファイル暗号化
: 暗号化とパスワードによって保護された論理ドライブ（金庫）を作成し、機密な情報や重要な文書を安全に保管します。

  暗号化およびパスワード保護した論理ドライブ（金庫）の作成方法については「ファイル暗号化」 (p. 132)をご参照ください。

ウェブカメラ保護
: Bitdefender のウェブカメラ保護は、信頼できないアプリケーションからのアクセスをブロックすることで、ウェブカメラを危険から守ります。

  ウェブカメラを不正なアクセスから保護する方法の詳細については「webカメラ保護」 (p. 125) を参照してください。

パスワード管理
: Bitdefender のパスワードマネージャーではパスワードの管理、プライバシーの保護、安全なウェブ閲覧などが可能です。

  パスワードマネージャーの設定の詳細については 「認証情報をパスワードマネージャーで保護」 (p. 137) を参照してください。

決済ブラウザ
: Bitdefender Safepay™ ブラウザを使うと、オンラインバンキングやショッピング、およびその他のオンライン決済を安全に利用できます。

  Bitdefender Safepay™ の詳細については 「安全なオンライン決済 : Safepay」 (p. 147) を参照してください。

ペアレンタルコントロール
Bitdefender のペアレンタルコントロールでは、お子様がコンピュータ上で何をしているかを監視することができます。 不適切コンテンツがあった場合には、インターネットまたは特定のアプリケーションへのアクセスを制限することができます。

「ペアレンタルコントロール」パネルの 設定 をクリックすると、お子様のデバイスの設定を行ったり、いつでも好きな場所からお子様のオンラインアクティビティを監視したりできます。

ペアレンタルコントロールの設定の詳細については 「お子様保護」(p. 153) を参照してください。

データ保護
データ保護機能では、ファイルを永久的に消去することができます。「データ保護」ウィンドウの ファイルシュレッダー をクリックすると、ファイルをシステムから完全に削除するためのウィザードが開始します。

データ保護の設定については 「データ保護」(p. 152) を参照してください。

ユーティリティ

ユーティリティのセクションで、システムの速度向上やデバイスの管理を行うことができます。

最適化ツール
Bitdefender Total Securityはセキュリティ対策だけではなく、パソコンのパフォーマンスを向上させる機能も搭載しています。

利用可能な最適化ツールは以下の通りです:
- クイック最適化ツール
- スタートアップ最適化ツール
- ディスク・クリーンアップ

チューンアップのツールに関する詳細については、「ユーティリティ」(p. 171)をご参照ください。

盗難対策
Bitdefender の窃盗防止機能は、コンピュータおよびコンピュータ上のデータを窃盗や喪失から保護します。 このような場合に、リモートからコンピュータの位置情報を確認したり、ロックしたりできます。 また、システム内のデータをすべてワイプ（消去）することもできます。

Bitdefender の窃盗防止機能には以下の特長があります:

- リモート探知
- リモートロック
- リモートワイプ
- リモートアラート

システムの安全を保護する方法の詳細については 「デバイス盗難対策」(p. 167) を参照してください。

2.2.5. ウィジェット

ウィジェットは、 Bitdefender Total Security を素早くかつ簡単に管理するためのツールです。 このウィジェットをデスクトップへ追加すれば、重要なセキュリティ情報や、セキュリティタスクをいつでも確認することができます:

- Bitdefender のメインウィンドウを開きます。
- リアルタイムでスキャンアクティビティを監視します。
- システムのセキュリティ状況を監視し、問題を修復します。
- アップデートの進行状況を表示します。
- 通知を表示し、 Bitdefender が報告した最新のイベントを確認します。
- ウィジェットへファイルやフォルダをドラッグ＆ドロップすることで、単体または複数のものを同時にウイルス検査することができます。

ウィジェット

ウィジェットの中央に、パソコンの総合セキュリティ状況が表示されます。このエリアに表示されるアイコンと色で状況を確認することができます。


重大な問題がシステムのセキュリティに影響を及ぼしています。

直ちに確認し、できるだけ早く対処する必要があります。 問題を修復するには、ステータスアイコンをクリックします。

 軽度の問題があります。 お時間があるときに、内容を確認して修復してください。 問題を修復するには、ステータスアイコンをクリックします。

 お使いのシステムは保護されています。

 手動検査が実行中の場合、このアニメーションアイコンが表示されます。

問題が報告された場合は、ステータスアイコンをクリックし、修復ウィザードを起動してください。

ウィジェットの 下側 には、未読イベントのカウンタ（Bitdefender が報告した未読のイベント数）が表示されます。 イベントカウンター（たとえば未読イベントが1件の場合は 1 ）をクリックすると「通知」ウィンドウが開きます。 詳しくは 「通知」（p. 14）を参照してください。

ファイルとフォルダの検査

ウィジェットを使ってファイルやフォルダを素早くウイルス検査することができます。 検査したいファイルやフォルダをウィジェット上にドラッグ＆ドロップしてください。

ウイルス対策 スキャン ウィザード で、スキャン手順についての案内が表示されます。 検査オプションは最適なウイルス検査を行うように設定されており、設定内容を変更することはできません。 ウイルスに感染したファイルが検出された場合、 Bitdefender はファイルの駆除（悪意のあるコードの除去）を試みます。 駆除できない場合は、ウイルス検査ウィザードがその他に可能な操作を表示します。

ウィジェットを表示する/非表示にする

ウィジェットを非表示にしたい場合は、✕をクリックしてください。

ウィジェットを再表示するには、以下の何れかの手順を行なってください：

- タスクトレイから：
  1. タスクトレイメニュー内のBitdefenderアイコンを右クリックしてください。
  2. 右クリックメニュー内のウィジェットを表示を選択します。
- Bitdefenderの製品画面から：

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. 一般 ウィンドウで セキュリティウィジェット をオンにします。

Bitdefender のセキュリティウィジェットは、デフォルトでは無効になっています。

2.3. Bitdefender Central

Bitdefender Central は、製品のオンライン機能およびサービスにアクセスしたり、 Bitdefender がインストールされているデバイス上でリモートタスクを実行したりできるプラットフォームです。 https://central.bitdefender.com にアクセスすることで、インターネットに接続されているあらゆるコンピュータまたはモバイルデバイスから Bitdefender アカウントにログインできます。Android または iOS デバイスに Bitdefender Central アプリをインストールして直接アカウントにアクセスすることも可能です。

お使いのスマートフォンに Bitdefender Central アプリをインストールするには:

- Android デバイス - Google Play で Bitdefender Central アプリを検索し、ダウンロードしてインストールします。 必要なステップを実行して、インストールを完了してください。
- iOS デバイス - App Store で Bitdefender Central アプリを検索し、ダウンロードしてインストールします。 必要なステップを実行して、インストールを完了してください。

ログインすると、以下の操作が可能になります:

- Bitdefender を Windows、macOS、iOS、および Android オペレーティングシステムにダウンロードしてインストールします。 ダウンロードできる製品は以下の通りです:
  - Bitdefender Total Security
  - Bitdefender Antivirus for Mac
  - Bitdefender Mobile Security for Android
  - Bitdefender Mobile Security for iOS
  - Bitdefender ペアレンタル コントロール
- Bitdefender のサブスクリプションを管理・更新します。

- ネットワークに新しいデバイスを追加して、いつでもどこでも管理できます。
- 盗難防止 機能を使って、ネットワーク機器やデータを窃盗や損失から保護できます。
- ペアレンタルコントロール を設定することで、お子様のデバイスの設定を行ったり、いつでも好きな場所でお子様のオンラインアクティビティを監視したりできます。

Bitdefender Centralにアクセス

Bitdefender Central にアクセスする方法はいくつか用意されています:

- Bitdefender のメイン管理画面から:
  1. Bitdefender インターフェイスのナビゲーションメニューにある マイアカウント をクリックします。
  2. Bitdefender Central を開く をクリックします。
  3. メールアドレスとパスワードを使って Bitdefender アカウントにログインします。
- ウェブブラウザから:
  1. インターネットに接続しているデバイスで、ウェブブラウザを起動します。
  2. 次のサイトへアクセスします : https://central.bitdefender.com
  3. メールアドレスとパスワードを使って Bitdefender アカウントにログインします。
- お使いの Android または iOS デバイスから:

  インストールした Bitdefender Central アプリを開きます。

注記
この資料では、Web インターフェイス上で見つけることのできるオプションと指示が提供されています。

2.3.1. サブスクリプション

Bitdefender Central 管理画面では、すべてのデバイスのサブスクリプションを簡単に管理することができます。

利用可能なサブスクリプションの確認

利用可能なサブスクリプションを確認するには:

1. Bitdefender Centralにアクセスします。
2. マイ サブスクリプション パネルを選択します。

ここでは、所有しているサブスクリプションの状態と、サブスクリプションを使用しているデバイス数を確認できます。

サブスクリプションカードを選択すると、サブスクリプションに新しいデバイスを追加したり、サブスクリプションを更新することができます。

注記
異なるプラットフォーム (Windows、macOS、iOS、Android) であれば、アカウントに複数のサブスクリプションを登録することが可能です。

新しいデバイスを追加する

サブスクリプションが複数のデバイスをカバーしている場合は、以下の手順で新しいデバイスを追加し、 Bitdefender Total Security をインストールできます:

1. Bitdefender Centralにアクセスします。
2. マイデバイス パネルを選択し、保護をインストール をクリックします。
3. 以下のいずれかのオプションを選択します:
   - このデバイスを保護

     このオプションを選択するとインストールファイルを保存できます。
   - 他のデバイスを保護

     このオプションを選択してから、ダウンロードリンクを送信 をクリックします。 当該フィールドにメールアドレスを入力してメールを送信をクリックします。 ダウンロードリンクは、以後 24 時間のみ有効です。 リンクの有効期限が切れた場合は、同じ手順を実行して新しいリンクを生成する必要があります。

     Bitdefender 製品をインストールしたいデバイス上で、登録したメールアドレスの受信トレイを開き、届いたメールに記載されているダウンロードボタンをクリックしてください。
4. ダウンロードが完了するまでお待ちください。ダウンロードが完了したら、インストーラーを実行します。

サブスクリプションの更新

Bitdefender のサブスクリプションの自動更新を有効にしていない場合は、以下の手順に従って手動で更新することができます:

1. Bitdefender Centralにアクセスします。
2. マイ サブスクリプション パネルを選択します。
3. 該当のサブスクリプション カードを選択します。
4. 更新 をクリックして続行します。

Bitdefender のサブスクリプションを更新するためのページが開きます。

サブスクリプションの有効化

サブスクリプションは、 Bitdefender アカウントを使ってインストール中に有効化できます。 有効化手順が完了すると、有効期限のカウントダウンが開始します。

アクティベーションコードを販売店から購入した場合やプレゼントとして入手した場合は、その内容をアカウント内の Bitdefender のサブスクリプションに追加することが可能です （同一製品のアクティベーションコードでなければなりません)。

アクティベーション コードを使ってサブスクリプションを有効化するには:

1. Bitdefender Centralにアクセスします。
2. マイ サブスクリプション パネルを選択します。
3. アクティベーション コード ボタンをクリックし、該当の入力欄にコードを入力します。
4. 続行するにはACTIVATEにクリックします。

サブスクリプションが有効になりました。 マイデバイス パネルに移動し、保護をインストール を選択してお使いのいずれかのデバイスに製品をインストールしてください。

2.3.2. マイ・デバイス

Bitdefender Central の マイデバイス エリアでは、管理しているデバイスにインストールされている Bitdefender 製品のインストール、管理、リモート操作などが可能です （デバイスの電源が入っていて、インターネットに接続されている必要があります)。 デバイスカードには、デバイス名、

保護状態、および保護状態に影響があるセキュリティリスク （存在する場合）が表示されます。

ステータスまたはユーザー順にソートされたデバイスのリストを表示するには、画面の右上隅にあるドロップダウン矢印をクリックします。

デバイスを簡単に識別できるように、デバイス名をカスタマイズすることが可能です:

1. Bitdefender Centralにアクセスします。
2. マイデバイス パネルを選択します。
3. 任意のデバイスカードをクリックし、ウィンドウの右上隅にある アイコンをクリックします。
4. 設定を選択します
5. デバイス名フィールドに新しい名前を入力して 保存 をクリックします。

各デバイスに所有者を作成して割り当てることで、より効率的な管理が可能です。

1. Bitdefender Centralにアクセスします。
2. マイデバイス パネルを選択します。
3. 任意のデバイスカードをクリックし、ウィンドウの右上隅にある アイコンをクリックします。
4. プロファイルを選択します。
5. オーナーを追加 をクリックし、該当するフィールドに入力します。 プロフィールをカスタマイズするには、写真を追加し、生年月日を設定します。
6. プロファイルを保存するには 追加 をクリックします。
7. デバイスの所有者 リストから任意の所有者を選択し、割り当て をクリックします。

Windows デバイス上の Bitdefender をリモートからアップデートするには:

1. Bitdefender Centralにアクセスします。
2. マイデバイス パネルを選択します。
3. 任意のデバイスカードをクリックし、ウィンドウの右上隅にある アイコンをクリックします。

4. アップデートを選択します。

特定のデバイス上の Bitdefender に対してリモート操作を行ったり情報を確認したりするには、該当するデバイスカードをクリックします。

デバイスカードをクリックすると、以下のタブが利用可能になります:

- ダッシュボード. このウィンドウでは、選択したデバイスの詳細を表示したり、保護状態をチェックしたり、 Bitdefender VPNのステータスや過去7日間にブロックされた脅威の件数を確認したりできます。 保護ステータスは、製品に問題がないときには緑、対処が必要な問題があるときには黄色、デバイスが危険に晒されているときには赤で表示されます。製品に影響する問題が発生している場合は、上部のステータスエリアにあるドロップダウンの矢印をクリックして詳細を確認します。 ここで、お使いのデバイスのセキュリティに影響を与えている問題を手動で修正することができます。
- 保護. このウィンドウでは、デバイスに対してクイックスキャンまたはシステムスキャンをリモートから実行できます。 スキャン ボタンをクリックして処理を開始します。 また、デバイス上で前回スキャンが実行された日時を確認したり、重要な情報を含む最新スキャンのレポートを確認したりできます。これら 2 つのスキャン処理の詳細については 「パソコン全体の検査を実行する」 (p. 87) および 「クイック検査を実行する」 (p. 86) を参照してください。
- オプティマイザ。 ここでは、リモートデバイス上の不要なファイルをすばやくスキャンし、クリーンアップすることができます。 開始 ボタンをクリックし、最適化したいエリアを選択します。 開始 ボタンをもう一度クリックして最適化処理を開始します。 ▪詳細表示 をクリックすると、修正済み問題に関するレポートにアクセスできます。▪

  さらに、システムリソースの消費が大きいアプリケーションを特定することで、デバイスの起動を高速化できます。 詳細表示 をクリックし、検出されたアプリにどう対処したいかを選択します。 これらの機能の詳細については 「シングルクリックでシステムの速度を最適化」 (p. 171) および 「PC の起動時間を最適化する」 (p. 172) を参照してください。
- 盗難対策. デバイスの紛失および盗難時には、盗難防止機能を使ってデバイスの位置情報を確認し、リモートから操作することができます。 デバイスの位置情報を確認するには、位置確認 をクリックします。 最後に把握されていた位置が、日付・時間とともに表示されます。 この機能についての詳細は、 「デバイス盗難対策」 (p. 167)を参照してください。

- 脆弱性. デバイスに未適用の Windows アップデート、古いバージョンのアプリケーション、脆弱なパスワードなどの脆弱性がないか確認するには、「脆弱性」タブの スキャン ボタンをクリックします。 脆弱性はリモートからは修復できません。 脆弱性が見つかった場合は、デバイス上で新たなスキャンを実行し、推奨されるアクションを取る必要があります。 詳細表示 をクリックすると、見つかった問題に関するレポートにアクセスできます。 この機能についての詳細は、 「脆弱性」 (p. 118) を参照してください。

2.3.3. マイアカウント

マイアカウント エリアでは、プロファイルを編集したり、アカウントのパスワードを変更したり、ログオンセッションや Bitdefender Central のヘルプメッセージを管理したりできます。

ウィンドウの右上隅にある アイコンをクリックして マイアカウント を選択すると、以下のタブが表示されます:

- プロファイル - ここでアカウント情報を追加および編集できます。
- パスワードの変更 - ここでは、アカウントに関連付けられたパスワードを変更することができます。
- セッション管理 - アカウントに関連付けされているデバイス上で実行されている最新のアクティブおよび非アクティブなログインセッションを表示・管理できます。
- 設定 - ここでは、 Bitdefender Central のヘルプメッセージをオン/オフにしたり、Android デバイス上でスナップフォトが撮影された際に通知を受け取るかどうかを指定したりできます。

2.3.4. 通知

アカウントに関連付けされているデバイス上のアクティビティを常に把握できるように、 アイコンが用意されています。 クリックすると、デバイス上にインストールされている Bitdefender 製品のアクティビティに関する視覚的データが表示されます。

2.4. Bitdefender を最新の状態に保つ

新しい脅威を日々発見し、対応しています。 このため、 Bitdefender をアップデートして、脅威情報データベースを常に最新の状態に保つことが大切です。

ブロードバンド接続やDSLでインターネットに接続している場合はBitdefender が自動で更新を行ないます。 初期の設定でアップデートの確認は、パソコン起動時と起動後の毎1時間ごとに確認するように設定されています。 アップデートが検出されると、パソコンへ自動的にダウンロードされ、インストールが実行されます。

アップデートの実行中、更新が必要なファイルは順次更新されていきます。これにより、アップデート処理は製品の動作に影響を与えず、また脆弱性も除外されます。

重要項目
最新の脅威からパソコンを保護するには、自動アップデート機能を常に有効にしておいてください。

Bitdefenderの保護を最新の状態に保つために、ユーザー操作が必要な場合があります：

- お使いのパソコンがプロキシ経由でインターネットへ接続している場合、「プロキシを使用してインターネットへ接続するようにBitdefenderを設定するにはどうすれば良いのですか？」 (p. 74)の説明の通りにプロキシを設定する必要があります。
- ダイアルアップ接続でインターネットを利用している場合は、手動でBitdefenderのアップデートを定期的に行うことをおすすめします。 詳細については、「アップデートを実行」 (p. 38)をご参照ください。

2.4.1. Bitdefenderが最新の状態か確認しています

Bitdefender の前回のアップデート日時を確認するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 通知 をクリックします。
2. 全て タブで、最新のアップデートに関する通知を選択します。

アップデートが実施された日時や、その他の詳細情報（インストールが無事完了したか、インストールに失敗したか、あるいはインストールを完了させるために再起動が必要かなど）を確認することができます。 必要な場合は、可能なタイミングでパソコンを再起動させます。

2.4.2. アップデートを実行

アップデートを行うには、インターネット接続が必要です。

アップデートを開始するには、システムトレイにある Bitdefender アイコンを右クリックし 今すぐアップデート を選択します。

アップデート機能は Bitdefender の更新サーバーに接続し、アップデートが利用可能かを確認します。 新しいアップデートがあった場合、アップデート設定で選択されているオプションによって、アップデートは自動で行なわれるか、またはダウンロードの確認を促します。

重要項目
アップデート完了後、パソコンの再起動が必要になる場合があります。 なるべく早く再起動を行うことをおすすめいたします。

デバイスをリモートからアップデートすることも可能ですが、リモートデバイスの電源がオンになっており、インターネットに接続されている必要があります。

Windows デバイス上の Bitdefender をリモートからアップデートするには:

1. Bitdefender Centralにアクセスします。
2. マイデバイス パネルを選択します。
3. 任意のデバイスカードをクリックし、ウィンドウの右上隅にある アイコンをクリックします。
4. アップデートを選択します。

2.4.3. 自動アップデートを有効または無効にする

自動更新をオン/オフにするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. ▪ 更新 タブを選択します。 ▪
3. 対応するスイッチをオン/オフにします。
4. 警告ウィンドウが表示されます。 確認画面のプルダウンメニューから、自動アップデートを無効にする時間を選択し、OKを押して変更を実行します。 自動更新は 5 分、15分、30 分、1 時間、無制限、あるいはシステムの次回再起動まで無効にできます。

警告
これは緊急レベルのセキュリティ問題です。 自動アップデートを無効にする場合は、期間をなるべく短くすることをおすすめします。 Bitdefenderを定

期的にアップデートしないと、最新の脅威などからパソコンを守れなくなってしまい大変危険です。

2.4.4. アップデート設定の調整

アップデートはローカルネットワーク、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。 Bitdefenderは、デフォルトの設定では1時間ごとにアップデートを確認し、自動的に利用可能なアップデートをインストールします。

アップデート設定は、初期設定の状態がほとんどのユーザーにとって最適な設定となっており、特に変更する必要はありません。

アップデート設定を調整するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. ▪ 更新 タブを選択し、必要に応じて設定を変更します。 ▪

更新頻度

Bitdefender は 1 時間ごとにアップデートを確認するように設定されています。 アップデートの頻度を変更するには、スライダーをドラッグして任意の間隔に設定します。

アップデートの確認方法

アップデートが利用可能になるたびに、 Bitdefender は通知は表示せずアップデートを自動的にダウンロードしてインストールします。 新しいアップデートが利用可能になるたびに通知を受け取りたい場合は、サイレントアップデート オプションをオフにしてください。

アップデートのインストールを完了するには、パソコンの再起動が必要な場合があります。

再起動が必要なアップデートが行なわれた場合、ユーザーがご自身でパソコンを再起動するまで、 Bitdefender は古いファイルを使って動作します。 これはBitdefender のアップデートが、パソコン作業を妨げないようにするためです。

再起動が必要なアップデートを通知させる場合は、再起動通知 オプションをオンにしてください。

2.4.5. 継続アップデート

最新バージョンを使用していることを確認するため、 Bitdefender は自動的に製品のアップデートを確認します。 これらのアップデートにより、製品に新機能や改良が適用されたり、製品の問題が修正されたり、製品が新しいバージョンに自動的にアップグレードされたりする可能性があります。 新しい Bitdefender バージョンがアップデート経由で提供された場合、個人設定は保存され、アンインストールおよび再インストール手順はスキップされます。

これらのアップデートは、新しいファイルをインストールするためにシステムの再起動を必要とします。 製品のアップデートが完了すると、システムの再起動を促すポップアップウィンドウが表示されます。 この通知を逃した場合は、最新のアップデートが記載されている 通知 ウィンドウの今すぐ再起動 をクリックするか、システムを手動で再起動してください。

注記
新たな機能や改良を含むアップデートは、 Bitdefender 2018 をインストールしているユーザーにのみ提供されます。

3. 操作手順

3.1. インストール

3.1.1. Bitdefenderを2台目のパソコンにインストールする方法は？

複数のコンピュータに使用可能なサブスクリプションを購入いただいた場合は、 Bitdefender アカウントを使って2台めのPCを登録できます。

Bitdefender を 2 台目のコンピュータにインストールするには:

1. Bitdefender インターフェイス の左下隅にある「別のデバイスにインストールする」 のリンクをクリックします。

   Bitdefender アカウントの Web ページにリダイレクトされます。 ご自身の認証情報を使ってログインしていることを確認してください。

2. 表示されるウィンドウで、ダウンロードリンクを送信をクリックします。
3. 当該フィールドにメールアドレスを入力してメールを送信 をクリックします。 ダウンロードリンクは、以後 24 時間のみ有効です。 リンクの有効期限が切れた場合は、同じ手順を実行して新しいリンクを生成する必要があります。

   Bitdefender をインストールしたいデバイス上で、登録したメールアドレスの受信トレイを開き、届いたメールに記載されているダウンロードボタンを押してください。

4. ダウンロードした Bitdefender 製品を実行します。

Bitdefender 製品をインストールした新しいデバイスが Bitdefender Central ダッシュボードに表示されます。

3.1.2. Bitdefender を再インストールするには?

Bitdefenderの再インストールが必要となる一般的な状況は以下の通りです：

- オペレーティングシステム（OS）を再インストールした場合。
- クラッシュや速度低下の原因となっている問題を修正したい
- Bitdefender 製品が起動していないか、正常に動作していません。

上記のいずれかのケースの場合は、次の手順を実行します:

- Windows 7の場合：
  1. Windows スタートボタンをクリックして、すべてのプログラムを選択してください。
  2. Bitdefender Total Securityを探していただき、削除を選択してください。
  3. 表示されるウィンドウで 再インストール をクリックします。
  4. パソコンを再起動して処理を完了させてください。
- Windows 8 および Windows 8.1:
  1. Windowsスタート画面からコントロールパネルを探して（またはスタート画面で「コントロールパネル」と入力して）、アイコンをクリックしてください。
  2. プログラムのアンインストールまたはプログラムと機能をクリックしてください。
  3. Bitdefender Total Securityを探していただき、削除を選択してください。
  4. 表示されるウィンドウで 再インストール をクリックします。
  5. パソコンを再起動して処理を完了させてください。
- Windows 10の場合：
  1. 開始 をクリックし、続いて「設定」をクリックします。
  2. 設定エリアの システム アイコンをクリックし、アプリケーション・機能 を選択します。
  3. Bitdefender Total Securityを探していただき、削除を選択してください。
  4. アンインストール をもう一度クリックして選択を確定します。
  5. 再インストール をクリックします。
  6. パソコンを再起動して処理を完了させてください。

注記
この再インストール手順に従うことで、ユーザー設定が保存され、新たにインストールされた製品で同じ設定が利用可能になります。 その他の設定は、デフォルトの設定に戻すことができます。

3.1.3. Bitdefender製品はどこでダウンロードできますか？

Bitdefender はインストールディスクまたは Bitdefender Central プラットフォーム を使ってコンピュータにダウンロードしたウェブインストーラからインストールできます。

注記
パソコンに別のセキュリティソリューションを導入している場合、インストーラーを実行する前にアンインストールすることをおすすめします。 同じコンピュータで別のセキュリティソフトを使用すると、システムが不安定になります。

Bitdefender を Bitdefender Central からインストールするには:

1. Bitdefender Centralにアクセスします。
2. マイデバイス パネルを選択し、保護をインストール をクリックします。
3. 以下のいずれかのオプションを選択します:
   - このデバイスを保護

     このオプションを選択するとインストールファイルを保存できます。
   - 他のデバイスを保護

     このオプションを選択してから、ダウンロードリンクを送信 をクリックします。 当該フィールドにメールアドレスを入力してメールを送信をクリックします。 ダウンロードリンクは、以後 24 時間のみ有効です。 リンクの有効期限が切れた場合は、同じ手順を実行して新しいリンクを生成する必要があります。

     Bitdefender 製品をインストールしたいデバイス上で、登録したメールアドレスの受信トレイを開き、届いたメールに記載されているダウンロードボタンをクリックしてください。
4. ダウンロードした Bitdefender 製品を実行します。

3.1.4. Bitdefender の言語を変更するには？

Bitdefender を別の言語で使用したい場合、製品を当該言語で再インストールする必要があります。

Bitdefender を別の言語で使用するには:

1. 以下の手順でBitdefenderを削除してください：
   - Windows 7の場合：

a. スタート ボタンをクリックし、コントロール パネル を開きます。その中にある プログラムおよび機能 をダブルクリックします。

b. Bitdefender Total Securityを探していただき、削除を選択してください。

c. 表示されるウィンドウで 削除 をクリックします。

d. アンインストール処理が完了するまで待ち、それからシステムを再起動します。

- Windows 8 および Windows 8.1:

a. Windowsスタート画面からコントロールパネルを探して（またはスタート画面で「コントロールパネル」と入力して）、アイコンをクリックしてください。

b. プログラムのアンインストールまたはプログラムと機能をクリックしてください。

c. Bitdefender Total Securityを探していただき、削除を選択してください。

d. 表示されるウィンドウで 削除 をクリックします。

e. アンインストール処理が完了するまで待ち、それからシステムを再起動します。

- Windows 10の場合 :

a. 開始 をクリックし、続いて「設定」をクリックします。

b. 設定エリアの システム アイコンをクリックし、インストールされているアプリケーション を選択します。

c. Bitdefender Total Securityを探していただき、削除を選択してください。

d. アンインストール をもう一度クリックして選択を確定します。

e. 表示されるウィンドウで 削除 をクリックします。

f. アンインストール処理が完了するまで待ち、それからシステムを再起動します。

2. Bitdefender Central の言語を変更します:

a. Bitdefender Centralにアクセスします。

b. ウィンドウの右上隅にある アイコンをクリックします。

c. スライドメニューで マイアカウント をクリックします。

d. プロファイル タブを選択します。

e. 言語 ドロップダウンリストから言語を選択し、保存 をクリックします。

3. インストールファイルをダウンロード:

a. マイデバイス パネルを選択し、保護をインストール をクリックします。

b. 以下のいずれかのオプションを選択します:

- このデバイスを保護

  このオプションを選択するとインストールファイルを保存できます。

- 他のデバイスを保護

  このオプションを選択してから、ダウンロードリンクを送信 をクリックします。 当該フィールドにメールアドレスを入力してメールを送信 をクリックします。 ダウンロードリンクは、以後 24 時間のみ有効です。 リンクの有効期限が切れた場合は、同じ手順を実行して新しいリンクを生成する必要があります。

  Bitdefender をインストールしたいデバイス上で、登録したメールアドレスの受信トレイを開き、届いたメールに記載されているダウンロードボタンをクリックしてください。

4. ダウンロードした Bitdefender 製品を実行します。

注記
この再インストール手順を実行すると、カスタマイズした設定が完全に削除されます。

3.1.5. Windows のアップグレード後に Bitdefender のサブスクリプションを利用するには?

この状況は、オペレーティングシステムのアップグレード後に Bitdefender のサブスクリプションの利用を継続したいときに発生します。

古いバージョンの Bitdefender をお使いの場合は、以下の手順で最新の Bitdefender に無料でアップグレードできます:

- 過去バージョンの Bitdefender Antivirus から、最新バージョンの Bitdefender Antivirus までを利用可能です。

- 過去バージョンの Bitdefender Internet Security から、最新バージョンの Bitdefender Internet Security までを利用可能です。
- 過去バージョンの Bitdefender Total Security から、最新バージョンの Bitdefender Total Security までを利用可能です。

以下の 2 通りのケースが考えられます:

- Windows Update を使用してオペレーティングシステムをアップグレードした後、 Bitdefender が動作しなくなってしまった場合。

  この場合、以下の手順で製品をインストールする必要があります:

  - Windows 7の場合 :

    1. スタート ボタンをクリックし、コントロール パネル を開きます。その中にある プログラムおよび機能 をダブルクリックします。
    2. Bitdefender Total Securityを探していただき、削除を選択してください。
    3. 表示されるウィンドウで 再インストール をクリックします。
    4. アンインストール処理が完了するまで待ち、それからシステムを再起動します。

       新たにインストールされた Bitdefender 製品のインターフェイスを開くと、各機能にアクセスできます。

  - Windows 8 および Windows 8.1:

    1. Windowsスタート画面からコントロールパネルを探して（またはスタート画面で「コントロールパネル」と入力して）、アイコンをクリックしてください。
    2. プログラムのアンインストールまたはプログラムと機能をクリックしてください。
    3. Bitdefender Total Securityを探していただき、削除を選択してください。
    4. 表示されるウィンドウで 再インストール をクリックします。
    5. アンインストール処理が完了するまで待ち、それからシステムを再起動します。

       新たにインストールされた Bitdefender 製品のインターフェイスを開くと、各機能にアクセスできます。

  - Windows 10の場合 :

1. 開始 をクリックし、続いて「設定」をクリックします。
2. 設定エリアの システム アイコンをクリックし、インストールされているアプリケーション を選択します。
3. Bitdefender Total Securityを探していただき、削除を選択してください。
4. アンインストール をもう一度クリックして選択を確定します。
5. 表示されるウィンドウで 再インストール をクリックします。
6. アンインストール処理が完了するまで待ち、それからシステムを再起動します。

   新たにインストールされた Bitdefender 製品のインターフェイスを開くと、各機能にアクセスできます。

注記
この再インストール手順に従うことで、ユーザー設定が保存され、新たにインストールされた製品で同じ設定が利用可能になります。 その他の設定は、デフォルトの設定に戻すことができます。

- システムを変更して、 Bitdefender を引き続き利用したい場合。 製品の最新バージョンを再インストールする必要があります。

  この状況を解決するには:

  1. インストールファイルをダウンロード:
     a. Bitdefender Centralにアクセスします。
     b. マイデバイス パネルを選択し、保護をインストール をクリックします。
     c. 以下のいずれかのオプションを選択します:
        - このデバイスを保護

          このオプションを選択するとインストールファイルを保存できます。
        - 他のデバイスを保護

          このオプションを選択してから、ダウンロードリンクを送信 をクリックします。 当該フィールドにメールアドレスを入力してメールを送信 をクリックします。 ダウンロードリンクは、以後 24

時間のみ有効です。 リンクの有効期限が切れた場合は、同じ手順を実行して新しいリンクを生成する必要があります。

Bitdefender 製品をインストールしたいデバイス上で、登録したメールアドレスの受信トレイを開き、届いたメールに記載されているダウンロードボタンをクリックしてください。

2. ダウンロードした Bitdefender 製品を実行します。

Bitdefenderのインストール手順に関する詳細については、「Bitdefender Antivirus for Macをインストールしています」 (p. 215)をご参照ください。

3.1.6. 最新のBitdefender バージョンにアップグレードするには？

今後は、手動によるアンインストールおよび再インストールの手順を実行することなく、最新バージョンにアップグレードすることが可能です。 より正確には、新しい機能や大幅な改良が加えられた新製品は製品アップデートを介して提供され、お客様が有効な Bitdefender サブスクリプションをお持ちの場合、新製品は自動的にアクティベートされます。

2018 バージョンを使用している場合は、次の手順で最新バージョンにアップグレードできます:

1. アップグレード情報とともに受け取った通知の 今すぐ再起動 をクリックします。 通知を逃した場合は、通知 ウィンドウにアクセスして最新の更新プログラムを参照し、今すぐ再起動 ボタンをクリックします。 コンピュータが再起動するのを待ちます。

   新機能 ウィンドウには、改良された機能や新機能に関する情報が表示されます。

2. もっと読む リンクをクリックすると専用のページにリダイレクトされ、さらに詳しい情報や役に立つ記事などを参照できます。

3. 新機能 ウィンドウを閉じると、新たにインストールされたバージョンのインターフェイスにアクセスできるようになります。

Bitdefender 2016 以前のバージョンから最新の Bitdefender バージョンにアップグレードしたい場合は、コントロールパネルから現在のバージョンを削除してから、 Bitdefender ウェブサイトから最新のインストールファイルをダウンロードする必要があります: https://www.bitdefender.com/Downloads/ 。 アクティベーションには有効なサブスクリプションが必須です。

3.2. サブスクリプション

3.2.1. ライセンスキーを使って Bitdefender のサブスクリプションを有効化するには?

有効なライセンスキーを所有していて、それを使って Bitdefender Total Security のサブスクリプションを有効化する場合は、以下の 2 通りの方法があります:

- 過去の Bitdefender バージョンから新しいバージョンにアップグレードする:
  1. Bitdefender Total Security へのアップグレードが完了すると、Bitdefender アカウントへのログインを求められます。 ▪
  2. サインイン をクリックし、入力欄に Bitdefender アカウントのメールアドレスとパスワードを入力します。
  3. サインイン をクリックして続行します。
  4. アカウント画面に、サブスクリプションが作成されたことを知らせる通知が表示されます。 作成されたサブスクリプションは、お持ちのライセンスキーの残りの有効日数、同じ数のユーザー分をご利用いただくことが可能です。

     過去の Bitdefender バージョンを使用していて、サブスクリプションを変換したライセンスキーで登録されているデバイスは、同じ Bitdefender アカウントで製品をアクティベーションする必要があります。
- 過去にBitdefender をシステムにインストールしたことがない場合
  1. インストール処理が完了すると、 Bitdefender アカウントへのログインを求められます。
  2. サインイン をクリックし、入力欄に Bitdefender アカウントのメールアドレスとパスワードを入力します。
  3. ▪サインイン をクリックして続行し、終了 をクリックして Bitdefender Total Security のインターフェイスにアクセスします。 ▪
  4. Bitdefender インターフェイスのナビゲーションメニューにある マイアカウント をクリックします。
  5. 今すぐ有効にする をクリックします。

新しいウィンドウが表示されます。

6. 無料アップグレードを今すぐ入手！リンクをクリックします。
7. 該当の入力欄にライセンスキーを入力し、製品をアップグレードするをクリックします。 ライセンスキーと同じ内容およびユーザー数のサブスクリプションがアカウントに紐付けされています。

3.3. Bitdefender Central

3.3.1. 別のオンラインアカウントを使って Bitdefender Central にログインするには?

Bitdefender アカウントを新規で作成すると、すぐに使い始めることができます。

別のアカウントを使用するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある マイアカウント をクリックします。
2. コンピュータにリンクされているアカウントを変更するには、画面の右上隅にある アカウントの切り替え をクリックします。
3. 該当のフィールドにアカウントのメールアドレスとパスワードを入力し、サインイン をクリックします。

注記
デバイス上の Bitdefender 製品は、新しい Bitdefender アカウントに紐付けられているサブスクリプションに応じて自動的に変更されます。
新しい Bitdefender アカウントに利用可能なサブスクリプションが紐付けられていない、もしくは以前のアカウントから移行したい場合は、セクション「サポートを依頼」 (p. 317)の説明に従って Bitdefender サポートにお問い合わせください。

3.3.2. Bitdefender Central ヘルプメッセージをオフにするには？

ダッシュボードに、 Bitdefender Central で利用できる各オプションの機能の説明が表示されます。

このようなメッセージを非表示にするには:

1. Bitdefender Centralにアクセスします。

2. ウィンドウの右上隅にある アイコンをクリックします。
3. スライドメニューで マイアカウント をクリックします。
4. 設定 タブを選択します。
5. ヘルプメッセージをオン/オフにする オプションを無効にします。

3.3.3. Bitdefender アカウントに設定したパスワードを忘れてしまった場合の リセット方法は？

Bitdefender アカウントに新しいパスワードを設定する方法は 2 つあります:

- Bitdefender の管理画面から:
  1. Bitdefender インターフェイスのナビゲーションメニューにある マイアカウント をクリックします。
  2. 画面の右上隅にある、アカウントの切り替え をクリックします。

     新しいウィンドウが表示されます。
  3. パスワードを忘れた場合をクリックします。
  4. Bitdefender アカウントの作成に使用したメールアドレスを入力し、パスワードを忘れた場合 をクリックします。
  5. メールをチェックして、記載されているボタンをクリックします。

     Bitdefender のパスワードのリセット用ウィンドウが開きます。
  6. メールアドレスと新しいパスワードをそれぞれのフィールドに入力します。 パスワードは最低 8 文字で、数字を含める必要があります。
  7. パスワードのリセット をクリックします。
- ウェブブラウザから:
  1. 次のサイトへアクセスします：https://central.bitdefender.com
  2. パスワードを忘れた場合をクリックします。
  3. メールアドレスを入力し、「パスワードを忘れた場合」をクリックします。
  4. メールアカウントを確認し、記載されている手順に従って Bitdefender アカウントに新しいシステムパスワードを設定します。

今後 Bitdefender アカウントにアクセスするには、メールアドレスと先ほど設定した新しいパスワードを入力します。

3.3.4. Bitdefenderアカウントに紐付けされているログオンセッションを管理するには?

Bitdefender アカウントでは、アカウントに紐付けされているデバイス上で実行されている最新のアクティブおよび非アクティブなログインセッションを表示できます。 また、以下の方法でリモートからサインアウトできます:

1. Bitdefender Centralにアクセスします。
2. ウィンドウの右上隅にある アイコンをクリックします。
3. スライドメニューで マイアカウント をクリックします。
4. セッション管理 タブをタップします。
5. アクティブなセッション エリアで、ログオンセッションを終了したいデバイスの横にある サインアウト オプションを選択します。

3.4. Bitdefenderによるスキャン

3.4.1. ファイルやフォルダのウイルス検査方法は？

最も簡単な方法は、検査対象のファイルやフォルダを右クリックして、メニュー内の Bitdefender ＞ Bitdefender で検査を選択することです。

検査を完了させるには、ウイルス対策 スキャン ウィザードの手順に従ってください。 Bitdefenderは検出したファイルに対して、推奨された対処法をとります。

対処されていない脅威がある場合は、処理を行うように促されます。

このスキャン方式は次の場合に使うことができます：

- 特定のファイル、フォルダへの感染が疑われる場合。
- 安全性が疑われるファイルをインターネットからダウンロードしたとき。
- パソコンへファイルをコピーする前にネットワーク共有フォルダを検査する。

3.4.2. パソコン全体のウイルス検査方法は？

システムの完全スキャンを実行するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。

2. アンチウイルスウィンドウで、 システムスキャンをクリックします。
3. システム スキャンウィザードに従ってスキャンを完了します。 Bitdefenderは検出したファイルに対して、推奨された対処法をとります。

   対処されていない脅威がある場合は、処理を行うように促されます。 詳細については、「ウイルス対策 スキャン ウィザード」 (p. 91)をご参照ください。

3.4.3. スキャンのスケジュールを設定するには?

コンピュータを使用していない間に、システム上の重要な場所をスキャンするように Bitdefender を設定できます。

スキャンをスケジュールするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護をクリックします。
2. アンチウイルス ウィンドウで、 スキャンの管理クリックします。
3. スケジュール設定したいスキャンの種類 (フルシステムスキャンまたはクイックスキャン) を選択し、スキャンオプション をクリックします。

   あるいは 新しいカスタムタスク をクリックして、ニーズに合わせたスキャンタイプを作成することができます。
4. スケジュール オプションを有効にします。

   スケジュールを設定するには、該当のいずれかのオプションを選択:

   - システム起動後に実行
   - 1 回のみ実行
   - 定期的に実行

スキャン対象 ウィンドウで、スキャンする場所を選択できます。 このオプションは、カスタムスキャンを新規作成する場合のみ利用可能です。

3.4.4. カスタム スキャン タスクの作成方法は?

コンピュータ上の特定の場所をスキャンしたい場合や、スキャンオプションを設定したい場合は、カスタムスキャンタスクを設定して実行します。

カスタム スキャン タスクを作成するには、以下の手順に従ってください:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. アンチウイルス ウィンドウで、 スキャンの管理クリックします。
3. 新しいカスタムタスク をクリックします。 基本設定 ウィンドウでスキャンの名前を入力し、スキャンする場所を選択します。
4. スキャンオプションを細かく設定する場合は、詳細設定 タブを選択します。

   スキャンレベルを調整することで簡単に検査のオプションを設定することができます。 スライダーをドラッグして、お好みの検査レベルに設定します。

   検査が完了して脅威が見つからなかった場合、そのままパソコンを自動的に終了させるように設定することも可能です。 タスクを実行した場合は、こちらがデフォルトの動作になります。
5. OK をクリックすると、変更が保存され、画面が自動で閉じます。
6. 該当するスイッチを使って、スキャンタスクのスケジュールを設定できます。
7. ウイルス検査を開始 をクリックし、スキャンウィザードの手順に従ってスキャンを完了してください。 検査の完了後、ウイルス検知があった場合、検知されたファイルの処理方法を選択するように促されます。
8. 利用可能なリストから該当する項目をクリックすることで、前回のスキャンを必要に応じてすばやく再実行することができます。

3.4.5. フォルダをスキャンから除外するには？

Bitdefenderでは、特定のファイル、フォルダ、ファイル拡張子をスキャンから除外することができます。

例外の設定は、パソコンに関して知識を持ったユーザーが、以下のような状況で行う場合のみ使用することをおすすめします：

- パソコン上に、動画や音楽ファイルが入った大きなフォルダがある場合。
- パソコン上に、複数のデータを含む大きなアーカイブがある場合。
- テスト目的でインストールしたさまざまな種類のソフトウェアのフォルダを保持しており、 フォルダを検査すると、一部データを失う可能性がある場合。

フォルダを例外設定リストに追加するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. ウイルス対策 パネルで 隔離フォルダ をクリックします。
3. 例外設定 タブをクリックします。
4. スキャン対象の例外に設定するファイルとフォルダの一覧のアコーディオンメニューをクリックし、追加 をクリックします。
5. 参照 をクリックし、スキャン対象から除外したいフォルダを選択してから、除外するスキャンの種類を選択します。
6. 追加 をクリックして変更を保存し、ウィンドウを閉じます。

3.4.6. Bitdefender が正常なファイルを感染ファイルとして誤検出した場合の対処方法は？

Bitdefender が、通常のファイルを脅威として誤認識してしまうことがあります。 このエラーを修正するには、 Bitdefender の例外設定エリアに、ファイルを追加してください:

1. Bitdefenderのリアルタイム保護を無効にします。
   a. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
   b. ウイルス対策 パネルで 隔離フォルダ をクリックします。
   c. シールド ウィンドウで Bitdefender シールド をオフにします。

      警告ウィンドウが表示されます。 メニューから、リアルタイム保護機能を無効にする時間を選択し、内容を確認します。 リアルタイム保護は 5 分、15分、30 分、1 時間、無制限、あるいはシステムの次回再起動まで無効にできます。
2. Windows 内で隠し属性のファイルを表示します。 これを行う方法については、「Windows で隠し属性のファイルを表示するには？」 (p. 76) を参照してください。
3. ファイルを隔離フォルダから復元する：
   a. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
   b. ウイルス対策 パネルで 隔離フォルダ をクリックします。
   c. ファイルを選択し、復元 をクリックします。

4. 例外リストにファイルを追加します。 これを行う方法については、「フォルダをスキャンから除外するには？」 (p. 55) を参照してください。
5. Bitdefenderのリアルタイム保護をONにしてください。
6. 誤検知を脅威情報アップデートから削除するために、サポートまでご連絡ください。 これを行う方法については、「サポートを依頼」 (p. 317) を参照してください。

3.4.7. Bitdefender が検知した脅威はどうやって確認するのでしょうか？

検査を行う度に、検査履歴が作成され、 Bitdefender が検知した問題を履歴に保存します。

スキャン ログには、スキャン オプション、スキャン対象、検出された脅威、実行した処理など、スキャン処理に関する詳細情報が記載されています。

スキャンが完了すると、スキャン ウィザードから、スキャン ログを開くことができます。ログを表示 をクリックしてください。

スキャンログや検出された脅威を後でチェックするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 通知をクリックします。
2. 全て タブで、最新のスキャンに関する通知を選択します。

   ここでは、アイドルスキャンで検知した脅威や、ユーザーが実行した検査、リアルタイム保護のステータス変更など、ウイルス検査のすべてのイベントを確認することができます。
3. 通知リストでは、最近実行したスキャンを確認できます。 通知をクリックするとその詳細が表示されます。
4. 検査ログを表示するには、ログを表示をクリックします。

3.5. お子様保護

3.5.1. 子供をオンラインの脅威から守るにはどうすればいいのですか？

Bitdefender のペアレンタルコントロールでは、インターネットおよび特定のアプリケーションへのアクセスを制限できるため、留守中にお子様が不適切コンテンツにアクセスしてしまうことを防止できます。

ペアレンタルコントロールを設定するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. ペアレンタルコントロール パネルで設定をクリックします。

   Bitdefender アカウントの Web ページにリダイレクトされます。 ご自身の認証情報を使ってログインしていることを確認してください。
3. ペアレンタルコントロールのダッシュボードが開きます。 ここからはペアレンタルコントロールの設定を確認したり、設定内容を変更することができます。
4. 子供 ウィンドウ右側の プロファイルの追加 をクリックします。
5. 対応するフィールドに名前、生年月日などを設定します。 プロフィール画像を追加するには、ファイルを選択リンクをクリックします。 次のステップ をクリックして続行します。

   お子様の生年月日を設定すると、お子様の年齢カテゴリーに適切と判断されたウェブ設定が自動的に読み込まれます。
6. お子様のデバイスに Bitdefender Total Security がすでにインストールされている場合は、リストからデバイスを選択して監視したいアカウントを選択します。 保存 をクリックします。

   お子様が Android または iOS デバイスを使用していて、 Bitdefender ペアレンタルコントロールアプリがまだインストールされていない場合は、デバイスの追加 をクリックします。 お子様が Mac デバイスを使用していて、 Bitdefender Antivirus for Mac がまだインストールされていない場合は同じボタンをクリックします。 アプリをインストールしたいオペレーティングシステムを選択し、次のステップ をクリックして続行します。
7. Bitdefender アプリケーションのダウンロード用リンクを受け取るメールアドレスを入力し、インストール用リンクを送信 をクリックします。

インターネットに接続されたコンピュータまたはモバイルデバイス上で Bitdefender アカウントにログインすることで、いつでもどこでもお子様のアクティビティをチェックしたり、ペアレンタル コントロールの設定の設定を変更したりできます。

重要項目
Windows ベースのデバイスでは、サブスクリプションに含まれている Bitdefender Total Security をダウンロードしてインストールする必要があります。
macOS デバイスでは、 Bitdefender Antivirus for Mac ダウンロードしてインストールする必要があります。
Android または iOS デバイスでは、 Bitdefender ペアレンタルコントロールアプリをダウンロードしてインストールする必要があります。

3.5.2. 特定のWebページへ子供がアクセスできないようにするには？

Bitdefender のペアレンタルコントロールでは、お子様が自分のデバイスでアクセスできるコンテンツを制限したり、特定のウェブサイトへのアクセスをブロックしたりできます。

ウェブサイトへのアクセスをブロックするには、以下の手順で例外リストに追加する必要があります:

1. 次のサイトへアクセスします : https://central.bitdefender.com
2. メールアドレスとパスワードを使って Bitdefender アカウントにログインします。
3. ペアレンタルコントロールをクリックしてダッシュボードを開きます。
4. お子様のプロファイルを 子供 画面で選択します。
5. ウェブサイト タブをタップします。
6. 管理ボタンをクリックします。
7. ブロックしたいウェブページを、対応するフィールドに入力します。
8. 許可 または ブロック を選択します。
9. FINISHをクリックして変更を保存します。

注記
制限は、Android および Windows デバイスに対してのみ設定できます。

3.5.3. 子供が特定のアプリを使えないようにするには？

Bitdefender　のペアレンタルコントロールでは、お子様がデバイス使用時にアクセスできるコンテンツを制御できます。

アプリへのアクセスをブロックするには:

1. 次のサイトへアクセスします：https://central.bitdefender.com
2. メールアドレスとパスワードを使って Bitdefender アカウントにログインします。
3. ペアレンタルコントロールをクリックしてダッシュボードを開きます。
4. お子様のプロファイルを 子供 画面で選択します。
5. アプリケーション タブをタップします。
6. 割り当てられているデバイスのリストが表示されます。

   アプリへのアクセスを制限したいデバイスのカードを選択します。
7. 次のユーザーが使用したアプリを管理... をクリックします。

   インストールされているアプリのリストが表示されます。
8. お子様に使用させたくないアプリの横にある ブロック を選択します。

3.5.4. 子供がオンラインで知らない人物とやり取りするのを防ぐには?

Bitdefender　のペアレンタルコントロールでは、お子様の連絡先リストにない電話番号や、連絡先リスト内の特定の電話番号/友達からの着信をブロックすることができます。

Bitdefender　ペアレンタルコントロールアプリがインストールされている Android デバイス上で、特定の連絡先をブロックするには:

1. 次のサイトへアクセスします：https://central.bitdefender.com
2. メールアドレスとパスワードを使って Bitdefender アカウントにログインします。
3. ペアレンタルコントロールをクリックしてダッシュボードを開きます。
4. 制限をかけたいお子様のプロファイルを選択します。

   選択したプロファイルに、使用中の Android デバイスが割り当てられていることを確認してください。

5. 電話の連絡先 タブをタップします。

   カードのリストが表示されます。 カードは、お子様のデバイスの連絡先を示しています。

6. ブロックしたい電話番号のカードを選択します。

   表示されるチェックマークは、選択した電話番号ではお子様につながらないことを示しています。

   SMS メッセージは、お子様のデバイス上で Bitdefender ペアレンタルコントロールを設定した際に、デフォルトのアプリの代わりにペアレンタルコントロールのメッセージングアプリの使用を選択した場合のみブロックされます。

Bitdefender ペアレンタルコントロールアプリがインストールされていない Android デバイス上で特定の連絡先をブロックするには:

1. 次のサイトへアクセスします : https://central.bitdefender.com
2. メールアドレスとパスワードを使って Bitdefender アカウントにログインします。
3. ペアレンタルコントロールをクリックしてダッシュボードを開きます。
4. 制限をかけたいお子様のプロファイルを選択します。
5. 任意のカードのデバイスにペアレンタルコントロールをインストールのリンクをクリックします。
6. 表示されるウィンドウで デバイスの追加 をクリックします。
7. リストから Android を選択し、次のステップ をクリックして続行します。
8. Bitdefender アプリケーションのダウンロード用リンクを受け取るメールアドレスを入力し、インストール用リンクを送信 をクリックします。
9. 弊社サーバーから届いたメールに記載されているインストール手順に従って、任意のデバイスにアプリをインストールしてください。
10. Bitdefender Central の電話 タブをタップします。

    カードのリストが表示されます。 カードは、お子様の Android スマートフォン上の連絡先を示しています。

11. ブロックしたい電話番号のカードを選択します。

    表示されるチェックマークは、選択した電話番号ではお子様につながらないことを示しています。

SMS メッセージは、お子様のデバイス上で Bitdefender ペアレンタルコントロールを設定した際に、デフォルトのアプリの代わりにペアレンタルコントロールのメッセージングアプリの使用を選択した場合のみブロックされます。

不明な電話番号への、あるいは不明な電話番号からの発着信は、不明な「発信者番号なし」のプライベート番号からのコールをブロックします　のスイッチを有効にすることでブロックできます。

注記
音声通話に対する制限は、お子様のプロファイルに割り当てられた Android デバイスに対してのみ設定でき、着信と発信の両方に対して適用されます。

3.5.5. 子供がアクセスしてもいい場所と、アクセスを禁止する場所を設定するには?

Bitdefender　ペアレンタルコントロールでは、子供がアクセスしてもいい場所と、アクセスを禁止する場所を設定できます。

場所を設定するには:

1. 次のサイトへアクセスします : https://central.bitdefender.com
2. メールアドレスとパスワードを使って Bitdefender アカウントにログインします。
3. ペアレンタルコントロールをクリックしてダッシュボードを開きます。
4. お子様のプロファイルを 子供 画面で選択します。
5. お子様の場所 タブをタップします。
6. お子様の場所 ウィンドウのフレーム内の デバイス をクリックします。
7. デバイスの選択 をクリックし、設定したいデバイスを選択します。
8. エリア ウィンドウで エリアの追加 ボタンをクリックします。
9. 場所の種類を 安全 または 制限 のいずれかから選択します。
10. お子様がアクセスできる（またはできない） エリアに付ける名前を入力します。
11. 半径 スライドバーで、モニタリングの適用範囲を設定します。
12. 設定を保存するには エリアを追加 をクリックします。

制限されている場所を安全として設定したり、安全とされている場所を制限したりするには、設定を変更したい場所をクリックして　エリアの編集

ボタンをクリックします。 希望の変更内容に応じて、安全 または 制限 オプションを選択し エリアを更新 をクリックします。

3.5.6. 平日アクティビティ時に子供が割り当てられたデバイスにアクセスするのをブロックするには？

Bitdefender ペアレンタルコントロールでは、お子様が学校にいる時間帯や、宿題をしているべき時間帯、もしくは寝ているべき時間帯に、割り当てられたデバイスへのアクセスを制限することができます。

時間制限を設定するには:

1. Bitdefender Central から、ペアレンタルコントロール パネルにアクセスします。
2. 子供 ウィンドウで、制限をかけたいお子様のプロファイルを選択します。
3. スクリーン時間 タブを選択します。
4. 時間制限の確認をクリックします。
5. 時間制限の設定 エリアで、時間制限を新規追加 をクリックします。
6. 設定する制限に名前を付けてください （たとえば寝る時間、宿題、テニスレッスンなど）。
7. 制限を適用したい日付と時間帯を設定し、追加 をクリックして設定を保存します。

3.5.7. 日中や夜間に子供が割り当てられたデバイスにアクセスするのをブロックするには？

Bitdefender ペアレンタルコントロールを使うと、日中の様々な時間帯でのお子様による割り当てられたデバイスへのアクセスを制限することができます。

1 日の使用制限を設定するには:

1. Bitdefender Central から、ペアレンタルコントロール パネルにアクセスします。
2. 子供 ウィンドウで、制限をかけたいお子様のプロファイルを選択します。
3. スクリーン時間 タブを選択します。

4. 時間制限の確認をクリックします。
5. 時間制限の設定 エリアで、1 日の時間制限を新規追加 をクリックします。
6. 制限を適用したい日時を設定し、保存 をクリックして設定を保存します。

3.5.8. お子様のプロフィールを削除するには

既存のお子様のプロファイルを削除するには:

1. 次のサイトへアクセスします : https://central.bitdefender.com
2. メールアドレスとパスワードを使って Bitdefender アカウントにログインします。
3. ペアレンタルコントロールをクリックしてダッシュボードを開きます。
4. 削除したいお子様のプロファイルの アイコンをクリックし、削除を選択します。

3.6. プライバシー保護

3.6.1. オンライン取り引きを安全に行う方法は？

オンライン取引やネット銀行を使用する際に、機密情報を第三者によって盗み取られるのを防ぐには、 Bitdefenderが提供する独自ブラウザを使用してください。

Bitdefender Safepay™ は、クレジットカード情報を含む重要な個人データをしっかりと保護するセキュアなブラウザです。

オンラインアクティビティを安全に保つには:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. 決済ブラウザ パネルで 決済ブラウザを起動 をクリックします。
3. バーチャルキーボード にアクセスするには ボタンをクリックします。

   パスワードなどの機密情報を入力する際にはバーチャル・キーボードをご利用ください。

3.6.2. デバイスが盗難に遭ったときは?

スマートフォンやタブレットなどのモバイル機器の盗難は、世界中の企業および個人にとって大きな問題になっています。

Bitdefender の盗難防止機能では、盗まれたデバイスの位置情報の確認やリモートロックが行えるだけでなく、デバイス上のデータをすべて完全に消去して情報を漏洩を防ぐことも可能です。

アカウントからデバイス盗難対策機能にアクセスするには:

1. Bitdefender Centralにアクセスします。
2. マイデバイス パネルを選択します。
3. 任意のデバイスカードをクリックして 窃盗防止 を選択します。
4. ご利用される機能を選択してください :
   - 位置確認- デバイスの位置を Google マップで表示します。
   - アラート- デバイスにアラートを送信します。
   - ロック - パソコンをロックし、解除用の暗証番号を設定します。あるいは、対応するオプションを有効にすることで、 Bitdefender はデバイスに不正にアクセスしようとする人物の写真を撮影できるようになります。
   - ワイプ - パソコンのデータを全て消去します。

     重要項目
     デバイスをワイプすると、盗難対策の機能も全て機能しなくなります。

   - IP を表示 - 選択したデバイスの前回の IP アドレスを表示します。

3.6.3. ファイル金庫の使用方法は?

Bitdefenderファイル金庫は、機密文書を格納することができる、パスワードがかけられて、暗号化された論理ドライブ（金庫）です。 ファイル金庫は、物理的には、ローカルのハードディスクに格納されたファイルで、.bvd の拡張子を持っています。

ファイル金庫の作成では、'サイズ' と 'パスワード' の 2点が重要です。初期設定の 100 MBは個人ドキュメントやExcelファイルには十分の容量です。 ただし、動画やその他サイズの大きいファイルについては、より大きな容量が必要になる場合があります。

Bitdefender ファイル金庫で重要なファイルやフォルダを安全に保管するには:

- ファイル金庫を作成し、強固なパスワードを設定してください。

  金庫を作成するには、デスクトップ上の任意の場所、またはコンピュータ上のフォルダを右クリックし、 Bitdefender> Bitdefender ファイル金庫 を開いて ファイル金庫の作成 を選択します。

  新しいウィンドウが表示されます。 次のように実行します :

  1. 参照をクリックして金庫の保存場所を選択し、任意のファイル名で保存します。
  2. メニューからドライブ文字を選択。 ファイル金庫を開くと、選択されたドライブレターがついた仮想ディスクドライブがマイ コンピュータ上に表示されます。
  3. ファイル金庫のパスワードをパスワードの入力と確認の欄に入力してください。
  4. 金庫のデフォルトのサイズ (100MB) を変更したい場合は、金庫のサイズ (MB)スピンボックスの上下矢印キーを使用します。
  5. 作成 をクリックします。

  注記
  ファイル金庫を開くと、仮想ディスクドライブがマイ コンピュータ上に表示されます。 このドライブは金庫に割り当てられたドライブ名で表示されます。

- ファイル金庫に追加して安全にするファイル/フォルダを追加します。

  ファイルを金庫に追加するには、まずその金庫を開く必要があります。

  1. 金庫ファイル (.bvd) を参照してください。
  2. 金庫ファイルを右クリックして、Bitdefender ファイル金庫にカーソルを当て、開く を選択します。
  3. 表示されるウィンドウでパスワードを入力し、金庫を割り当てるドライブ文字を選択して OKをクリックします。

  これによりファイル金庫に関連付けられたドライブ上の操作を、Windows エクスプローラを使って、あたかも普通のドライブにするように行うことができます。 ファイルを開いている金庫に追加するには、ファイルを

右クリックして、 Bitdefender 金庫を指定し、ファイル金庫に追加 を選択する方法もあります。

- ファイル金庫には常にロックをかけてください。

  ファイル金庫は、保管ファイルへのアクセスが必要になった場合や、内容を管理する場合にのみ、開くようにしてください。 ファイル金庫をロックするにはマイ コンピュータ上の仮想ドライブを右クリックして、Bitdefenderファイル金庫 > ロックを選択してください。

- .bvd 金庫ファイルを削除しないようにします。

  ファイルを削除することで、ファイル金庫の内容も削除されます。

ファイル金庫の操作方法についての詳細は、「ファイル暗号化」 (p. 132)をご参照ください。

3.6.4. Bitdefenderを使ってファイルを完全に削除する方法は？

パソコンからファイルを完全に削除するには、データを物理的にハードディスクから削除する必要があります。

Bitdefenderファイル シュレッダーを使用すれば、Windowsの右クリックメニューから簡単にかつ素早くファイルを完全削除することができます。手順は以下の通りです：

1. 完全に削除するファイルまたはフォルダを右クリックし、右クリックメニュー内のBitdefenderにカーソルを当て、ファイル シュレッダーを選択してください。
2. 完全に削除 をクリックして、削除処理を続行することを確認します。

   Bitdefender がファイル シュレッダーを完了するまでお待ちください。
3. 結果が表示されます。 終了をクリックしてウィザードを終了します。

3.6.5. ウェブカメラをハッキングから守るには?

インストールされたアプリケーションのウェブカムへのアクセスを許可または拒否するように Bitdefender 製品を設定するには、次の手順を実行します。

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。

2. ウェブカメラ保護ウィンドウで、ウェブカメラアクセス をクリックします。

   ウェブカメラへのアクセスを要求したアプリケーションがここに表示されます。

3. アクセスを許可または禁止したいアプリケーションを参照し、対応するスイッチをクリックします。

   選択アプリに対する他の Bitdefender ユーザーの対応を確認するには アイコンをクリックします。 リストにあるアプリケーションが Bitdefender ユーザーによってブロックされるたびに通知されます。

このリストにアプリケーションを手動で追加するには 新規アプリケーションをリストに追加 リンクをクリックします。

3.6.6. 復元プロセスが失敗した場合に、暗号化されたファイルを手動で復元するにはどうすればよいですか？

暗号化されたファイルを自動的に復元できない場合は、次の手順により手動で復元することができます:

1. Bitdefender インターフェイスのナビゲーションメニューにある 通知 をクリックします。
2. 全て タブで、検出された最新のランサムウェア攻撃に関する通知を選択し、暗号化ファイル をクリックします。
3. 暗号化されたファイルの一覧が表示されます。

   ファイルを復元 をクリックして続行します。
4. 修復処理のすべてまたは一部が失敗した場合、復元されたファイルを保存する場所を選択する必要があります。 復元場所をクリックして、PC上の任意の場所を選択します。
5. 確認画面が表示されます。

   終了をクリックして復元処理を終了します。

以下の拡張子を持つファイルが暗号化された場合、復元することが可能です:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb; .doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html; .ico; .jar; .java; .jpeg; .jpg; .js; .jsp; .key; .m4v; .mdb;

.mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp; .odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

3.7. 最適化ツール

3.7.1. パソコンのパフォーマンスを向上させるにはどうすればいいですか？

パソコンのパフォーマンスは、CPU・メモリ容量・ハードディスク容量などのハードウェア構成にのみ依存するわけではありません。 ソフトウェア構成やデータ管理に直接結び付きます。

Bitdefender はパソコンのスピードとパフォーマンスを向上させるために、以下の機能を実装しています。

- 「シングルクリックでシステムのパフォーマンスを最適化」（p. 69）
- 「定期的にパソコンの検査を行う」（p. 70）

シングルクリックでシステムのパフォーマンスを最適化

ワンクリック オプティマイザでは、システム内の不要なファイルをすばやくスキャンしてクリーンアップすることで、簡単にシステムのパフォーマンスを改善できます。

クイック最適化ツールの処理を開始するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある ユーティリティ をクリックします。
2. デバイスを最適化する をクリックします。
3. Bitdefender が安全に削除可能なファイルを検索しますので、最適化 ボタンをクリックして処理を完了します。

シングルクリックでコンピュータの速度を向上する方法の詳細については、「シングルクリックでシステムの速度を最適化」（p. 171）を参照してください。

定期的にパソコンの検査を行う

パソコンのパフォーマンスや通常動作も脅威に影響される可能性があります。

パソコンは定期的に（1週間に一度）ウイルス検査を行うことをおすすめします。

システムスキャンはセキュリティに影響するあらゆる脅威を検出し、圧縮ファイル内も検査するため、システムスキャンを実行することをおすすめします。

システム スキャンを開始:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. アンチウイルスウィンドウで、 システムスキャンをクリックします。
3. ウィザードの手順に随ってください。

3.7.2. システムの起動時間を短縮するには?

起動オプティマイザは、PC の起動時間を遅くしている不要なアプリケーションを無効または延期できるため、貴重な時間を節約できます。

スタートアップ最適化ツールを使用するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある ユーティリティ をクリックします。
2. デバイスの起動を最適化 をクリックします。
3. システム起動時に延期したいアプリケーションを選択します。

PC の起動時間を最適化する方法の詳細については 「PC の起動時間を最適化する」 (p. 172) を参照してください。

3.8. その他の便利な情報

3.8.1. セキュリティソリューションをテストする方法はありますか？

Bitdefenderが正常に動作しているか確認するには、Eicarテストを利用することをおすすめします。

Eicarテストは安全なテストファイルを使ってセキュリティソリューションの動作を確認することができます。

セキュリティソリューションをテストするには:

1. EICARの公式Webサイトからテストファイルを入手してください。 http://www.eicar.org/
2. Anti-Malware Testfileのタブを選択してください。
3. メニュー左側のDownloadを選択してください。
4. Download area using the standard protocol httpの項目内にあるeicar.comテストファイルを選択してください。
5. 製品が現在開こうとしているページにEICAR-Test-File （脅威ではない）が含まれていることを検知します。

   I understand the risks, take me there anywayをクリックするとBitdefenderが警告を表示し、脅威を検出したことをお知らせします。

   この動作についてより詳細な情報を表示する場合は詳細表示を選択してください。

Bitdefenderの通知が届かない場合は、「サポートを依頼」 (p. 317)に記載された手順でBitdefenderサポートまでご連絡ください。

3.8.2. Bitdefenderをアンインストール（削除）するには？

Bitdefender Total Security を削除したい場合: ▪

- Windows 7の場合 :
  1. スタート ボタンをクリックし、コントロール パネル を開きます。その中にある プログラムおよび機能 をダブルクリックします。
  2. Bitdefender Total Securityを探していただき、削除を選択してください。
  3. 表示されるウィンドウで 削除 をクリックします。
  4. アンインストール処理が完了するまで待ち、それからシステムを再起動します。
- Windows 8 および Windows 8.1:
  1. Windowsスタート画面からコントロールパネルを探して（またはスタート画面で「コントロールパネル」と入力して）、アイコンをクリックしてください。

2. プログラムのアンインストールまたはプログラムと機能をクリックしてください。
3. Bitdefender Total Securityを探していただき、削除を選択してください。
4. 表示されるウィンドウで 削除 をクリックします。
5. アンインストール処理が完了するまで待ち、それからシステムを再起動します。

- Windows 10の場合：
  1. 開始 をクリックし、続いて「設定」をクリックします。
  2. 設定エリアの システム アイコンをクリックし、インストールされているアプリケーション を選択します。
  3. Bitdefender Total Securityを探していただき、削除を選択してください。
  4. アンインストール をもう一度クリックして選択を確定します。
  5. 表示されるウィンドウで 削除 をクリックします。
  6. アンインストール処理が完了するまで待ち、それからシステムを再起動します。

注記
この再インストール手順を実行すると、カスタマイズした設定が完全に削除されます。

3.8.3. Bitdefender VPN を削除するには？

Bitdefender VPN を削除する方法は、コンピュータから他のプログラムを削除する方法とよく似ています:

- Windows 7の場合：
  1. スタート ボタンをクリックし、コントロール パネル を開きます。その中にある プログラムおよび機能 をダブルクリックします。
  2. Bitdefender VPNを探し、削除を選択してください。

     アンインストールのプロセスが完了するまでお待ちください。
- Windows 8 および Windows 8.1:

1. Windowsスタート画面からコントロールパネルを探して（またはスタート画面で「コントロールパネル」と入力して）、アイコンをクリックしてください。
2. プログラムのアンインストールまたはプログラムと機能をクリックしてください。
3. Bitdefender VPNを探し、削除を選択してください。

   アンインストールのプロセスが完了するまでお待ちください。

● Windows 10の場合：

1. 開始 をクリックし、続いて「設定」をクリックします。
2. 設定エリアの システム アイコンをクリックし、インストールされているアプリケーション を選択します。
3. Bitdefender VPNを探し、削除を選択してください。
4. アンインストール をもう一度クリックして選択を確定します。

   アンインストールのプロセスが完了するまでお待ちください。

3.8.4. 検査完了後、自動的にパソコンを終了させるには？

Bitdefenderは、パソコンが脅威に感染していないことを確認するために複数のスキャンタスクをご用意しています。 パソコン全体の検査は、パソコンのハードウェアやソフトウェア構成などによって、より多くの時間を要する場合があります。

このため、 Bitdefender は、設定から検査完了時に自動的にパソコンを終了させることが可能です。

例：パソコンでの作業が完了して、就寝の時間になった場合。 Bitdefenderでパソコン全体を検査して、脅威の感染がないか確認したい。

以下の手順でBitdefenderを設定すれば、検査完了時に自動的にパソコンを終了させることができます：

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護をクリックします。
2. アンチウイルス ウィンドウで、 スキャンの管理クリックします。
3. 検査タスクを管理 ウィンドウで新しいカスタムタスク をクリックしてスキャン名を入力し、スキャンする場所を選択します。

4. スキャンオプションを細かく設定する場合は、詳細設定 タブを選択します。
5. 検査が完了して脅威が見つからなかった場合、そのままパソコンを自動的に終了させるように設定します。
6. OK をクリックすると、変更が保存され、画面が自動で閉じます。
7. スキャン開始 をクリックしてスキャンを開始します。

脅威が検出されなかった場合は、パソコンが自動的に終了します。

対処されていない脅威がある場合は、処理を行うように促されます。 詳細については、「ウイルス対策 スキャン ウィザード」 (p. 91)をご参照ください。

3.8.5. プロキシを使用してインターネットへ接続するようにBitdefenderを設定するにはどうすれば良いのですか？

お使いのパソコンがプロキシ経由でインターネットへ接続している場合、Bitdefenderでもプロキシを設定する必要があります。 通常、Bitdefenderは、コンピュータ内のプロキシ設定を自動的に検出し、その設定をインポートします。

重要項目
一般的な家庭のインターネット接続は、プロキシサーバーを使用しません。アップデートが正常に動作しない場合は、まずはBitdefenderのプロキシ接続設定を確認することをおすすめします。 Bitdefenderが正常にアップデートできる場合は、インターネット接続の設定は正しく行なわれています。

プロキシ設定を管理するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. 詳細設定 タブを選択します。
3. プロキシサーバー をオンにします。
4. プロキシ変更 をクリックします。
5. プロキシを設定するには、2つ選択肢があります :
   - デフォルトブラウザからプロキシ設定をインポートする - デフォルト設定されているブラウザから現在のユーザーのプロキシ設定を抽出します。 プロキシサーバーでユーザー名とパスワードの入力が必要な場合、該当する各項目を記入する必要があります。

注記
Bitdefender は、Microsoft Edge、Internet Explorer、Mozilla Firefox、および Google Chrome の最新版を含むほとんどのブラウザからプロキシ設定をインポートできます。

- カスタム プロキシ設定 - 自分で設定することができるプロキシ設定。以下の設定を指定してください：
  - アドレス - プロキシサーバのIPアドレスを入力します。
  - ポート - プロキシ サーバへの接続時に Bitdefender が使うポートを入力します。
  - ユーザ名 - プロキシによって認識されるユーザ名を入力します。
  - パスワード - 先に指定したユーザの有効なパスワードを入力します。

6. OK をクリックすると、変更が保存され、画面が自動で閉じます。

Bitdefenderは、インターネットに接続ができるまで、有効なプロキシ設定を使用します。

3.8.6. 使用している Windows のバージョン（32bit・64bit）の確認方法は？

お使いのオペレーティングシステムが 32 ビットか 64 ビットのどちらかを確認するには:

- Windows 7の場合：
  1. スタート をクリックしてください。
  2. スタート メニューから、コンピュータ を探してください。
  3. コンピュータ を右クリックし、プロパティ を選択します。
  4. システム情報を確認するには システム の下をご覧ください。
- Windows 8の場合：
  1. Windowsスタート画面からコンピュータを探して（またはスタート画面で「コンピュータ」と直接入力して）、アイコンを右クリックしてください。

     Windows 8.1 で この PC を参照します。
  2. メニュー下部のプロパティを選択してください。
  3. システムエリアで、システムのタイプを確認します。

● Windows 10の場合：

1. タスクバーの検索ボックスに「システム」と入力し、アイコンをクリックします。
2. システムエリアで、システムのタイプに関する情報を確認します。

3.8.7. Windows で隠し属性のファイルを表示するには？

これらは、感染したファイルや隠しファイルを検出・削除する必要がある場合に、有効な手順です。

隠し属性のファイルを表示するには、これらの手順に従って下さい：

1. スタートを選択して、コントロールパネルを選択してください。

   Windows 8 または Windows 8.1 :Windowsのスタート画面から コントロール パネル にアクセスし（スタート画面に ”コントロール パネル”と直接入力する方法も可)、アイコンをクリックします。

2. フォルダオプションを選択してください。
3. 表示 タブを開きます。
4. すべてのファイルとフォルダを表示する （Vista、Windows7では「隠しファイル、隠しフォルダー、および隠しドライブを表示する」）を選択します。
5. 登録されている拡張子は表示しないのチェックボックスのチェックを外してください。
6. 保護されたオペレーティング システム ファイルを表示しない のチェックを外します。
7. 適用 をクリックし、続いて OK をクリックします。

Windows 10の場合：

1. タスクバーの検索ボックスに「隠しファイルとフォルダを表示」と入力し、アイコンをクリックします。
2. 隠しファイル、フォルダ、ドライブを表示する を選択します。
3. 登録されている拡張子は表示しないのチェックボックスのチェックを外してください。
4. 保護されたオペレーティング システム ファイルを表示しない のチェックを外します。
5. 適用 をクリックし、続いて OK をクリックします。

3.8.8. 他のセキュリティソフトはどうやって削除するのですか？

セキュリティ対策ソフトを使用する主な理由は、コンピュータを保護し、データを安全にするためです。 しかし、同一システム上に複数のセキュリティ製品があるとどのようなことが起こるでしょうか？

同じコンピュータで別のセキュリティソフトを使用すると、システムが不安定になります。 Bitdefender Total Security インストーラは他のセキュリティ製品を自動的に検出し、それらのアンインストールを案内します。

初回インストール時に他のセキュリティソリューションを削除しなかった場合:

- Windows 7の場合：
  1. スタート ボタンをクリックし、コントロール パネル を開きます。その中にある プログラムおよび機能 をダブルクリックします。
  2. インストールされているソフトウェアの一覧が表示されるまで、少々お待ち下さい。
  3. 削除するプログラム名を探し、アンインストール を選択してください。
  4. アンインストール処理が完了するまで待ち、それからシステムを再起動します。
- Windows 8 および Windows 8.1:
  1. Windowsスタート画面からコントロールパネルを探して（またはスタート画面で「コントロールパネル」と入力して）、アイコンをクリックしてください。
  2. プログラムのアンインストールまたはプログラムと機能をクリックしてください。
  3. インストールされているソフトウェアの一覧が表示されるまで、少々お待ち下さい。
  4. 削除するプログラム名を探し、アンインストール を選択してください。
  5. アンインストール処理が完了するまで待ち、それからシステムを再起動します。
- Windows 10の場合：

1. 開始 をクリックし、続いて「設定」をクリックします。
2. 設定エリアの システム アイコンをクリックし、インストールされているアプリケーション を選択します。
3. 削除するプログラム名を探し、アンインストール を選択してください。
4. アンインストール をもう一度クリックして選択を確定します。
5. アンインストール処理が完了するまで待ち、それからシステムを再起動します。

コンピュータから他のセキュリティ対策製品を削除できない場合は、その製品のウェブサイトからアンインストール ツールを取得するか、その製品のサポートに直接連絡して、アンインストール方法についてお問い合わせください。

3.8.9. セーフモードでパソコンを再起動させる方法は？

セーフモードはWindowsで起きた問題の調査を行うときに使用するモードです。主にWindowsの通常モードで影響する問題の解決に使用されます。 この問題はドライバのコンフリクトから脅威によるWindowsの通常起動の妨げまで幅広いものとなります。 セーフ モードで動作しているアプリケーションはごくわずかで、Windows は基本構成のドライバと、最低限の OS コンポーネントのみを読み込みます。 殆どの脅威が Windows がセーフ モードのときに活動しないのはそのためで、簡単に削除することができます。

Windows をセーフ モードで開始する：

- Windows 7の場合：
  1. コンピュータを再起動してください。
  2. Windows が起動される前に、コンピュータの電源投入直後にキーボードの F8 キーを何回か押して、Windows のブート メニューを開きます。
  3. 起動メニューからセーフモードを選択してください。インターネット接続も必要な場合は、セーフモードとネットワークを選択してください。
  4. Enterを押し、Windowsがセーフモードで起動するのをお待ちください。
  5. この作業は、確認メッセージで終了となります。 確認し、OKを選択してください。
  6. Windows を通常起動するには、再起動を行ってください。

- Windows 8、Windows 8.1、および Windows 10:

  1. Windows で システム設定 を起動するには、キーボードで Windows + R キーを同時押しします。
  2. 開く ダイアログボックスで msconfig と入力し、OK をクリックします。
  3. 起動 タブを選択します。
  4. 起動オプションエリアで セーフブート チェックボックスを選択します。
  5. ネットワーク をクリックしてから OK をクリックします。
  6. 変更内容を反映するには、システム設定 ウィンドウで OK をクリックします。

     システムが「セーフモードとネットワーク」で再起動します。

  通常モードで再起動するには、システム操作 を再度起動し、セーフブート チェックボックスのチェックを外します。 OK をクリックしてから 再起動 をクリックします。 新しい設定が反映されるまでお待ちください。

4. セキュリティを管理する

4.1. ウイルス対策

Bitdefender は、あらゆる種類の脅威（マルウェア、トロイの木馬、スパイウェア、ルート キット 等）からコンピュータを保護します。 Bitdefender が提供する保護機能は、2 つのカテゴリで構成されています。

- リアルタイム保護 – パソコンを脅威の侵入から守ります。 例えば Bitdefenderは、WORD文書を開いた時に既知の脅威を対象に文書をスキャンします。メールの場合は受信時にスキャンを行します。

  リアルタイム保護機能は、脅威からの継続的な保護を提供する、セキュリティ対策ソフトには欠かせない機能です。

  重要項目
  パソコンを脅威の感染から保護するためにリアルタイム保護 を常に有効にしておいてください。

- 手動検査 – システム内に存在する脅威を検出および駆除することができます。 これはユーザの要求に応じて実行される従来のスキャン方式です。（ Bitdefender がスキャンするドライブ、フォルダ、ファイルをユーザが指定するため、「手動」と呼んでいます。 Bitdefender はユーザが指定したものをスキャンします。）

Bitdefenderは、パソコンに接続されたリムーバブル メディアを自動的に検査し、安全かどうかを確認します。 詳細については、「外付けメディアの自動スキャン」 (p. 95)をご参照ください。

特定のファイルや特定の種類のファイルを検査しないように設定したい場合は、スキャン例外設定から行うことができます。 詳細については、「スキャン例外を設定する」 (p. 97)をご参照ください。

脅威を検出すると、 Bitdefender は、感染したファイルから自動的に悪意のあるコードを取り除き、元のファイルに再構成しなおします。 この操作は、'駆除' と呼ばれます。 '駆除'ができないファイルについては、感染の可能性があるため、'隔離領域'に移動させます。 詳細については、「隔離されたファイルの管理」 (p. 99)をご参照ください。

コンピュータが脅威に感染している場合は、「パソコンからウイルスを駆除する」をご参照ください。「パソコンから脅威を駆除する」 (p. 203) Windows オペレーティングシステムから削除できない脅威をコンピュータ

から駆除する必要がある場合、 Bitdefender では 「Bitdefender レスキューモード (Windows 10 のレスキュー環境)」 (p. 204) を利用することができます。 これは脅威を削除するために準備された信頼できる環境で、Windowsを使わずにパソコンを起動できるようにします。 コンピュータをレスキューモード (Windows 10 ではレスキュー環境) で起動すると、Windowsの脅威は非アクティブな状態になるため、容易に駆除することができます。

4.1.1. リアルタイム保護

Bitdefender は、ファイルへのすべてのアクセスおよびメールメッセージをスキャンすることで、あらゆる脅威に対する継続的なリアルタイム保護を提供します。

リアルタイム保護を有効または無効にする

脅威に対するリアルタイム保護をオン/オフにするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. ウイルス対策 パネルで 隔離フォルダ をクリックします。
3. シールド ウィンドウで Bitdefender シールド をオン/オフにします。
4. リアルタイム保護を無効にする場合、警告ウィンドウが表示されます。メニューから、リアルタイム保護機能を無効にする時間を選択し、内容を確認します。 リアルタイム保護は 5 分、15分、30 分、1 時間、無制限、あるいはシステムの次回再起動まで無効にできます。 選択した時間が経過すると、リアルタイム保護は自動的に有効になります。

警告
これは緊急レベルのセキュリティ問題です。 リアルタイム保護を無効にする場合は、期間をなるべく短めにすることをおすすめします。 リアルタイム保護が無効になっていると、パソコンは脅威から保護されません。

リアルタイム保護の高度な設定を行う

上級者の方向けに、 Bitdefender が提供するウイルス検査設定をさらに活用する方法があります。 カスタム保護レベルを作成することで、リアルタイム保護設定を詳細に構成できます。

リアルタイム保護の詳細設定を編集するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. ウイルス対策 パネルで 隔離フォルダ をクリックします。
3. シールド ウィンドウで 詳細設定を表示 アコーディオンメニューをクリックします。

   ペインで分割されたウィンドウが表示されます。
4. ウィンドウを下にスクロールし、必要に応じてスキャンの設定を行います。

検査オプションの詳細

以下に、詳細な情報を記載します。

- アプリケーションのみを検査. アクセスしたアプリのみをスキャンするよう Bitdefender を設定できます。
- 望ましくない可能性があるアプリケーションをスキャン. 不要なアプリケーションをスキャンする場合は、このオプションを選択します。 望ましくない可能性があるアプリケーション（PUA）または望ましくない可能性があるプログラム（PUP）は通常、フリーソフトウェアと一緒にバンドルされ、ポップアップ広告を表示したり、デフォルトのブラウザにツールバーをインストールしたりします。 そのうちのいくつかは、ホームページや検索エンジンを変更し、またバックグラウンドで複数のプロセスを実行して PC の速度を低下させたり、多数の広告を表示したりします。 これらのプログラムは、お客様の同意なしにインストールすることができるか（アドウェアとも呼ばれます）、もしくはデフォルトでエクスプレスインストールキット（広告入り）に含まれています。
- ネットワーク共有を検査する. コンピュータからリモートネットワークに安全にアクセスするために、ネットワーク共有をスキャンするオプションは有効にしておくことをお勧めします。
- アーカイブ（圧縮ファイル）内部を検査. アーカイブ内部のスキャンには、時間と高いリソースを必要とします。そのため、リアルタイム保護での実行は推奨していません。 感染したファイルが含まれているアーカイブは、システムへの差し迫った脅威とはなりません。 リアルタイム保護機能が有効になっていない時に、アーカイブから感染ファイルを解凍し、実行した時のみ、脅威はコンピュータに影響を及ぼします。

  このオプションを使用する場合は、オプションをオンにしてから、スライダーを動かしてリアルタイムスキャン時の最大アーカイブサイズ（MB）を設定します。

- メールをスキャン. 脅威がコンピュータにダウンロードされるのを防ぐため、 Bitdefender は送受信メールを自動的にスキャンします。

  お勧めはできませんが。メールの脅威機能を無効にすることで、システムのパフォーマンスを向上することは可能です。 対応するスキャンオプションを無効にすると、受信メールおよびファイルはスキャンされず、感染ファイルをコンピュータに保存することが可能になります。 しかし感染したファイルにアクセス（開く・移動・コピー・実行）した時に、リアルタイム保護機能が脅威をブロックするため、それほど重大な脅威にはなりません。

- ブートセクタを検査. ハードディスクのブート セクタをスキャンするよう Bitdefender を設定できます。 ハードディスクのこのセクタには、起動プロセスを開始するために必要なコンピュータ コードが含まれています。 脅威がブート セクタに感染すると、通常、そのドライブにはアクセスできなくなり、システムを起動させることも、データへのアクセスもできなくなります。

- 新しいファイルと変更されたファイルのみスキャン. 新規または変更されたファイルのみをスキャンすることで、セキュリティへの影響を最小限に抑えながら、システム全体のレスポンスを改善します。

- キーロガーを検査の対象にする. キーロガーのアプリケーションの有無を検査する場合は、こちらのオプションを選択してください。 キーロガーはキーボードで入力された情報を記録し、これらの情報をユーザーに気づかれないようにインターネット上の攻撃者（ハッカーなど）へ送信します。 ハッカーは盗んだデータから重要な情報（銀行の口座番号とパスワードなど）を見つけ、それを使って資産を取得します。

- システム起動時にスキャン. 早期ブートスキャン オプションを選択した場合、システム起動時に重要なサービスの読み込みが完了すると、直ちにシステムスキャンが実施されます。 この機能の目的は、システム起動時の脅威の保護を強化し、システムの起動時間を短縮することです。

検知した脅威に対する処理

リアルタイム保護機能によって実行されるアクションは、次の手順で設定できます:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. ウイルス対策 パネルで 隔離フォルダ をクリックします。

3. シールド ウィンドウで 詳細設定を表示 アコーディオンメニューをクリックします。

   ペインで分割されたウィンドウが表示されます。

4. 脅威アクションオプションが表示されるまで、ウィンドウを下にスクロールします。

5. スキャン設定を構成します。

Bitdefender のリアルタイム保護によって、次のアクションを実行できます:

自動駆除（削除）

Bitdefenderは検出されたファイルの種類にあわせて、推奨された処理を行ないます：

- 感染したファイル. 「感染」として判定されたファイルは、Bitdefender 脅威情報データベース内にあるパターンと合致したファイルです。 Bitdefender は、自動的に悪意のあるコードを感染したファイルから削除し、削除後に元のファイルの再構成を試みます。この操作は、'駆除' と呼ばれます。

  '駆除'ができないファイルについては、感染の可能性があるため、'隔離領域'に移動させます。 隔離されたファイルは実行されることも開かれることもありません。そのためそれ以上感染が広がるリスクはありません。 詳細については、「隔離されたファイルの管理」 (p. 99)をご参照ください。

  重要項目

  脅威の種類によっては、ファイルの一部が感染しているのではなく、ファイル全体が悪意あるコードで書かれているため、駆除できないものもあります。 このような場合、感染したファイルはディスクから完全に削除されます。

- 疑わしいファイル. ヒューリスティック分析により疑いあるものとして検出されたファイルです。 疑わしいファイルに対しては、駆除する方法がないため、駆除を行うことができません。 これらのファイルは感染を防ぐため、隔離フォルダへ移動されます。

  初期設定では、隔離されたファイルは自動的に Bitdefender のラボに送付され、 Bitdefender のリサーチャーによって解析されます。脅威の存在が確認された場合、その脅威を削除するために必要となる脅威情報データベースがリリースされます。

- 感染したファイルを含むアーカイブ.
  - 感染したファイルしか含まれていないアーカイブは自動的に削除されます。
  - 感染したファイルと正常なファイル両方が含まれるアーカイブがあった場合、 Bitdefender は感染したファイルのみを削除するように試みます（正常なファイルでアーカイブを再構成できる場合のみ）。 アーカイブの再構成ができない場合は、正常なファイルを失ってしまわないよう、対処することができないという警告が表示されます。

隔離フォルダへ移動
感染ファイルを隔離領域へ移動します。 隔離されたファイルは実行されることも開かれることもありません。そのためそれ以上感染が広がるリスクはありません。 詳細については、「隔離されたファイルの管理」(p. 99)をご参照ください。

アクセス拒否
感染ファイルが検出された場合にはこのファイルへのアクセスは拒否されます。

初期設定へ戻す

デフォルトのリアルタイム保護設定で、システム パフォーマンスへの影響を最小限に抑えつつ、脅威に対して優れた保護機能を実現します。

デフォルトのリアルタイム保護設定を復元：

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. ウイルス対策 パネルで 隔離フォルダ をクリックします。
3. シールド ウィンドウで 詳細設定を表示 アコーディオンメニューをクリックします。

   ペインで分割されたウィンドウが表示されます。
4. 設定をリセットオプションが表示されるまで、ウィンドウを下にスクロールします。 アンチウイルスの設定をデフォルトの状態にリセットするには、このオプションを選択します。

4.1.2. オンデマンドスキャン（手動スキャン）

Bitdefenderの主な目的はパソコンを脅威から守り、安全な状態を保つことです。　これらは新しい脅威の感染を防いだり、送受信されたメールを検査、ダウンロードした新しいファイルを検査することで実現しています。

Bitdefenderをインストールする前からすでに脅威がパソコンに潜んでいるというリスクもあります。　このためBitdefenderをインストールしたら、すぐにパソコン全体の脅威の検査を行うことをおすすめしています。 またインストール直後だけではなく、定期的にパソコン全体の脅威検査を行うこともおすすめいたします。

手動検査の設定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、ウイルス検査の各種オプションや、検査対象を指定します。 デフォルト（初期設定）の検査タスク、あるいはユーザーが設定した独自の検査タスクを実行すれば、いつでもパソコンのウイルス検査が行なえます。 パソコン上の特定の場所を検査する場合は、カスタム　スキャン　タスクを設定して実行します。

ファイルまたはフォルダの脅威検査

感染が疑われるファイル/フォルダは、必ずスキャンしてください。　検査するファイルまたはフォルダを右クリックし、右クリックメニュー内のBitdefenderにカーソルを当て、Bitdefenderで検査を選択してください。 ウイルス対策 スキャン ウィザード で、スキャン手順についての案内が表示されます。 検査の完了後、ウイルス検知があった場合、検知されたファイルの処理方法を選択するように促されます。

クイック検査を実行する

クラウドのスキャン技術を使って、システムで動作している脅威を検出します。　クイック　スキャンは、通常、1分もかかりません。また、通常のウィルス　スキャンに比べ、ごくわずかなシステム　リソースしか消費しません。

クイック スキャンを実行するには:

1. Bitdefender　インターフェイスのナビゲーションメニューにある　保護　をクリックします。
2. アンチウイルスウィンドウで、 クイックスキャンをクリックします。
3. ウイルス対策 スキャン ウィザードに従い、検査を完了させてください。 Bitdefenderは検出したファイルに対して、推奨された対処法をとりま

す。　対処されていない脅威がある場合は、処理を行うように促されます。

パソコン全体の検査を実行する

パソコン全体の検査はマルウェア、スパイウェア、アドウェア、ルートキットなど、あらゆる脅威を検査します。

> **注記**
> パソコン全体の検査はシステム全体を徹底的に検査するため、検査に時間がかかる場合があります。 このため、このタスクはなるべくパソコンを使用していない時に実行することをおすすめします。

パソコン全体の検査を実行する前に以下を行うことをおすすめします：

- Bitdefender　の脅威情報データベースが最新であることを確認してください。 古い脅威情報データベースを使用してパソコンを検査している場合、 Bitdefender　が最新の脅威を検出できない可能性もあります。 詳細については、「Bitdefender　を最新の状態に保つ」 (p. 37)をご参照ください。
- 起動中のプログラムをすべて終了する。

パソコン上の特定の場所を検査する場合には、カスタム　スキャン　タスクを設定して実行します。　詳細については、「カスタム検査を設定する」 (p. 87)をご参照ください。

システム スキャンを実行するには:

1. Bitdefender　インターフェイスのナビゲーションメニューにある　保護をクリックします。
2. アンチウイルスウィンドウで、 システムスキャンをクリックします。
3. 「パソコン全体の検査」機能に初めてアクセスすると、機能の紹介が表示されます。 わかりました。 をクリックして続行します。
4. ウイルス対策 スキャン ウィザードに従い、検査を完了させてください。 Bitdefenderは検出したファイルに対して、推奨された対処法をとります。　対処されていない脅威がある場合は、処理を行うように促されます。

カスタム検査を設定する

カスタムスキャンを細かく設定して実行するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. アンチウイルス ウィンドウで、 スキャンの管理クリックします。
3. 新しいカスタムタスク をクリックします。 基本設定 ウィンドウでスキャンの名前を入力し、スキャンする場所を選択します。
4. スキャンオプションを細かく設定する場合は、詳細設定 タブを選択します。 新しいウィンドウが表示されます。 次の手順に従ってください：
   a. スキャンレベルを調整することで簡単に検査のオプションを設定することができます。 スライダーをドラッグして、お好みの検査レベルに設定します。 スライダーを動かすと、その右側に説明が表示されますので、最適なレベルを選択してください。

      上級者の方向けに、 Bitdefender が提供するウイルス検査設定をさらに活用する方法があります。 検査オプションを細かく設定する場合は、カスタムを選択してください。 こちらの詳細については本セクションの最後で説明されています。
   b. 以下のオプションを構成できます：
      - タスクを低優先度で実行 . スキャン処理の優先度を下げます。 他のプログラムの実行速度を優先するため、スキャンにかかる時間が長くなります。
      - 検査画面をシステムトレイに格納 . 検査画面をタスクトレイ内に最小化して格納します。 Bitdefenderアイコンをダブルクリックして開きます。
      - 脅威が発見されなかった場合に行う処理を指定
   c. OK をクリックすると、変更が保存され、画面が自動で閉じます。
5. 基本 ウィンドウの スケジュール スイッチを使って、スキャンタスクのスケジュールを設定できます。 スケジュールを設定するには、該当のいずれかのオプションを選択:
   - システム起動後に実行
   - 1 回のみ実行
   - 定期的に実行
6. ウイルス検査を開始 をクリックし、ウイルス対策 スキャンウィザードの手順に従ってスキャンを完了してください。 検査する場所によっては

時間がかかる場合があります。 検査の完了後、ウイルス検知があった場合、検知されたファイルの処理方法を選択するように促されます。

7. 利用可能なリストから該当する項目をクリックすることで、前回のスキャンを必要に応じてすばやく再実行することができます。

検査オプションの詳細

以下に、詳細な情報を記載します。

- 不明な用語がある場合は、こちら をクリックしてください。（用語集を開きます。） またインターネット検索でも、役立つ情報を見つけることができます。
- スキャンファイル. Bitdefenderは、すべての種類のファイルを検査するように設定したり、アプリケーション（プログラムファイル）のみを検査するように設定することもできます。 全てのファイルをスキャンすることで最高の保護が実現できます。一方、アプリケーションのみをスキャンすることで、迅速なスキャンが実行できます。

  アプリ （もしくはプログラムファイル） は、他の種類のファイルと比較すると、マルウェアの攻撃に対して非常に脆弱です。 このカテゴリは、以下のファイル拡張子を含みます： 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsm; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp
- アーカイブ用の検査オプション. 感染したファイルが含まれているアーカイブは、システムへの差し迫った脅威とはなりません。 リアルタイム保護機能が有効になっていない時に、アーカイブから感染ファイルを解

凍し、実行した時のみ、脅威はコンピュータに影響を及ぼします。 しかし、すぐに脅威となるものではなくても、全ての潜在的な脅威を検出・駆除するために、このオプションを使用することを推奨します。

注記
アーカイブのスキャンはスキャン時間を増加させ、より多くのシステムリソースを必要とします。

- ブートセクタを検査. ハードディスクのブート セクタをスキャンするよう Bitdefender を設定できます。 ハードディスクのこのセクタには、起動プロセスを開始するために必要なコンピュータ コードが含まれています。 脅威がブート セクタに感染すると、通常、そのドライブにはアクセスできなくなり、システムを起動させることも、データへのアクセスもできなくなります。
- メモリを検査. システムのメモリ上で動作しているプログラムを検査する場合は、こちらのオプションを選択してください。
- レジストリを検査. レジストリキーを検査する場合は、このオプションを選択します。 WindowsレジストリはWindows OSのコンポーネントや、インストールされているアプリケーションの構成設定やオプションなどを保存したデータベースです。
- Cookieを検査. ブラウザによってパソコンへ保存された Cookie を検査する場合は、こちらのオプションを選択します。
- 新規および変更ファイルのみ検査. 新規または変更されたファイルのみをスキャンすることで、セキュリティへの影響を最小限に抑えながら、システム全体のレスポンスを改善します。
- キーロガーを検査しない. 一般的なキーロガー機能を持つソフトウェアをパソコンに導入している場合、こちらのオプションを選択してください。 市販のキーロガーとは、パソコンを監視する正当なアプリケーションを指します。アプリケーションの基本的な機能として、キーボードからの入力を記録するという機能を備えています。
- ルートキットを検査の対象にする. ルートキットなどのアプリケーションによって隠蔽されたオブジェクトを検査する場合はこちらのオプションを選択します。
- 望ましくない可能性があるアプリケーションをスキャン. 不要なアプリケーションをスキャンする場合は、このオプションを選択します。 望ましくない可能性があるアプリケーション (PUA) または望ましくない可能性があるプログラム (PUP) は通常、フリーソフトウェアと一緒にバンド

ルされ、ポップアップ広告を表示したり、デフォルトのブラウザにツールバーをインストールしたりします。　そのうちのいくつかは、ホームページや検索エンジンを変更し、またバックグラウンドで複数のプロセスを実行して PC の速度を低下させたり、多数の広告を表示したりします。 これらのプログラムは、お客様の同意なしにインストールすることができるか（アドウェアとも呼ばれます）、もしくはデフォルトでエクスプレスインストールキット（広告入り）に含まれています。

ウイルス対策 スキャン ウィザード

手動検査を実行した場合（例：フォルダを右クリックし、Bitdefenderにカーソルを当ててBitdefenderで検査を選択した場合）、Bitdefenderスキャン ウィザード画面が表示されます。 ウィザードの手順に従って、検査を完了させてください。

注記

スキャンウィザードが表示されない場合には、スキャンがバックグラウンドで実行されるように設定されています。 スキャンが進行していることを表すアイコンが システム トレイ にあります。 このアイコンをクリックすると、スキャンの状態を確認する画面が開きます。

手順1 - 検査を実行

Bitdefenderは選択したオブジェクトのスキャンを開始します。　検査の状況に関する情報をリアルタイムで確認することができます（検査開始から経過した時間、完了までの残り時間、検知された脅威の数など）。

Bitdefender がスキャンを完了するまでお待ちください。 スキャンの内容によっては処理に時間がかかる場合があります。

スキャンを停止または一時停止: スキャンは 停止 をクリックすることでいつでも停止できます。 ウィザードの最終手順へ直接進みます。 一時的に検査を停止させる場合は一時停止をクリックしてください。　再開をクリックすると検査を再開します。

パスワード保護されたアーカイブ: パスワード保護されたアーカイブが検出されると、スキャン設定によっては、パスワードの入力を求められる場合があります。 パスワードで保護されたアーカイブについては、パスワードを入力しない限り、スキャンすることはできません。 以下のオプションを利用できます：

- パスワード. Bitdefender にこのアーカイブをスキャンさせる場合は、このオプションを選択してパスワードを入力します。 パスワードが分からない場合は、他のオプションを選択してください。
- パスワードを入力せず、このファイルのウイルス検査をスキップする。. このアーカイブに対するスキャンをスキップします。
- スキャンを行わないで、パスワード保護されている全ての項目をスキップします: パスワード保護されたアーカイブに対して、パスワード入力を全て無視する場合は、このオプションを選択します。 Bitdefenderはそれらをスキャンできませんが、ログファイルに記録が残ります。

希望するオプションを選択し、OKをクリックして検査を続行します。

手順 2 - 処理を選択

検査の完了後、ウイルス検知があった場合、検知されたファイルの処理方法を選択するように促されます。

注記

クイックスキャンまたはシステムスキャンの実行時、 Bitdefender はスキャン中に検出されたファイルに対して推奨されるアクションを自動的に実行します。 対処されていない脅威がある場合は、処理を行うように促されます。

感染したオブジェクトは感染した脅威に基づくグループごとに表示されます。 詳細な情報については、検出された脅威に対応するリンクを開きます。

すべての問題に対して一括した処理を行うか、もしくは個々の問題のグループごとに個別の処理を行うかを選択できます。 1つまたは複数のオプションがメニューで表示されます:

自動駆除（削除）

Bitdefenderは検出されたファイルの種類にあわせて、推奨された処理を行ないます:

- 感染したファイル. 「感染」として判定されたファイルは、Bitdefender 脅威情報データベース内にあるパターンと合致したファイルです。 Bitdefender は、自動的に悪意のあるコードを感染したファイルから削除し、削除後に元のファイルの再構成を試みます。この操作は、'駆除' と呼ばれます。

  '駆除'ができないファイルについては、感染の可能性があるため、'隔離領域'に移動させます。 隔離されたファイルは実行されることも開

かれることもありません。そのためそれ以上感染が広がるリスクはありません。 詳細については、「隔離されたファイルの管理」 (p. 99)をご参照ください。

重要項目
脅威の種類によっては、ファイルの一部が感染しているのではなく、ファイル全体が悪意あるコードで書かれているため、駆除できないものもあります。 このような場合、感染したファイルはディスクから完全に削除されます。

- 疑わしいファイル. ヒューリスティック分析により疑いあるものとして検出されたファイルです。 疑わしいファイルに対しては、駆除する方法がないため、駆除を行うことができません。 これらのファイルは感染を防ぐため、隔離フォルダへ移動されます。

  初期設定では、隔離されたファイルは自動的に Bitdefender のラボに送付され、 Bitdefender のリサーチャーによって解析されます。脅威の存在が確認された場合、その脅威を削除するために必要となる脅威情報データベースがリリースされます。

- 感染したファイルを含むアーカイブ.
  - 感染したファイルしか含まれていないアーカイブは自動的に削除されます。
  - 感染したファイルと正常なファイル両方が含まれるアーカイブがあった場合、 Bitdefender は感染したファイルのみを削除するように試みます（正常なファイルでアーカイブを再構成できる場合のみ）。 アーカイブの再構成ができない場合は、正常なファイルを失ってしまわないよう、対処することができないという警告が表示されます。

削除
検出したファイルをディスクから削除します。

感染したファイルが正常なファイルと一緒にアーカイブされている場合、 Bitdefender は感染したファイルのみを削除し、アーカイブの再構成を試みます。 アーカイブの再構成ができない場合は、正常なファイルを失ってしまわないよう、対処することができないという警告が表示されます。

処理しない
検出したファイルに対して処理を実行しません。 スキャン完了後、スキャンログを開いてこれらのファイルの情報をみることができます。

指定した処理を適用するには、続ける をクリックします。

手順 3 - 結果の確認

Bitdefender による問題の修正が終了すると、スキャン結果が新しい画面に表示されます。 スキャン処理に関する内容を参照する場合は、ログを表示 をクリックし、スキャン ログを確認してください ログは .xml 形式で提供され、ログを保存 ボタンをクリックして保存場所を選択することで、ローカルに保存することができます。

重要項目

殆どの場合、Bitdefender は検出した感染ファイルの駆除や隔離を正常に行います。 しかし、自動では解決できない問題もあります。 削除処理を完了するために必要に応じてシステムを再起動してください。 手動で脅威を駆除する方法や説明については、「パソコンから脅威を駆除する」 (p. 203) をご参照ください。

検査ログを確認

スキャンを実行する毎にスキャンログが作成され、 Bitdefender は検出された問題を「アンチウイルス」ウィンドウに記録します。 スキャン ログには、スキャン オプション、スキャン対象、検出された脅威、実行した処理など、スキャン処理に関する詳細情報が記載されています。

スキャンが完了すると、スキャン ウィザードから、スキャン ログを開くことができます。ログを表示 をクリックしてください。

スキャンログや検出された脅威を後でチェックするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 通知 をクリックします。
2. 全て タブで、最新のスキャンに関する通知を選択します。

   ここでは、アイドルスキャンで検知した脅威や、ユーザーが実行した検査、リアルタイム保護のステータス変更など、ウイルス検査のすべてのイベントを確認することができます。
3. 通知リストでは、最近実行したスキャンを確認できます。 通知をクリックするとその詳細が表示されます。
4. 検査ログを表示するには、ログを表示をクリックします。

4.1.3. 外付けメディアの自動スキャン

Bitdefender は、コンピュータに接続されたリムーバブルストレージデバイスを自動的に検出し、自動スキャンオプションが有効になっている場合は、バックグラウンドでデバイスのスキャンを実行します。 これは、コンピュータを脅威の感染から保護するための動作です。

以下のカテゴリのデバイスが検出されます。

- CD / DVD
- USB ストレージ デバイス（USBメモリや、外付けハードドライブなど）
- マップされた（リモート）ネットワーク ドライブ

自動スキャンは、ストレージデバイスの種類ごとに設定することができます。 ネットワークドライブの自動スキャンは、初期設定で無効になっています。

どのような仕組みですか？

リムーバブルストレージデバイスを検出した場合、 Bitdefender はバックグラウンドで脅威スキャンを実行します（接続されたデバイスの自動スキャンが有効の場合のみ）。 新しいデバイスが検出され、検査の実行をポップアップウィンドウで通知します。

Bitdefender スキャン アイコンが システムトレイ に表示されます。このアイコンをクリックすると、スキャンの状態を確認する画面が開きます。

検査が完了すると、検査の結果画面が表示され、リムーバブル メディア内のファイルを安全に開くことができるか通知されます。

ほとんどの場合、 Bitdefender は検知した脅威を自動的に削除するか、感染したファイルを隔離フォルダへ移動します。 検査完了後に、対処されていない脅威がある場合は、処理を行うように促されます。

> **注記**
> CDやDVD内に検出された疑わしいファイルは対処することはできません。 またネットワークドライブなどで検出されたウイルスや疑わしいファイルに関しても、権限がない場合は対処することができません。

次の情報を参考にしてください：

- 脅威情報を含むCDやDVDなどで操作を行う場合はご注意ください。ディスクにある脅威は（メディアが読み取り専用のため）削除することができません。 脅威がシステムへ感染しないよう、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。 重要なデータはディスクからシステムにコピーし、コピー完了後にディスクを廃棄することを推奨しています。

- 場合によってはBitdefenderは、法律上の制限や技術的制限のため、脅威をファイルから削除できない可能性があります。 特殊技術を用いて圧縮されたアーカイブファイルなどが1つの例です（アーカイブを最再構築することができないため）。

  脅威への対処方法については 「パソコンから脅威を駆除する」（p. 203）を参照してください。

外付けのメディア検査を管理する

リムーバブルメディアの自動スキャンを管理するには:

最適な保護のために、すべての種類のリムーバブルストレージデバイスに対して 自動スキャン オプションを有効にすることをお勧めします。

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. ウイルス対策 パネルで 隔離フォルダ をクリックします。
3. ドライブとデバイス タブを選択します。

スキャン オプションは、最高の検出結果を得られるように事前に設定されています。 ウイルスに感染したファイルが検出された場合、 Bitdefenderはファイルの駆除（悪意のあるコードの除去）を試み、駆除できない場合は隔離フォルダへ移動します。 どちらの対処も行なえなかった場合は、スキャン ウィザードが別の対処法を選択するように促します。 スキャン オプションは基本機能であるため、変更することはできません。

4.1.4. Hostsファイルのスキャン

Hosts ファイルはオペレーティングシステムに標準で含まれており、新しい Web ページにアクセスしたり、FTP やその他のインターネットサービスに接続するたびにホスト名を IP アドレスにマッピングする役割を果たします。 これはプレーンテキストファイルで、悪意のあるプログラムによって改変される可能性があります。 上級ユーザーは、これを使って不要な広告や第三者のcookie、ハイジャッカーなどをブロックすることができます。

スキャンホストファイルを設定するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。

2. 詳細設定 タブを選択します。
3. Hostsファイルのスキャンをオン/オフにします。

4.1.5. スキャン例外を設定する

Bitdefenderでは、特定のファイル、フォルダ、ファイル拡張子をスキャンから除外することができます。 本機能はユーザーのパソコン作業を妨げずに、システムのパフォーマンスを向上させることを目的として実装されています。 例外の設定は、パソコンの知識をお持ちの方、または Bitdefender サポート担当者のアドバイスをもとに行うことをおすすめします。

例外設定は、手動スキャンのみ、リアルタイムスキャンのみ、あるいは両方に適用するように設定することができます。 リアルタイム保護から例外したオブジェクトは、ユーザーやアプリがアクセスした場合もスキャンされません。

注記

除外設定は、システムスキャンおよびコンテキストスキャンには適用されません。 システムスキャンは、お客様のデータのセキュリティを危険にさらす可能性のある、悪意のある脅威が存在しないかシステム全体を分析できるオンデマンドスキャナーです。 コンテキスト スキャンは、手動検査機能の一つです：スキャンするファイルやフォルダを右クリックし、Bitdefender でウイルス検査 を選択します。

ファイルおよびフォルダをスキャンから除外する

ファイルおよびフォルダをスキャン対象から除外するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. ウイルス対策 パネルで 隔離フォルダ をクリックします。
3. 例外設定 タブを選択します。
4. スキャン対象の例外に設定するファイルとフォルダの一覧のアコーディオンメニューをクリックします。 開いたウィンドウで、スキャンから除外するファイルやフォルダを管理することができます。
5. 例外を追加するには、下記の手順に従ってください:
   a. 追加をクリックします。

b. 参照 をクリックし、スキャン対象から除外したいファイルやフォルダを選択して 追加 をクリックします。 または、ファイルやフォルダのパスを直接記入（もしくはコピー＆ペースト）することも可能です。

c. デフォルトでは、選択されたファイルやフォルダはリアルタイムスキャンと手動スキャンの両方から除外されます。 例外を適用するスキャンを変更する場合は、もう片方のオプションを選択してください。

d. 追加をクリックします。

特定のファイル拡張子をスキャン例外に設定する

ファイル拡張子を検査から除外した場合、パソコン上での保存場所に関わらず、 Bitdefender はその拡張子がついたファイルを検査しなくなります。 例外設定は、CD、DVD、USBメディアや、ネットワークドライブなどのリムーバブルメディア上のファイルにも適用されます。

重要項目
特定の拡張子をスキャンから除外設定すると、脅威に対して脆弱になってしまう可能性がありますので、除外する拡張子には十分ご注意ください。

特定のファイル拡張子をスキャン例外に設定するには

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. ウイルス対策 パネルで 隔離フォルダ をクリックします。
3. 例外設定 タブを選択します。
4. スキャン対象の例外に設定する拡張子の一覧のアコーディオンメニューをクリックします。 開いたウィンドウで、スキャンから除外する拡張子を管理することができます。
5. 例外を追加するには、下記の手順に従ってください:
   a. 追加をクリックします。
   b. スキャンから除外する拡張子をセミコロン (;)で区切って入力します。 例：

      txt;avi;jpg

   c. デフォルトでは、指定されたファイル拡張子はリアルタイムスキャンと手動スキャンの両方から除外されます。 例外を適用するスキャンを変更する場合は、もう片方のオプションを選択してください。
   d. 追加 をクリックします。

スキャン例外を管理する

スキャンの例外設定が必要なくなった場合は、設定を削除または無効にしてください。

スキャン例外を管理するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. ウイルス対策 パネルで 隔離フォルダ をクリックします。
3. 例外設定 タブを選択します。
4. スキャン対象の例外に設定するファイルとフォルダの一覧のアコーディオンメニュー内のオプションを使って、スキャン例外を管理できます。
5. スキャンの除外設定を編集または削除するには、該当のリンクをクリックしてください。 次のように実行します :
   - リストから項目を削除するには、項目を選択して削除ボタンをクリックします。
   - テーブルの項目を編集するには、項目をダブルクリック （または選択して編集をクリック）します。 新しいウィンドウが表示され、除外する拡張子やパス、および除外対象のスキャンなどを必要に応じて変更できます。 必要な変更を行ない、変更をクリックします。

4.1.6. 隔離されたファイルの管理

Bitdefenderは、駆除できない脅威に感染しているファイルや、脅威感染の疑いがあるファイルを安全な隔離フォルダへ移動します。 隔離領域にある脅威を実行したり読み出したりすることはできないため、脅威が被害を及ぼすことはありません。

初期設定では、隔離されたファイルは自動的に Bitdefender のラボに送付され、 Bitdefender のリサーチャーによって解析されます。 脅威の存在が確認された場合、その脅威を削除するために必要となる脅威情報データベースがリリースされます。

さらに、 Bitdefender 脅威情報アップデートした後に、隔離したファイルのスキャンも行います。 駆除されたファイルは、自動的に元の場所に戻されます。

隔離ファイルの確認および管理を行うには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. ウイルス対策 パネルで 隔離フォルダ をクリックします。

   ここでは、隔離されたファイルの名前、元の場所、および検出された脅威の名前を確認できます。
3. 隔離ファイルは、Bitdefenderのデフォルト隔離設定の通り自動的に処理されます。

   変更はおすすめしませんが、設定を表示 をクリックすることで、隔離設定を好みに合わせて変更することができます。

   以下の機能を有効または無効にするには、スイッチをクリックします：

   脅威情報のアップデート後に隔離フォルダを再スキャン
   隔離されたファイルを脅威情報データベース後に自動的に再検査する場合は、こちらのオプションを有効にしておいてください。 駆除されたファイルは、自動的に元の場所に戻されます。

   30日以上経過したファイルを削除する
   隔離されたファイルは 30日間経過した後に自動的に削除されます。

   復元されたファイルに対して例外を作成
   隔離フォルダから復元したファイルは、修復されないまま元の場所に戻され、それ以降実行されるスキャンの対象から除外されます。
4. 隔離されたファイルを削除するには、当該ファイルを選択して 削除 をクリックします。 隔離されたファイルを元の場所に戻すには、ファイルを選択して 復元 をクリックします。

4.2. 高度な防御

Bitdefender の高度な脅威防御は、ヒューリスティック分析を使って潜在的な脅威をリアルタイムで検出する、革新的なプロアクティブ検知テクノロジーです。

高度な脅威防御は、コンピュータ上で動作するアプリケーションを常にモニタリングし、脅威的な挙動を検知します。 各アクションに対してスコアが算出され、プロセスごとに総合スコアが計算されます。

安全対策として、脅威や潜在的に有害なプロセスが検出され、ブロックされるたびに通知されます。

高度な脅威防御をオン/オフにするには

高度な脅威防御をオン/オフにするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. 高度な脅威防御 パネルでスイッチをオン/オフにします。

> **注記**
> システムをランサムウェアやその他脅威の攻撃から保護するには、リアルタイム保護を無効にする期間をなるべく短めにすることをおすすめします。

検出された悪意のある攻撃を確認する

脅威や潜在的に有害なプロセスが検出されると、 Bitdefender はそれらをブロックしてコンピュータがランサムウェアやその他マルウェアに感染することを防ぎます。 検出された悪意のある攻撃のリストは、以下の手順でいつでも確認することができます:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. 高度な脅威防御ウィンドウで、脅威に対する防御をクリックします。
3. 「ランサムウェア防御」機能に初めてアクセスすると、機能の紹介が表示されます。 わかりました。 をクリックして続行します。

   過去 90 日間に検出された攻撃が表示されます。 検出されたランサムウェアのタイプ、悪意のあるプロセスのパス、除染に成功したかどうかなどを詳しく確認するには、表示したい項目をクリックします。

プロセスを除外設定に追加する

信頼できるアプリケーションに対しては例外ルールを設定することで、それらのアプリケーションが脅威のような似た挙動を示したとしても、高度な脅威防御にブロックさせないようにできます。

高度な脅威防御の例外リストにプロセスを追加するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. 高度な脅威防御 パネルで 設定 をクリックします。
3. 例外設定 ウィンドウで アプリケーションを例外に追加 をクリックします。

4. 除外したいアプリを選択し、OKをクリックします。

   リストから項目を削除するには、項目を選択して横の削除オプションをクリックします。

4.3. オンライン脅威対策

Bitdefender のオンライン脅威対策は、危険が疑われるウェブサイトを警告することで、安全なブラウジングができる環境を提供します。

Bitdefenderは、以下に対するオンライン脅威対策を提供します:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

オンライン脅威対策を設定するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. オンライン脅威対策 パネルで 設定 をクリックします。

Web 保護ウィンドウで、オン/オフにしたいスイッチをクリックします:

- Web 攻撃防止機能は、ダウンロードされるデータを含めた、さまざまなオンライン脅威をブロックします。
- サーチ アドバイザは検索エンジンの検索結果や、SNS上のリンクの安全性を確認し、URLの横にアイコンを表示します :

  このウェブページは開かないでください。

  このページには危険なコンテンツが含まれている可能性があります。ページを開く場合はご注意ください。

  このページは安全です。

  サーチ アドバイザは以下の検索エンジンに対応しています :
  - Google
  - Yahoo!
  - Bing
  - Baidu

サーチ　アドバイザは以下のSNS（ソーシャル・ネットワーキング・サービス）に対応しています：
- Facebook
- Twitter

- 暗号化 Web スキャン。

  より巧妙なフィッシング詐欺の手法として、セキュアなウェブ通信が利用される可能性があります。 そのため、暗号化 Web スキャンのオプションは有効にしたままにすることを推奨します。

- 詐欺サイトからの保護

- フィッシング保護。

ネットワーク脅威対策ウィンドウには、ネットワーク脅威対策オプションが用意されています。 脆弱性を悪用した複雑なマルウェア（ランサムウェアなど） からコンピュータをしっかりと保護できるよう、このオプションは有効のままにしてください。

Bitdefender　の脅威対策、フィッシング詐欺、および詐欺サイト検知エンジンによってスキャンされないウェブサイトのリストを作成できます。 リストには、完全に信頼できるウェブサイトのみを登録してください。 例えば、よく利用するオンライン ショップなどを追加します。

Bitdefender　が提供するオンライン脅威対策機能を使ってウェブサイトを設定および管理するには:

1. Bitdefender　インターフェイスのナビゲーションメニューにある　保護　をクリックします。
2. オンライン脅威対策 パネルで 例外設定 をクリックします。
3. にホワイトリストに追加するウェブサイトの名前を当該フィールドに入力し、追加 をクリックします。

   リストからウェブサイトを削除するには、任意のサイトをリストで選択し、対応する 削除 リンクをクリックします。

   保存 をクリックして変更を保存し、ウィンドウを閉じます。

ブラウザ内のBitdefender警告

安全ではないウェブサイトを開こうとすると、ウェブサイトはブロックされ、警告ページがブラウザで表示されます。

ページにはウェブサイトのURLなど、検知された脅威の情報が記載されています。

オプションから次の操作を選択してください。 以下のオプションを利用できます：

- 安全なページへ戻るをクリックして危険なウェブページから離れます。
- 警告を無視して、ウェブページを開く場合は、リスクを理解し、容認した上で進みますをクリックします。
- 検出されたページが間違いなく安全である場合は、送信 をクリックしてホワイトリストに追加してください。 絶対に信頼できるサイトだけを追加することをお勧めします。

4.4. 迷惑メール対策

スパムとは、迷惑メールを表す用語です。 迷惑メールは個人レベルだけではなく、企業や組織レベルでも問題となってきています。 内容は決して好ましいものではありませんし、お子様に見られたり、社内で受け取ってしまうと大変です。ただし、こういったメールの送信元を止めるのは難しいことです。 次に取れる最善策は、受け取らないようにすることです。 残念ながら、迷惑メールにはあらゆる種類があり、その数も莫大です。

Bitdefender 迷惑メール対策機能は、非常に優れた革新的技術と業界標準の迷惑メール対策フィルタを採用しており、受信ボックスに到達する前に迷惑メールを削除します。 詳細については、「スパム対策支援」（p. 105）をご参照ください。

Bitdefender 迷惑メール対策機能は、POP3 プロトコル経由の電子メールメッセージに対してのみ有効です。 POP3 とは、メール サーバから電子メール メッセージをダウンロードするために最も使用されているプロトコルの 1 つです。

注記
Bitdefender は、ウェブ メールのような、ウェブ上で提供されているメールサービスに対しては、迷惑メール対策を行うことはできません。

Bitdefender がスパム メッセージを検出すると、件名の先頭に [SPAM] の文字を付けます。 Bitdefender は自動的にスパム メッセージを特定のフォルダに移動します。以下、主要なメーラーでの動作です：

- Microsoft Outlook ： スパム メッセージは、削除済みアイテム フォルダ内の Spam フォルダに移動されます。 スパムフォルダは、メールをスパムとしてラベルした際に作成されます。

- Thunderbird : スパム メッセージは、ごみ箱 フォルダ内の Spam フォルダに移動されます。 スパムフォルダは、メールをスパムとしてラベルした際に作成されます。

その他のメールクライアントを使用している場合は、ルールを作成して、Bitdefender がメールに、 [spam] と付けたものを、適切な隔離フォルダへ移動するようにしてください。 削除アイテムやゴミ箱フォルダが削除されると、スパムフォルダも削除されます。 ただし、新しいスパムフォルダは、メールをスパムとしてラベルした際に作成されます。

4.4.1. スパム対策支援

迷惑メール対策フィルタ

Bitdefender迷惑メール対策エンジンはクラウド技術をはじめ、友人リスト、スパマーリスト、文字コードフィルタなどさまざまなフィルタを使って迷惑メールの受信を防ぎます。.

友人リスト / スパマー リスト

大抵の人は毎日同じドメインの会社や組織と連絡を取ったり、メールを受け取っています。 友人リストとスパマーリストを利用することで、メールの受信を許可する人（友人）とメールの受信を必ずブロックする人（スパマー）を簡単に設定することができます。

注記
友人リストへお友達の名前とメールアドレスを登録しておくことをおすすめします。 Bitdefenderは友人リストに登録されたメールアドレスから届くメールは決してブロックすることはありません。友人登録しておくことで、正常なメールが必ずブロックされずに届くようにすることができます。

文字コードフィルタ

迷惑メールの多くはキリル文字やアジア圏の文字で書かれています。 言語フィルタはこれらの言語を含むメールを検出し、迷惑メールとして対処します。

迷惑メール対策の操作

Bitdefender 迷惑メール対策エンジンは、各種迷惑メール対策フィルタを使用して、メールをそのまま 受信ボックス に入れるべきかの判定を行います。

インターネットから届くメールはまず最初に友人リスト/スパマーリストフィルタを通してチェックされます。 送信者のメールアドレスが友人リストに登録されている場合、メールは受信トレイへ直接移動されます。

それ以外の場合はスパマーリストフィルタが、メール送信者のアドレスがスパマーリストに登録されていないかを確認します。 リスト内の項目に一致するものがあった場合は、SPAMとしてマーキングされ、迷惑メールフォルダへ移動されます。

スパマーリストにも該当しないメールの場合は、次に言語フィルタがメールの言語をチェックし、キリル文字やアジア圏の文字が含まれていないかを確認します。 該当する場合、メールはSPAMとしてマーキングされ、迷惑メールフォルダへ移動されます。

注記
メールの件名に SEXUALLY EXPLICIT（アダルト コンテンツ）と記されていると、 Bitdefender はスパム メールと判断します。

対応メールクライアントとプロトコル

迷惑メール対策機能は、全ての POP3 / SMTP メール クライアントに対応しています。 Bitdefender 迷惑メール対策ツールバーは、以下の製品に対応しています：

- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 以降

4.4.2. 迷惑メール対策機能を有効または無効にする

迷惑メール対策は初期設定で有効です。

迷惑メール対策をオン/オフにするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. 迷惑メール対策 パネルでスイッチをオン/オフにします。

4.4.3. メールクライアント上の迷惑メール対策ツールバーを使用して

メール クライアントの上部に、迷惑メール対策ツールバーが表示されます。 迷惑メール対策ツールバーによって、メール クライアントから直接、迷惑メール対策機能を操作・管理することができます。 正しいメッセージ

をBitdefenderがスパムと判断した場合、それを簡単に修正することができます。

重要項目

Bitdefender は、迷惑メール対策ツールバーを介して、最も共通して使用されるメール クライアントを統合します。 サポートされた全てのメールクライアントの一覧は、「対応メールクライアントとプロトコル」 (p. 106)をご参照ください。

Bitdefender ツールバーの機能：

設定 – 迷惑メール対策ツールバーの設定を行う画面を開きます。
迷惑メール – メールが迷惑メール（スパムメール）であることを示します。 メールは直ちにスパムフォルダへ移動されます。 迷惑メール対策のクラウド サービスが有効になっている場合、メールは分析のためにBitdefenderクラウドへ提供されます。
通常メール – 選択したメールがスパム（迷惑メール）ではなく、Bitdefender が誤ってスパムと判断したことを示します。 電子メールは迷惑メール フォルダから、受信ボックス に移動されます。 迷惑メール対策のクラウド サービスが有効になっている場合、メールは分析のためにBitdefenderクラウドへ提供されます。

重要項目

通常メールボタンはBitdefenderがスパム（迷惑メール）としての登録を外すことができます（これらのメールは迷惑メール フォルダにあります）

スパマーの追加 – 選択した電子メールの送信者を、スパマー リストに追加します。 承認のため、OK のクリックを求められ場合があります。 スパマー リストのアドレスから受信した電子メールは、自動的に [spam] として区別されます。
友人の追加 – 選択した電子メールの送信者を友人リストに追加します。 承認のため、OK のクリックを求められ場合があります。 このアドレスから届くメール メッセージは、その内容に関わらず、常に受信されます。
スパマー – 内容に関わらず、メッセージを一切受信しない全てのメールアドレス一覧が記載された スパマー リスト を開きます。 詳細については、「スパマー リストの設定」 (p. 110)をご参照ください。
友人 – 内容に関わらず、常に受信するメールの送信者アドレスが全て保管された 友人リスト が開きます。 詳細については、「友人リストの設定」 (p. 109)をご参照ください。

誤検出されたメールを通常メールに変更する

対応メールクライアントを使用している場合は、（間違えて[spam]としてマーキングされたメールを選択することで）簡単に迷惑メールフィルタの修正を行うことができます。 これをすることで迷惑メールフィルタの精度を上げることもできます。 次の手順に従ってください：

1. メール クライアントを開きます。
2. SPAM（迷惑）メールが移動された、フォルダを開きます。
3. Bitdefenderが [spam] と誤って区別した、正常なメッセージを選択します。
4. Bitdefender 迷惑メール対策ツールバーの 友人の追加 ボタンをクリックし、送信者を友人リストに追加します。 承認のため、OK のクリックを求められ場合があります。 このアドレスから届くメール メッセージは、その内容に関わらず、常に受信されます。
5. Bitdefender 迷惑メール対策ツールバー（お使いのメールクライアントの上部に表示）の 通常メール ボタンをクリックしてください。 メールは受信トレイへ移動されます。

未検出の迷惑メールを迷惑メールに登録する

対応メールクライアントを使用している場合は、迷惑メールとして対処させるメールを簡単に設定することができます。 これをすることで迷惑メールフィルタの精度を上げることもできます。 次の手順に従ってください：

1. メール クライアントを開きます。
2. 受信トレイを開きます。
3. 検出されていない迷惑メール メッセージを選択します。
4. Bitdefender迷惑メールツールバーにある 迷惑メール ボタンを選択します（ツールバーはメールクライアントの上部に表示されます）。 [spam]としてマーキングされ、直ちに迷惑メールフォルダへ移動されます。

ツールバー設定を変更

メールソフトの迷惑メール対策ツールバー設定を変更するには、ツールバー上の 設定 ボタンをクリックし、次に ツールバー設定 タブをクリックします。

ここでは以下の選択肢があります：

- 迷惑メールを'開封済み'にする - 迷惑メールを自動的に開封済みにすることで、受信時にわざわざ開く必要がなくなります。
- 迷惑メール対策ツールバーの スパマーの追加 and 友人の追加ボタンをクリックした際に確認ダイアログを表示するか否かを選択することができます。

  確認ウィンドウは、誤って送信元メールアドレスを友達リスト/スパマーリストへ追加するのを防ぎます。

4.4.4. 友人リストの設定

友人リストはメール内容にかかわらず、常にメッセージを受信するメールアドレスの一覧です。 例え内容が迷惑メールに似ていたとしても、友人リストから届くメールは迷惑メールとして処理されません。

注記
友人リスト のアドレスから届いたメールは全て、それ以上の処理は行われずに、自動的に受信ボックスに移動されます。

友人リストの構成・管理：

- Microsoft Outlook または Thunderbird をお使いの場合、Bitdefender 迷惑メール対策ツールバー の 友人 ボタンをクリックします。
- または:
  1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
  2. 迷惑メール対策 ウィンドウで、友達の管理 をクリックします。

メールアドレスを追加するには、メールアドレス オプションを選し、メールアドレスを入力して 追加 をクリックします。 構文：name@domain.com

特定のドメインのメールアドレスをすべて追加するには、ドメイン名 オプションを選択して 追加 をクリックします。 構文：

- @domain.com、domain.com - domain.com からの全てのメールは、その内容に関わらず 受信ボックス に入ります。
- domain - domain からの全てのメールに、SPAM タグが付加されます。
- com - ドメイン末尾が com であるすべてのメールに SPAM タグが付加されます。

ドメイン全体の追加については、できるだけ避けることをお勧めしますが、ある状況においては役立ちます。 例えば、会社のドメインや、信頼できるパートナーを追加する時です。

リストから項目を削除するには、リスト内の項目を選択し、削除のリンクをクリックします。 すべての項目をリストから削除するには 一覧を削除ボタンをクリックします。

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

以前保存した友人リストを読み込むには、読み込む ボタンをクリックし、該当する .bwl ファイルを開きます。 過去に保存したリストの読み込み時に、既存のリストの内容をリセットするには、現在のリストを上書きするを選択します。

OK をクリックすると、変更が保存され、画面が自動で閉じます。

4.4.5. スパマー リストの設定

スパマー リスト は、内容に関わらず、メッセージを一切受け取らないメール アドレスの一覧です。 スパマー リスト のアドレスから受信したメールは全て、それ以降の処理なしで自動的に迷惑メールとして登録されます。

スパマー リストの構成・管理：

- Microsoft Outlook または Thunderbird をお使いの場合、Bitdefender 迷惑メール対策ツールバー の スパマーボタンをクリックします。
- または:
  1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
  2. 迷惑メール対策 ウィンドウで、スパマーの管理 をクリックします。

メールアドレスを追加するには、メールアドレス オプションを選し、メールアドレスを入力して 追加 をクリックします。 構文：name@domain.com

特定のドメインのメールアドレスをすべて追加するには、ドメイン名 オプションを選択して 追加 をクリックします。 構文：

- @domain.com、domain.com - domain.com からの全てのメールは、その内容に関わらず 受信ボックス に入ります。
- domain - domain からの全てのメールに、SPAM タグが付加されます。
- com - ドメイン末尾が com であるすべてのメールに SPAM タグが付加されます。

ドメイン全体の追加については、できるだけ避けることをお勧めしますが、ある状況においては役立ちます。

警告

スパマーリストには、正当なwebメールサービス（例：Yahoo!メール、Gmail、Hotmailなど）のドメインを追加しないでください。 正当なwebメールサービスをドメインでスパマー登録してしまうと、そのwebメールサービスを利用しているすべてのユーザーから届くメールが迷惑メールとして処理されてしまいます。 例えば、yahoo.com をスパマー リストに追加すると、yahoo.com から送信された全ての電子メールが［spam］として区別されます。

リストから項目を削除するには、リスト内の項目を選択し、削除のリンクをクリックします。 すべての項目をリストから削除するには 一覧を削除 ボタンをクリックします。

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

以前保存したスパマーリストを読み込むには、読み込む ボタンをクリックし、該当する .bwl ファイルを開きます。 過去に保存したリストの読み込み時に、既存のリストの内容をリセットするには、現在のリストを上書きする を選択します。

OK をクリックすると、変更が保存され、画面が自動で閉じます。

4.4.6. ローカルの迷惑メール対策フィルタを設定

「スパム対策支援」（p. 105）に記載されているように、Bitdefender はスパムを見分けるために、異なる迷惑メール対策フィルタの組み合わせを使用します。 迷惑メール対策フィルタは、効果的な保護ができるよう、事前に構成されています。

重要項目

Asian（アジア）や Cyrillic（キリル）文字で書かれているメールについては、正規のメールを受信するしないによって、自動ブロックの設定を無効もしくは有効に設定してください。 文字セット（例えば、ロシア語、中国語等）を使用したプログラムの現地語化されたバージョン内では、対応する設定は無効となります。

ローカルのアンチスパムフィルタを設定するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。

2. 迷惑メール対策 パネルで 設定 をクリックします。

3. 対応するスイッチをクリックしてオン/オフにします。

Microsoft Outlook または Thunderbird を使用している場合は、ローカルの迷惑メール対策フィルタをメールソフトから直接設定できます。Bitdefender 迷惑メール対策ツールバー上の ⚙ 設定 ボタン（通常はメールソフトのウィンドウ上部に表示） をクリックし、次に 迷惑メール対策フィルタ タブをクリックします。

4.4.7. クラウド保護を設定する

クラウド保護機能は、Bitdefenderクラウド技術を利用して迷惑メール対策機能を常に最新の状態に保ちます。

クラウド保護機能はBitdefender迷惑メール対策を有効にしておく限り、常に動作します。

誤って迷惑メールとして処理されたメールや未対応の迷惑メールがあった場合は、通常メール・迷惑メールのサンプルとして Bitdefender クラウドへ提出することができます。 これをすることによってBitdefenderの迷惑メール検出の精度を上げることができます。

メールのサンプルをBitdefenderクラウドに提供する場合は、以下の手順に従ってください：

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。

2. 迷惑メール対策 パネルで 設定 をクリックします。

3. 対応するスイッチをクリックしてオン/オフにします。

Microsoft Outlook または Thunderbird を使用している場合は、クラウド検出機能をメールソフトから直接設定できます。 Bitdefender 迷惑メール対策ツールバー上の ⚙ 設定 ボタン（通常はメールソフトのウィンドウ上部に表示）をクリックし、次に クラウド設定 タブをクリックします。

4.5. ファイアウォール

ファイアウォールは、パソコンが送受信するネットワーク通信を監視し、許可されていないローカルネットワークとの通信やインターネットとの通信を防ぎます。 これは家の扉を守る門番のようなものです。入ってこようとする通信を監視し続けて、許可するものとブロックするものを判断しています。

Bitdefenderファイアウォールは、いくつかのルールを元にパソコンから送受信されるデータをフィルタします。

通常、 Bitdefenderは、アプリケーションがインターネットへのアクセスを試みた際に自動的にルールを作成します。 アプリケーションのルールを手動で追加したり、編集することもできます。

安全対策として、疑わしいアプリがインターネットへの接続を試みるたびに通知されます。

Bitdefenderは検出したすべてのネットワークに対してネットワークタイプを自動で割り当てます。 ネットワークの種類にあわせて、ファイアウォールが各通信に適切な保護レベルを設定します。

各ネットワークの種類に対するファイアウォールの設定や、ネットワーク設定を変更する方法については、「通信設定を管理する」 (p. 116)をご参照ください。

ファイアウォールを有効または無効にする

ファイアーウォール保護をオン/オフにするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. ファイアウォール パネルでスイッチをオン/オフにします。

警告

パソコンを外部の侵入や不正アクセスから守れなくなるため、ファイアウォールを無効にする場合は一時的な回避策のみとしてください。 なるべくお早めにファイアウォールを有効に戻してください。

4.5.1. アプリルールを管理する

アプリケーションによるネットワークリソースおよびインターネットへのアクセスを制御するファイアーウォールのルールを確認・管理するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. ファイアウォール パネルで アプリケーションアクセス をクリックします。
3. 「ファイアウォール」機能に初めてアクセスすると、機能の紹介が表示されます。 わかりました。 をクリックして続行します。

Bitdefenderファイアウォールを通過した直近の 15 個のプログラム（プロセス）と、現在接続しているインターネットネットワークが表示されます。特定のアプリケーション用に作成されているルールを表示するには、アプリケーションをクリックしてアプリケーションルールを確認リンクをクリックします。 ルール ウィンドウが開きます。

各ルールごとに、以下の情報が表示されます：

- ネットワーク - ルールを適用するプロセスおよびネットワークアダプタのタイプ（ホーム / オフィス / 公共 / すべて）。 ルールは自動的に作成され、アダプタを通過するネットワーク、インターネット アクセスをフィルタします。 デフォルトでは、ルールはすべてのネットワークに適用されます。 ルールを作成、または既存のルールを編集して、特定のアダプタ（例えばワイヤレス ネットワーク アダプタ）を介したアプリケーションのネットワーク・インターネット アクセスのフィルタを制御することができます。
- プロトコル - ルールが適用される IP プロトコルです。 デフォルトでは、ルールはすべてのプロトコルに適用されます。
- トラフィック - このルールは送信と受信の両方に適用されます。
- ポート - ルールが適用されるポートプロトコル。 デフォルトでは、ルールはすべてのポートに適用されます。
- IP - ルールが適用されるインターネットプロトコル（IP）。 デフォルトでは、ルールはすべての IP アドレスに適用されます。
- アクセス- 特定の状況において、各アプリケーションによるネットワークまたはインターネットへのアクセスを許可するかどうかを指定します。

選択アプリに対するルールを編集または削除するには アイコンをクリックします。

- ルールを編集- 現在のルールを編集するためのウィンドウを表示します。
- ルールを削除 - 選択アプリに対する現在のルールセットを削除できます。

アプリルールを追加する

アプリルールを追加するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. ファイアウォール パネルで 設定 をクリックします。

3. ルール ウィンドウで ルールを追加 をクリックします。

設定 ウィンドウでは、以下の設定を変更できます:

- このルールをすべてのアプリケーションへ適用. 作成したルールをすべてのアプリケーションに適用する場合は、このスイッチを有効にしてください。
- プログラムのパス. 参照をクリックして、ルールを適用するアプリを選択します。
- 許可. 以下のパーミッションから一つ選択してください :

許可	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。

- 種類. ルールを適用するネットワークの種類を選択してください。 ネットワーク種類を開き、プルダウンメニューから種類を選択することでネットワークの種類を変更することができます。

種類	説明
すべてのネットワーク	ネットワークの種類に関係なく、自分のコンピュータと他のコンピュータ間のすべての通信を許可します。
プライベート	このコンピュータとローカル ネットワーク上のコンピュータ間の通信を許可します。
パブリック	すべての通信はフィルタされています。

- プロトコル. メニューからルールを適用するIPプロトコルを選択します。
  - 全てのプロトコルにルールを適用するにはすべてを選択します。
  - このルールをTCPに適用するには、TCPを選択します。
  - このルールをUDPに適用するには、UDPを選択します。
  - ルールを ICMP に適用する場合は、ICMP を選択します。
  - ルールを IGMP に適用する場合は、IGMP を選択します。

- ルールを特定のプロトコルに適用したい場合は、フィルターしたいプロトコルに割り当てられている番号を、空白の編集フィールドに入力します。

  注記

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

- 方向. メニューからルールを適用する通信方向を選択します。

方向	説明
送信	送信通信にのみ適用
受信	受信通信にのみ適用
両方	双方向にルールが適用されます。

詳細設定 ウィンドウでは以下の設定をカスタマイズできます:

- カスタムローカルアドレス. ルールを適用するローカルのIPアドレスとポートを指定してください。
- カスタムリモートアドレス. ルールを適用するリモートのIPアドレスとポートを指定してください。

現在のルールセットを削除してデフォルトのルールセットを復元するには、ルールウィンドウ内のルールをリセットリンクをクリックします。

4.5.2. 通信設定を管理する

Wi-Fi またはイーサネットアダプタを使用してインターネットに接続する場合に、安全にインターネットを利用するための設定を構成することができます。 以下のいずれかのオプションを選択できます:

- 動的 - ネットワークタイプは接続されたネットワークのプロファイルに基づき「ホーム/オフィス」または「公共」に自動的に設定されます。この場合、特定のネットワークタイプのファイアウォールルール、またはすべてのネットワークタイプを対象に定義されたファイアウォールルールのみが適用されます。

- ホーム/オフィス - ネットワークタイプは常に「ホーム/オフィス」になり、接続されたネットワークのプロファイルは無視されます。　この場合、「ホーム/オフィス」のファイアウォールルール、またはすべてのネットワークタイプを対象に定義されたファイアウォールルールのみが適用されます。
- 公共　-　ネットワークタイプは常に「公共」になり、接続されたネットワークのプロファイルは無視されます。 この場合、「公共」のファイアウォールルール、またはすべてのネットワークタイプを対象に定義されたファイアウォールルールのみが適用されます。

ネットワークアダプタを設定するには:

1. Bitdefender　インターフェイスのナビゲーションメニューにある　保護　をクリックします。
2. ファイアウォール　パネルで　設定　をクリックします。
3. ネットワークアダプタ　タブを選択します。
4. 次のアダプターに接続するときに適用する設定を選択します:
   - Wi-Fi
   - イーサネット

4.5.3. 詳細設定を設定する

高度なファイアーウォール設定を行うには:

1. Bitdefender　インターフェイスのナビゲーションメニューにある　保護　をクリックします。
2. ファイアウォール　パネルで　設定　をクリックします。
3. 設定　タブを選択します。

以下の機能を設定できます:

- ポートスキャン保護 - 開いているポートを検出し、ポートスキャンをブロックします。

  ポートスキャンはハッカーがよく使う手口で、コンピュータのどのポートが開いているかを調べるものです。　彼らはセキュアではない脆弱なポートを見つけると、それを利用してコンピュータに侵入を試みます。
- アラートモード - アプリがインターネットに接続しようとするたびにアラートが表示されます。 許可　または　ブロック　を選択します。 アラー

トモードがオンになると、プロファイル　機能が自動的にオフになります。 アラートモードはバッテリーモードと併用できます。

- ステルス　モード　-　他のコンピュータからこのコンピュータを検出できるかを表します。 ステルス設定の編集をクリックして、自分のデバイスを他のコンピュータから見えるようにするかどうかを選択します。
- デフォルトのアプリケーション動作 - ルールが定義されていないアプリケーションに対し、 Bitdefender が自動的に設定を適用することを許可します。 デフォルトのルールを編集クリックして、自動設定を適用するかどうかを選択します。
  - 自動 - アプリケーションのアクセスは、自動ファイアウォールおうおびユーザー定義ルールに基づいて許可または拒否されます。
  - 許可 - ファイアウォールルールが定義されていないアプリケーションは自動的に許可されます。
  - ブロック　-　ファイアウォールルールが定義されていないアプリケーションは自動的にブロックされます。

4.6. 脆弱性

コンピュータを悪意のある攻撃やアプリケーションから保護するには、オペレーティングシステムやアプリケーションを定期的にアップデートし、最新の状態に保つことが非常に重要です。 また、コンピュータへの物理的な不正アクセスを防止するには、簡単に推測できない強力なパスワードを各 Windows ユーザーアカウントおよび接続する Wi-Fi ネットワークに対して設定する必要があります。

Bitdefender　は、システムの脆弱性を自動的に検出し、警告を行います。スキャン対象は下記の通りです:

- コンピュータ上の古いアプリ
- Windowsアップデートが行われているか
- 弱いパスワードが設定されている Windows ユーザ アカウント
- 保護されていないワイヤレスネットワークおよびルーター。

Bitdefenderは脆弱性を簡単に修正するために2つの方法を提供します：

- 脆弱性スキャンオプションを使って、システムの脆弱性を着実に修復する。

- 自動脆弱性監視機能により、通知 ウィンドウで検出された脆弱性を確認および修復できます。

システムの脆弱性チェックは、1〜2週間に一度ほどの頻度で行うことをおすすめします。

4.6.1. パソコンの脆弱性を検査する

脆弱性スキャンオプションを使ってシステムの脆弱性を修復するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. 脆弱性 パネルで 脆弱性検査 をクリックします。
3. Bitdefender によるシステムの脆弱性チェックが完了するまでお待ちください。 スキャン処理を停止するには、ウィンドウ上部の スキップ ボタンをクリックします。
   - 重要なWindowsアップデート

     詳細を表示 をクリックすると、コンピュータに現在インストールされていない重要なWindows アップデートのリストが表示されます。

     選択したアップデートのインストールを開始するには、アップデートをインストール をクリックします。 アップデートのインストールには時間がかかることがあり、パソコンの再起動が必要になる場合もあります。 必要な場合は、可能なタイミングでパソコンを再起動させます。
   - その他アプリケーションのアップデート

     アプリケーションが最新の状態でない場合は、新バージョンをダウンロード リンクをクリックして最新のバージョンをダウンロードします。

     詳細の表示 をクリックすると、アップデートする必要のあるアプリケーションについての情報を確認できます。
   - 弱い Windows アカウントパスワード

     このコンピュータの Windows アカウントに設定されているパスワードに脆弱性がないか確認することができます。

     新しいシステムパスワードを設定するには、ログイン時にパスワードを変更 をクリックします。

脆弱なパスワードを変更するには　詳細を表示　をクリックします。ユーザーに次回ログイン時にパスワードを変更するように要求するか、すぐに自分でパスワードを変更することができます。 安全なパスワードを作るためには、大文字と小文字を混ぜる、数字と記号（例えば #, $, @）を使ってください。

- Wi-Fi 接続情報

  接続しているワイヤレスネットワークの詳細を確認するには 詳細を表示 をクリックします。 ホームネットワークにもっと強力なパスワードを設定することが推奨された場合には、該当するリンクをクリックします。

  その他の推奨事項がある場合は、所定の手順にしたがってホームネットワークのセキュリティを確保してください。

ウィンドウの右上端で、必要に応じて結果をフィルタすることができます。

4.6.2. 自動脆弱性監視を使用

Bitdefender は、システムの脆弱性を定期的にバックグラウンドでスキャンし、検出した問題をすべて 通知 ウィンドウに記録します。

検出された問題を確認・修復するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 通知 をクリックします。
2. 全て タブで、脆弱性スキャンに関する通知を選択します。
3. 検出されたパソコンの脆弱性に関する詳細情報を確認することができます。 問題に応じて、以下に指定した脆弱性を修復します：
   - Windows アップデートが利用可能な場合は、インストール をクリックします。
   - 自動 Windows Update が無効になっている場合は 有効にする をクリックします。
   - アプリケが最新でない場合は、今すぐアップデート をクリックしてベンダーの Web ページへのリンクを参照し、アプリの最新バージョンをインストールしてください。
   - Windows ユーザーアカウントのパスワードが弱い場合は、パスワードの変更 をクリックして、ユーザーに次回ログオン時にパスワードを強制的に変更させるか、自分でパスワードを変更できます。 安全なパス

ワードを作るためには、大文字と小文字を混ぜる、数字と記号 （例えば #, $, @）を使ってください。

- Windows の自動実行機能が有効になっている場合は、修復 をクリックして無効にします。
- 設定したルーターのパスワードが弱い場合は、パスワードを変更 をクリックし、パスワードを変更するための管理画面にアクセスします。
- 接続しているネットワークに、システムを危険にさらす恐れのある脆弱性がある場合は Wi-Fi 設定の変更 をクリックします。

脆弱性の監視設定を編集するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. 脆弱性 パネルで 設定 をクリックします。

   重要項目
   システムやアプリケーションの脆弱性についての通知を自動的に受け取るには、脆弱性診断 オプションを有効にしたままにします。

3. 該当するスイッチを使い、定期的にチェックしたいシステムの脆弱性を選択します。

   Windowsアップデート
   お使いのWindows OSにMicrosoftから提供される最新の重要セキュリティアップデートが適用されているかチェックします。

   その他アプリケーションのアップデート
   システムにインストールされているアプリケーションが最新の状態かどうかを確認します。 最新の状態に保たれていないアプリケーションは、悪意あるプログラムによって悪用されたり、外部から脆弱性をついた攻撃を受ける可能性があります。

   ユーザーパスワード
   システム上で設定されている Windows アカウントおよびルーターのパスワードが安全かどうかを確認します。 安易に破られないパスワード（複雑なパスワード）を設定すると、ハッカーからシステムを侵入されにくくなります。 安全性の高い、強いパスワードを作るには、大文字、小文字、数字、特殊文字（#、$、@など）を組み合わせて作ります。

自動再生
Windowsの自動再生機能のステータスを確認します。 この機能は、CD、DVD、USBメモリなどの外部デバイス上にあるアプリケーションを自動で実行させるようにできます。

脅威には、Autorunを利用してUSBメモリのような外部接続メディアからパソコン本体へ感染するものがあります。 これを防ぐために、このWindowsの機能を無効にすることをおすすめします。

Wi-Fi セキュリティ
接続しているワイヤレスホームネットワークが安全かどうか、および脆弱性があるかどうかをチェックします。 また、ホームルーターのパスワードの強度が十分かどうかを確認する方法や、さらに強度をアップする方法を確認できます。

保護されていないワイヤレスネットワークは安全でないため、ハッカーによるデータの不正傍受に対して無防備です。

注記
特定の脆弱性のモニタリングをオフにすると、その脆弱性に関連する問題は通知ウィンドウに記録されなくなります。

4.6.3. WiFiアドバイザー

カフェでの仕事中や空港での待ち時間などに、オンラインバンキングやメール送受信、ソーシャルメディアを利用する場合、公共のワイヤレスネットワークに接続する必要に迫られることも少なくありません。 しかし公共のワイヤレスネットワークには、あなたの個人データを盗み出そうとする、悪意を持つハッカーが潜んでいる恐れがあります。

なお個人データとは、メールや銀行口座、ソーシャルメディアなどを含むオンラインアカウントにアクセスするためのユーザー名およびパスワードを指します。

通常、公共のワイヤレスネットワークはログイン時にパスワードを必要としないため （また、パスワードが必要な場合でも、同一のパスワードを不特定多数のユーザーが共有するため)、セキュリティの面で大きく劣ります。 また、サイバー犯罪のターゲットとなる悪意のあるネットワークやハニーポット ネットワークである可能性もあります。

セキュリティ保護されていない、もしくは暗号化されていない公共ワイヤレス ホットスポットにおける脅威・危険を防ぐため、 Bitdefender Wi-Fi Security Advisor はワイヤレスネットワークの安全性を解析し、必要と判

断した場合には、Bitdefender VPN を使用することをユーザーに推奨します。

Bitdefender Wi-Fi Security Advisor は以下についての情報を提供します:

- ホーム Wi-Fi ネットワーク
- 公共 Wi-Fi ネットワーク

Wi-Fi Security Advisor の通知をオン/オフにする

Wi-Fi Security Advisor の通知をオン/オフにするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. 脆弱性 パネルで 設定 をクリックします。
3. 設定 ウィンドウで、Wi-Fi セキュリティ オプションをオン/オフにします。

ホーム Wi-Fi ネットワークを設定する

ホームネットワークの設定を開始するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. 脆弱性 パネルで Wi-Fi セキュリティ をクリックします。
3. ホーム Wi-Fi タブで、ホーム WI-FI を選択 ボタンをクリックします。

   これまでに接続したワイヤレスネットワークの一覧が表示されます。
4. ホームネットワークを選び、選択 をクリックします。

ホームネットワークが保護されていない、または安全でないと判断された場合、セキュリティを向上するための推奨設定が表示されます。

ホームネットワークとして設定したワイヤレスネットワークを削除するには 削除 ボタンをクリックします。

公共Wi-Fi

保護されていない、または安全でないワイヤレスネットワークに接続している間は、公共 Wi-Fi プロファイルが有効になります。 このプロファイル実行時、 Bitdefender Total Security は自動的に以下のプログラム設定を実行します: ▪

- 高度な脅威に対する防御は有効です
- Bitdefender ファイアウォールがオンになり、以下の設定がワイヤレスアダプタに対して適用されます:
  - ステルスモード - ON
  - ネットワークの種類 - 公共
- オンライン脅威対策の以下の設定がオンになっています:
  - 暗号化 Web スキャン
  - 詐欺サイトからの保護
  - フィッシングサイトからの保護
- Bitdefender Safepay™ を起動するボタンが利用可能です。 この場合、安全でないネットワークに対するホットスポット保護はデフォルトで有効になります。

Wi-Fi ネットワークに関する情報を確認する

ワイヤレスネットワークに関する情報は、下記の手順でご確認いただけます:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. 脆弱性 パネルで Wi-Fi セキュリティ をクリックします。
3. 必要な情報に応じて、ホーム Wi-Fi または 公共 Wi-Fi のいずれかのタブを選択します。
4. 詳細を確認したいネットワークの横の 詳細を表示 リンクをクリックします。

ワイヤレスネットワークはその重要度に応じて 3 種類に分類されており、それぞれが固有のアイコンで表示されます:

 Wi-Fi は危険です- は、利用しているネットワークのセキュリティレベルが低いことを示します。 これはつまり、ネットワークの使用に高いリスクがあり、追加の保護対策を取らない場合はオンラインでの支払いやネットバンキングを利用すべきでないことを意味します。 そのような状況では、安全でないネットワーク用のホットスポット保護を有効にした状態で Bitdefender Safepay™ を利用することをお勧めします。

 Wi-Fi は危険です- は、利用しているネットワークのセキュリティレベルが高くないことを示します。 これはつまり、ネットワークに脆弱性が

あり、追加の保護対策を取らない場合はオンラインでの支払いやネットバンキングを利用すべきでないことを意味します。 そのような状況では、安全でないネットワーク用のホットスポット保護を有効にした状態でBitdefender Safepay™ を利用することをお勧めします。
Wi-Fi は安全です - は、利用しているネットワークが安全であることを示します。 この場合、オンライン操作で重要なデータを使用できます。

各ネットワークの詳細を表示リンクをクリックすると、以下の詳細情報が表示されます:

- 安全 - ここでは、選択したネットワークが保護されているかどうかを確認できます。 暗号化されていないネットワークでは、データが漏洩の危険に晒される恐れがあります。
- 暗号化の種類： - ここでは、選択したネットワークが使用している暗号化の種類を確認できます。 一部の暗号化は安全でない可能性があります。 そのためネット閲覧時には、表示される暗号化の種類に関する情報をチェックし、適切に保護されていることを確認してください。
- チャンネル/周波数 - ここでは、選択したネットワークが使用しているチャンネル/周波数を確認できます。
- パスワードの強度： - パスワードの安全性を確認できます。 脆弱なパスワードを使用しているネットワークは、サイバー犯罪のターゲットになりやすくなります。
- サインインの種類 - ここでは、選択したネットワークがパスワードで保護されているかどうかを確認できます。 強力なパスワードが設定されているネットワーク以外には接続しないことを推奨します。
- 認証の種類： - ここでは、選択したネットワークが使用している認証の種類を確認できます。

システムがネットワークに接続するたびに通知を受け取りたい場合は、通知する オプションを有効にしたままにします。

4.7. webカメラ保護

ハッカーによるウェブカメラ乗っ取りは現実的な脅威であり、アプリのアクセス権限の剥奪、設定によるカメラの無効化、カメラにカバーを付けるといった解決方法はあまり実用的ではありません。 お客様のプライバシーへのアクセスをより強固に防ぐため、 Bitdefender ウェブカメラ保護はカメラへのアクセスを試みるアプリを恒久的に監視、信頼されていないアプリをブロックし続けます。

安全対策として、信頼できないアプリがカメラにアクセスを試みるたびに通知されます。

ウェブカメラ保護をオン/オフにする

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. ウェブカメラ保護 パネルでスイッチをオン/オフにします。

ウェブカメラ保護の設定

次の手順により、アプリケーションがカメラにアクセスしようとした際に適用するルールを設定できます:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. ウェブカメラ保護 パネルで 設定 をクリックします。

アプリケーションブロックルール

- ウェブカメラへのすべてのアクセスをブロック - どのアプリケーションもウェブカメラにアクセスすることはできなくなります。
- ブラウザのウェブカメラへのアクセスをブロック - Internet Explorer と Microsoft Edge 以外のブラウザはウェブカメラにアクセスできません。 Windows ストアアプリは単一のプロセスで実行されるため、Internet Explorer および Microsoft Edge は Bitdefender によってウェブブラウザとして検出されず、この設定からは除外されます。
- Bitdefender ユーザーの設定にあわせて、アプリからのwebカメラ・アクセスを設定 - Bitdefender ユーザーの大半がある人気アプリを無害と判断している場合、そのアプリによるウェブカメラへのアクセスは自動的に許可されます。 ある人気アプリが多数のユーザーによって危険とみなされている場合、アクセスは自動的に［ブロック］に設定されます。

  インストール済みアプリが Bitdefender ユーザーの過半数がブロックしているアプリのリストに追加されるたびに通知されます。

通知

- 信頼できるアプリケーションがウェブカメラに接続すれば通知します - 許可されているアプリがウェブカメラにアクセスするたびに通知されます。

ウェブカメラ保護リストにアプリを追加する

ウェブカメラに接続しようとするアプリは自動的に検出され、その振る舞いやコミュニティによる評価に応じてアクセスが許可または拒否されます。ただし、次の手順を実行することで、実行するアクションを手動で構成することができます:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. ウェブカメラ保護ウィンドウで、ウェブカメラアクセス をクリックします。
3. 「ウェブカメラ保護」機能に初めてアクセスすると、機能の紹介が表示されます。
4. 任意のリンクをクリック:
   - アクセス許可リストに追加する Windows ストアアプリを選択する – 検出された Windows ストアアプリの一覧が表示されます。 一覧に追加したいアプリの横にあるスイッチをオンにします。
   - ウェブカメラアクセスリストにアプリケーションを追加する – 一覧に追加したい .exe ファイルに移動し、OKをクリックします。

     アプリケーションをさらに追加するには 新規アプリケーションをリストに追加 リンクをクリックします。

許可されたアクセス/ブロックされたアクセス スイッチをクリックします。

選択アプリに対する他の Bitdefender ユーザーの対応を確認するには アイコンをクリックします。

ウェブカメラへのアクセスを要求するアプリケーションが、直近のアクティビティの日時と共にこのウィンドウに表示されます。

許可されているアプリケーションが Bitdefender ユーザーによってブロックされるたびに通知されます。

4.8. Safe Files

ランサムウェアは、脆弱性のあるシステムを攻撃してシステムにロックをかけ、ロックを解除する見返りに金銭を要求する悪意のあるソフトウェアです。 この悪意のあるソフトウェアは、偽のメッセージを表示してユーザーをパニックに陥れ、金銭を早く支払うように促します。

感染は、スパムメール、添付ファイルのダウンロード、感染したウェブサイトへのアクセス、悪意のあるアプリのインストールなどによって引き起こされます。通常、ユーザーはシステムが感染したことに直ちに気付くことはありません。

ランサムウェアは、以下のいずれかの動作により、ユーザーがシステムにアクセスできないようにします:

- 重要なファイルを含む個人データを暗号化し、被害者が金銭を支払わない限りデータを復元できないようにします。
- コンピュータの画面をロックし、金銭を要求するメッセージを表示します。 この場合、ファイルは暗号化されず、ユーザーが支払いに進むことを強制されます。
- アプリが実行されないようにブロックします。

Bitdefender のセーフファイル機能を使用すると、文書、写真、およびムービーなどの個人データをランサムウェアによる攻撃から保護することができます。

注記
高度な脅威防御とセーフファイルの 2 層保護によって、ランサムウェアの攻撃からシステムも守ります。 高度な脅威防御は、システムの重要な領域に対するランサムウェア攻撃を阻止する機能です。セーフファイルは、コンピュータ上の重要なファイルが第三者によって暗号化されることを防ぐ機能です。

4.8.1. セーフファイルをオン/オフにする

セーフファイル機能をオン/オフにするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. 安全なファイル パネルでスイッチをオン/オフにします。

アプリケーションが保護されたファイルにアクセスしようとするたびに、Bitdefender のポップアップウィンドウが表示されます。 アクセスを許可するか、それとも拒否するかを選択できます。

注記
「安全なファイル」機能はデフォルトでは有効になっています。

4.8.2. 個人データをランサムウェア攻撃から保護

個人データをシェルターに退避するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. セーフファイルウィンドウで、保護されたフォルダをクリックします。
3. 「保護されたフォルダ」機能に初めてアクセスすると、機能の紹介が表示されます。 保護するフォルダを追加 をクリックして続行します。
4. 保護したいフォルダを選択し、OKをクリックします。

   フォルダをさらに追加するには、保護するフォルダを追加リンクをクリックします。 または、フォルダをこのウィンドウにドラッグします。

デフォルトの設定では「ピクチャ」、「ビデオ」、「ドキュメント」、および「ミュージック」フォルダが攻撃に対して保護されます。 Box、Dropbox、Google Drive、OneDrive などのオンラインストレージサービスに保存されている個人データも保護環境に含まれます （システムにそれぞれのアプリケーションがインストールされていることが条件になります）。

システム速度の低下を防ぐため、フォルダ数は 30 個以内におさめるか、あるいは複数のファイルを 1 つのフォルダに保存することをお勧めします。

注記
カスタムフォルダは、現在のユーザーに対してのみ保護可能です。 システムおよびアプリケーションファイルは例外に追加できません。

4.8.3. アプリのアクセスを設定する

保護されたファイルを変更または削除しようとするアプリケーションは、安全でないと判断され、ブロック中のアプリケーションのリストに追加される場合があります。 そのようなアプリケーションがブロックされたが、問題のないアプリケーションであることが確かな場合は、次の手順で許可することができます:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. 安全なファイル パネルで アプリケーションアクセス をクリックします。
3. 保護フォルダ内のファイルを変更しようとしたアプリケーションがここに表示されます。 間違いなく安全であるアプリの横にあるスイッチをクリックします。

同じウィンドウで、該当するスイッチをクリックすることで、特定のアプリに対するランサムウェア保護を無効にすることができます。

新しいアプリケーションをリストに追加するには 新規アプリケーションをリストに追加 リンクをクリックします。

4.8.4. 起動時の保護

悪意のあるアプリの多くはシステムの起動時に実行されるように作られており、コンピュータに深刻なダメージを与える恐れがあります。 Bitdefenderの起動時保護は、すべてのファイルが読み込まれる前に、システムのパフォーマンスに影響を与えることなく重要なシステムファイルをスキャンします。

起動時の保護を無効にするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護をクリックします。
2. 安全なファイル パネルで 設定 をクリックします。
3. 起動時の保護 をオフにします。

> **注記**
> 除外に追加されたアプリもスキャンされ、設定に応じて適切に処理されます。

4.9. ランサムウェア防御

Bitdefender ランサムウェア修復機能は、お客様のドキュメント、写真、動画、音楽などのファイルをバックアップし、万が一ランサムウェアによって暗号化されてしまった場合にも復元できるように保護します。 ランサムウェア攻撃が検出されるたびに、 Bitdefender は攻撃に関連するすべてのプロセスをブロックし、修復処理を開始します。 これにより、要求された身代金を支払うことなく、すべてのファイルを取り戻すことが可能になります。

ランサムウェア修復をオン/オフにする

ランサムウェア修復をオン/オフにするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護をクリックします。
2. ランサムウェア修復 パネルでスイッチをオン/オフにします。

注記
ファイルをランサムウェアによる被害から保護するため、ランサムウェア修復機能は有効にしておくことをお勧めします。

自動復元を有効または無効にする

自動復元機能により、ランサムウェアによる暗号化が発生した際に、ファイルが自動的に復元されます。

自動復元をオン/オフにするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. ランサムウェア修復 パネルで 設定 をクリックします。
3. 自動復元スイッチをオン/オフにします。

自動的に復元されたファイルを表示する

自動復元 オプションが有効になっていると、 Bitdefender はランサムウェアで暗号化されたファイルを自動的に復元します。 これにより、すべてのファイルが安全に保護された状態で、安心してコンピュータを使うことができます。

自動的に復元されたファイルを表示するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 通知 をクリックします。
2. 全て タブで、修復された最新のランサムウェア攻撃に関する通知を選択し、復元されたファイル をクリックします。

   復元されたファイルの一覧が表示されます。 ここでは、ファイルが復元された場所を確認できます。

暗号化ファイルを手動で復元する

暗号化されたファイルを手動で復元する必要がある場合は、次の手順に従ってください:

1. Bitdefender インターフェイスのナビゲーションメニューにある 通知 をクリックします。
2. 全て タブで、検出された最新のランサムウェア攻撃に関する通知を選択し、暗号化ファイル をクリックします。

3. 暗号化されたファイルの一覧が表示されます。

   ファイルを復元 をクリックして続行します。

4. 修復処理のすべてまたは一部が失敗した場合、復元されたファイルを保存する場所を選択する必要があります。　復元場所をクリックして、PC上の任意の場所を選択します。

5. 確認画面が表示されます。

   終了をクリックして復元処理を終了します。

以下の拡張子を持つファイルが暗号化された場合、復元することが可能です:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb; .doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html; .ico; .jar; .java; .jpeg; .jpg; .js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp; .odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

アプリケーションを例外に追加

信頼できるアプリケーションに対しては、例外ルールを設定することで、それらのアプリケーションがランサムウェアのような似た挙動を示したとしても、ランサムウェア修復機能にブロックさせないようにできます。

アプリをランサムウェア修復の例外リストに追加するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. ランサムウェア修復 パネルで 設定 をクリックします。
3. アプリをリストに追加するには、新規アプリケーションをリストに追加 をクリックします。

4.10. ファイル暗号化

Bitdefender ファイル暗号化は、暗号化されパスワードがかけられた仮想ドライブ（ファイル金庫）をコンピュータ上に作成します。そこに秘密の

ドキュメントを格納することができます。 ファイル金庫に格納されたデータはパスワードを知っているユーザーのみがアクセスできます。

セキュリティのため、ファイル金庫を開く、データを格納する、閉じる際に、パスワードが必要となります。 金庫を開いている間は新しいファイルを追加したり、現在のファイルにアクセスしたり、変更することができます。

実際には、このファイル金庫はローカルのハードディスク上に保存された、.bvdという拡張子のファイルです。 ファイル金庫は、実際は普通のファイルなので、他のOS（Linuxなど）からもアクセスすることができますが、ファイル内に格納されている情報は暗号化されているため読み取ることはできません。

ファイル金庫はBitdefender画面またはWindowsの右クリックメニュー、あるいは論理ドライブから管理することができます。

金庫を管理する

ファイル金庫を Bitdefender から管理するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. ファイル暗号化 パネルで 設定 をクリックします。

   既存のファイル金庫がこのウィンドウに表示されます。

ファイル金庫を作成

新しい金庫を作成するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. ファイル暗号化 パネルで 新しいファイル金庫を作成 をクリックします。
3. 金庫ファイルの場所と名前を指定します。
   - 金庫ファイルの名前を、対応するフィールドに入力します。
   - 参照をクリックして金庫の保存場所を選択し、任意のファイル名で保存します。

4. 該当のメニューからドライブ文字を選択します。 金庫を開くと、マイコンピュータ上に選択したドライブ名で仮想ディスクドライブが表示されます。
5. 金庫のデフォルトのサイズ（100MB）を変更したい場合は、金庫のサイズ(MB)スピンボックスの上下矢印キーを使用します。
6. パスワード と パスワードの確認 の入力欄に、金庫のパスワードを入力します。 パスワードは半角で最低８文字が必要です。 金庫を開いたり、そのファイルにアクセスする際には必ずパスワードが要求されます。
7. 作成をクリックします。

Bitdefenderはすぐに処理結果を表示します。 エラーが発生した場合は、エラーメッセージをもとに問題をトラブルシューティングしてください。

新しい金庫をよりすばやく作成するには、デスクトップまたはコンピュータ上のフォルダを右クリックし、 Bitdefender> Bitdefender ファイル金庫 を開いて ファイル金庫の作成 を選択します。

注記
ファイル金庫はすべて一箇所に保存すると すばやく見つけることができて便利です。

ファイル金庫のインポート

ローカルに保存されているファイル金庫をインポートするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. ファイル暗号化 ウィンドウで、金庫のインポート をクリックします。
3. 金庫の場所を検索して選択します（.bvd ファイル)。
4. 開く をクリックします。

ファイル金庫を開く

金庫にあるファイルにアクセスして作業するためには、必ずその金庫を開く必要があります。 金庫を開くと、仮想ディスクドライブがマイコンピュータ上に現れます。 このドライブは金庫に割り当てられたドライブ名で表示されます。

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。

2. ファイル暗号化 パネルで 設定 をクリックします。
3. 開きたい金庫を選択し、ロックを外す クリックします。
4. 必要なパスワードを入力し、OK をクリックします。
5. 開く をクリックしてファイル金庫を開きます。

Bitdefenderはすぐに処理結果を表示します。 エラーが発生した際、そのエラーメッセージをもとに問題解決を行ってください。

金庫をよりすばやく開くには、開きたい金庫の .bvd ファイルをコンピュータ上で検索します。 ファイルを右クリックし、 Bitdefender > Bitdefender ファイル金庫 を選択して ロックを外す を選びます。 必要なパスワードを入力し、OK をクリックします。

金庫へファイルを追加

金庫にファイルやフォルダを追加する前に、金庫を開いておく必要があります。

金庫に新しいファイルを追加するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. ファイル暗号化 パネルで 設定 をクリックします。
3. ファイルを追加したい金庫を選択し、ロックを外す クリックします。
4. 必要なパスワードを入力し、OK をクリックします。
5. 開く をクリックしてファイル金庫を開きます。
6. Windows と同様にファイルやフォルダを追加できます（コピーアンドペーストなど）。

金庫にファイルをすばやく追加するには、金庫にコピーしたいファイルやフォルダを右クリックし、Bitdefender > Bitdefender ファイル金庫 を選択し、ファイル金庫に追加 を選びます。

- ファイル金庫が1つだけ開いている場合は、ファイルやフォルダは金庫にそのままコピーされます。
- 複数の金庫が開いている場合は、コピー先の金庫を選択するように促されます。 メニューからコピー先の金庫のドライブレター（Cドライブなど）を選択し、OKをクリックしてください。

ファイル金庫をロックする

ファイル金庫での作業を終えたら、データを守るためにロックする必要があります。 ファイル金庫をロックすると、仮想ドライブは非表示になり、マイ コンピュータ上から見えない状態になります。 このためロックされた金庫内のデータへのアクセスは完全にブロックされた状態になります。

金庫をロックするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. ファイル暗号化 パネルで 設定 をクリックします。
3. ロックしたい金庫を選択し、ロックする クリックします。

Bitdefenderはすぐに処理結果を表示します。 エラーが発生した場合は、エラーメッセージをもとに問題をトラブルシューティングしてください。

金庫をよりすばやくロックするには、任意の金庫の .bvd ファイルを右クリックし、 Bitdefender > Bitdefender ファイル金庫 を選択して ロックする を選びます。

ファイル金庫からファイルを除去

ファイル金庫からファイルやフォルダを削除する場合は、金庫を開いている必要があります。 ファイルまたはフォルダを金庫から削除するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. ファイル暗号化 パネルで 設定 をクリックします。
3. 金庫がロックされている場合は、ファイルを削除したい金庫を選択し、ロックを外す をクリックします。
4. 開く をクリックします。

   ファイルやフォルダの削除は Windows の通常の操作で行います（削除するファイルを右クリックし 削除 を選択）。

ファイル金庫のパスワードを変更

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

パスワードを変更するにはまずその金庫がロックされている必要があります。 金庫のパスワードを変更するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. ファイル暗号化 パネルで 設定 をクリックします。
3. パスワードを変更したい金庫を選択し、設定 をクリックします。
4. 現在の金庫のパスワードを古いパスワード欄に入力します。
5. 金庫の新しいパスワードを新しいパスワードと新しいパスワード(再入力) 欄に入力します。

> **注記**
> パスワードは半角で最低８文字が必要です。 安全なパスワードを作るためには、大文字と小文字を混ぜる、数字と記号 (例えば #, $, @)を使ってください。

Bitdefenderはすぐに処理結果を表示します。 エラーが発生した場合は、エラーメッセージをもとに問題をトラブルシューティングしてください。

金庫のパスワードをすばやく変更するには、当該金庫の .bvd ファイルをコンピュータ上で検索します。 ファイルを右クリックし、 Bitdefender > Bitdefender ファイル金庫 を選択して 金庫のパスワードを変更 を選びます。

4.11. 認証情報をパスワードマネージャーで保護

毎日パソコンを使って支払いを行なったり、ソーシャルメディアを閲覧したり、チャットアプリケーションにログインすることが多くなってきています。

しかしこれらすべてのパスワードを覚えておくのは容易なことではありません。

そしてWebを閲覧中は特に気をつけておかないと、個人情報やメールアドレス、インスタントメッセンジャーIDやクレジットカード情報が盗み取られる可能性があります。

パスワードや個人データをパソコン内にそのままの状態で保管すると、悪意ある人物によって盗み出されたり、悪用される可能性があるため、危険です。 しかし複数あるオンラインのアカウントやサービスで個別のパスワードをすべて頭で記憶しておくのは容易ではありません。

ではどのように必要な時に必要なパスワードを入力できるようにするべきでしょうか？ また、どのようにしてパスワードを安全に保管すればいいでしょうか？

パスワードマネージャーではパスワードの管理、プライバシーの保護、安全なウェブ閲覧の実現などが可能です。

パスワードマネージャーでは、ウォレットにすべてのパスワードを保存し、1つのマスターパスワードですべてのパスワードにアクセスできます。

オンラインアクティビティに対する最高の保護のため、パスワードマネージャーは Bitdefender Safepay™ と連携し、個人データを危険に晒す恐れのあるオンライン脅威に対して包括的なセキュリティソリューションを提供します。

パスワードマネージャーは以下の個人情報を保護します:

- メールアドレス、電話番号などの個人情報
- 各種Webサイトで使用するログイン情報
- 銀行口座情報、クレジットカード番号など
- メールアカウントへのアクセスデータ
- アプリ用のパスワード
- Wi-Fi通信用のパスワード

新しいパスワード管理データベースを作成

Bitdefender ウォレットには、個人データを保管することができます。 ブラウザでの操作をより簡単にするため、以下の手順に従ってウォレットを作成してください:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. パスワード管理モジュールで、マイ・パスワード管理を選択します。
3. 新規作成 をクリックします。
4. 該当する欄に必要な情報を入力してください。
   - ウォレット ラベル - ウォレット データベースに対して一意の名前を入力します。
   - マスターパスワード - ウォレットのパスワードを入力します。
   - パスワードの再入力 - 設定したパスワードを再度入力します。

- ヒント - パスワードを思い出すためのヒントを入力しましょう。

5. 続けるをクリックします。
6. このステップで、クラウドに情報を保存するかどうか選択できます。[はい] を選択した場合、バンキング情報はデバイス上にローカルでのみ保存されます。 任意のオプションを選択し、続行 をクリックします。
7. 認証情報のインポート元となるウェブブラウザを選択してください。
8. 終了をクリックします。

既存のデータベースを読み込む

ローカルに格納されているウォレットデータベースをインポートするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. パスワード管理モジュールで、マイ・パスワード管理を選択します。
3. 読み込む をクリックします。
4. ウォレットデータベースを保存したるデバイス上の場所を参照し、名前を設定します。
5. 開く をクリックします。
6. ウォレットに名前を付け、作成時に割り当てたパスワードを入力します。
7. インポートをクリックします。
8. ウォレットに認証情報をインポートしたいプログラムを選択し、終了 ボタンをクリックします。

パスワード管理のデータベースをエクスポート

ウォレットデータベースをエクスポートするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. パスワード管理モジュールで、マイ・パスワード管理を選択します。
3. 任意のウォレットの ⋮ アイコンをクリックし、エクスポート を選択します。
4. ウォレットデータベースの場所を検索して選択します（.db ファイル）。
5. 保存 をクリックします。

注記
エクスポート オプションを使用するには、ウォレットを開いておく必要があります。
エクスポートする必要のあるウォレットがロックされている場合、ウォレットを有効化 をクリックして、ウォレット作成時に割り当てられたパスワードを入力します。

ウォレットをクラウドで同期する

クラウドでのウォレット同期をオン/オフにするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. パスワード管理モジュールで、マイ・パスワード管理を選択します。
3. 任意のウォレットの ⋮ アイコンをクリックし、設定 を選択します。
4. 表示されるウィンドウで任意のオプションを選択し、保存 をクリックします。

注記
エクスポート オプションを使用するには、ウォレットを開いておく必要があります。
エクスポートする必要のあるウォレットがロックされている場合、ウォレットを有効化 をクリックして、ウォレット作成時に割り当てられたパスワードを入力します。

「パスワード管理」に登録するログイン情報を管理

パスワードを管理するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. パスワード管理モジュールで、マイ・パスワード管理を選択します。
3. 任意のウォレットデータベースを選択し、ウォレットを有効化 をクリックします。
4. マスターパスワードを入力し、OKをクリックします。

新しいウィンドウが表示されます。 画面上部から該当するカテゴリを選択してください:

- 個人情報

- webサイト
- オンライン銀行
- 電子メール
- アプリ
- Wi-Fi 接続情報

認証情報を追加/編集する

- 新しいパスワードを追加するには、画面上部からカテゴリを選択して＋項目を追加を選択し、必要な情報を記入し、「保存」ボタンをクリックしてください。
- 表の項目を編集するには、項目を選択して編集ボタンをクリックします。
- エントリを削除するには、削除するエントリを選択し、 削除ボタンをクリックします。

パスワードマネージャー保護をオン/オフにする

パスワードマネージャー保護をオン/オフにするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. パスワード管理 パネルでスイッチをオン/オフにします。

パスワードマネージャーの設定を管理する

マスターパスワードを細かく設定するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. パスワード管理モジュールで、設定を選択します。
3. ▪ セキュリティ設定 タブを選択します。 ▪

以下のオプションを利用できます :

- デバイスにログオンする際にマスターパスワードを求める- デバイスにログインする際にパスワードの入力を求められます。
- ブラウザやアプリを起動する際にマスター・パスワードを求める - ブラウザやアプリを起動した際にマスター・パスワードを入力するように促されます。

- マスターパスワードを要求しない- コンピュータ、ブラウザ、またはアプリにアクセスする際にマスターパスワードの入力を求められなくなります。
- パソコンから離れた場合はパスワード管理を自動的にロックする - 15分間デバイスを操作しなかった場合は、次回の操作時にマスターパスワードを入力するように促します。

重要項目
マスター・パスワードは紛失しないように大切に保管してください。 パスワードを忘れてしまった場合は、プログラムを再インストールするか、Bitdefender サポートページをご覧ください。

パソコンをより快適に

パスワードマネージャーを使用するブラウザやアプリケーションを選択するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. パスワード管理モジュールで、設定を選択します。
3. ・プラグイン タブを選択します。・

   パスワードマネージャーを使用するアプリケーションをチェックすると、使い勝手がさらに向上します:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - 決済ブラウザ

自動入力を設定する

自動入力機能は、お気に入りのサイトやログインが必要とされるサイトへアクセスしやすくします。 ウェブブラウザにログイン情報や個人データを入力すると、それらの情報はウォレットに自動的に移動し保護されます。

自動入力設定 を編集するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。

2. パスワード管理モジュールで、設定を選択します。
3. 自動入力の設定 タブを選択します。 ▪
4. 以下のオプションを設定してください：
   - パスワードマネージャーによる個人データの保護方法を設定:
     - 重要なデータをウォレットに自動的に保存する - ログイン情報やクレジットカード情報などの重要なデータをウォレットに自動的に保存し、常に最新の状態に保ちます。
     - 毎回確認する - ログイン情報を保存するかどうか、毎回確認画面を表示して確認します。
     - 保存しません。手動で情報を更新します。 - 入力されたログイン情報は保存しません。認証情報は手動でのみ追加することが可能です。
   - ログイン情報を自動入力:
     - ログイン情報を毎回自動入力する - ログイン情報をブラウザの入力欄に自動的に入力します。
   - フォームの自動入力:
     - フォームを含むページにアクセスした際に、選択可能なオプションを表示 - オンラインショッピングやサインアップなど、入力フォームを含む ページが検出されると、 Bitdefender は入力オプションを選択するためのポップアップウィンドウが表示されます。

パスワードマネージャーの情報をブラウザから管理

パスワードマネージャーの詳細はブラウザから直接簡単に管理できますので、重要なデータをすべて手元で把握できます。 Bitdefender ウォレットアドオンは、以下のブラウザで利用できます： Google Chrome、Internet Explorer、Mozilla Firefox が Safepay に対応しています。

Bitdefender ウォレット拡張機能にアクセスするには、ウェブブラウザを開いてアドオンのインストールを許可し、ツールバーの  アイコンをクリックします。

Bitdefender のウォレット拡張機能には以下のオプションが含まれています:

- ウォレットを開く - ウォレットを開きます。
- ウォレットをロック - ウォレットをロックします。

- ウェブページ - ウォレットに保存されているすべてのウェブサイトのログイン情報を含むサブメニューが開きます。 リストにウェブサイトを新たに追加するには ウェブページを追加 をクリックします。
- フォームを自動入力 - 特定のカテゴリーに追加した情報を含むサブメニューが開きます。 ここから、ウォレットに新しいデータを追加できます。
- パスワードジェネレータ - 新規または既存のアカウントで使用できるランダムなパスワードを生成できます。 詳細設定を表示 をクリックして、パスワードの複雑さをカスタマイズします。
- 設定 - パスワードマネージャーの設定ウィンドウを開きます。
- 問題を報告 - Bitdefender パスワードマネージャーで問題が発生した際に、それを報告できます。

4.12. VPN

VPN アプリは、お使いの Bitdefender 製品からインストールでき、接続の保護をさらに強化したいときに利用することができます。 VPNは、デバイスとネットワークとの間の安全なトンネルとして機能し、銀行と同等レベルの暗号化を使用してデータを暗号化することで、常に IP アドレスを隠すことができます。 トラフィックは別のサーバーを経由してリダイレクトされます。 そのため、弊社のサービスを利用している他の多数のデバイスの中から、お客様のデバイスを識別することはほぼ不可能です。 さらに、Bitdefender VPN を経由してインターネットに接続すると、通常は特定の地域からしかアクセスできないコンテンツも楽しむことができます。

注記
一部の国ではインターネット検閲が行われているため、法律によって VPN の使用が禁止されています。 法的な問題を回避するため、 Bitdefender VPN アプリの初回起動時に警告メッセージが表示される場合があります。 このアプリを引き続き使用することで、該当される法律や条例と、生じうるリスクを理解したことになります。

VPN をインストールする

VPN アプリは、お客様の Bitdefender インターフェイスから次のようにしてインストールできます:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。

2. VPN パネルで VPN を有効にする をタップします。
3. VPN の詳細が表示されているウィンドウで、「サブスクリプション契約」をよく読んでから、BITDEFENDER VPN をインストールする をクリックします。

   ファイルがダウンロードされ、インストールされるまでしばらくお待ちください。
4. BITDEFENDER VPN を開くをクリックしてインストール処理を終了します。

> **注記**
> Bitdefender VPN を使用するには .Net Framework 4.5.2 以上がインストールされている必要があります。 このパッケージをインストールしていない場合、通知ウィンドウが表示されます。 .Net Framework のインストール をクリックすると、このソフトウェアの最新バージョンをダウンロードできるページにリダイレクトされます。

VPN を開く

Bitdefender VPN のメインインターフェイスには、以下のいずれかの方法でアクセスできます:

- タスクトレイから：
  1. システムトレイの アイコンをクリックし、表示 をクリックします。
- Bitdefenderの製品画面から：
  1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
  2. VPN パネルで VPN を開く をタップします。

VPN インターフェース

VPN インターフェイスには、アプリの状態（接続・切断）が表示されます。無料バージョンの場合、接続するサーバーの場所は Bitdefender によって最適なサーバーに自動的に設定されますが、プレミアムユーザーはリストから接続したいサーバーを自由に選択できます。 VPN サブスクリプションの詳細については 「サブスクリプション」 (p. 264) を参照してください。

接続または切断するには、画面上部に表示されている状態をクリックするか、システムトレイのアイコンを右クリックします。 VPN 接続時はシステ

ムトレイのアイコンに緑のチェックが表示され、VPN 切断時には赤のチェックが表示されます。

接続中は、経過時間とデバイスに自動的に割り当てられた IP アドレスがインターフェイス下部に表示されます。

その他オプションにアクセスするには、左上の ≡ アイコンをクリックしてメニューエリアにアクセスしてください。 ここでは以下の選択肢があります：

- マイアカウント - Bitdefender アカウントと、VPN サブスクリプションについての詳細が表示されます。 別のアカウントでサインインしたいときはアカウントの切り替えをタップします。
- 設定 - 必要に応じて、製品の挙動をカスタマイズできます:
  - VPN が自動的に接続または切断したときに通知を受け取る
  - Windows 起動時に VPN アプリを自動的に実行
  - デバイスがセキュリティ保護されていないワイヤレスネットワークに接続した際に、VPN アプリを自動的に起動します
- Premium にアップグレードする - 無料版を使用している場合は、ここからプレミアムプランにアップグレードできます。
- ヘルプ - サポートセンターのプラットフォームにリダイレクトされ、BitdefenderVPNの使用方法に関する参考資料をご覧いただけます。
- アプリ情報 - インストールされているバージョンに関する情報が表示されます。

サブスクリプション

Bitdefender VPN では、デバイスごとに毎日 200MB のトラフィックを無料で使用できます。最適なサーバーに自動的に接続するため、必要なときにいつでも接続を保護することが可能です。

サーバーの場所を自由に選択して無制限のトラフィックおよび無制限のコンテンツへアクセスを利用したい場合は、プレミアムバージョンにアップグレードする必要があります。

製品のインターフェース内に表示されている 無制限トラフィックを入手ボタンをタップすることで、いつでも Bitdefender VPN のプレミアムバージョンにアップグレードできます。

Bitdefender VPN プレミアムサブスクリプションは、 Bitdefender Total Security のサブスクリプションとは独立しているため、VPN はセキュリ

ティソリューションのサブスクリプションの状態とは関係なく常に利用可能です。 Bitdefender VPN プレミアムサブスクリプションの有効期限が終了したが、 Bitdefender Total Security のサブスクリプションがまだ有効な場合、自動的に無料プランへと切り替わります。

Bitdefender VPN はクロスプラットフォームの製品であり、Windows、macOS、Android、および iOS に対応した Bitdefender 製品で利用することができます。 プレミアムプランにアップグレードすると、同じ Bitdefender アカウントでログインするだけで、お使いのすべての製品でサブスクリプションを利用することができます。

4.13. 安全なオンライン決済：Safepay

今日、ユーザーの多くがショッピングやネットバンキングを、コンピュータを使って行っています。 請求書の支払い、送金、商品やサービスの購入についても、昔とは比べ物にならないほど簡単かつスピーディになりました。

これらの手続きには個人情報の送信、クレジットカード情報の入力、パスワードなどの機密情報をインターネット上で送信する必要があり、サイバー犯罪者のターゲットになりえる情報ばかりです。 ハッカーなどはあらゆる手段でこのような情報を入手しようとしますので、オンライン取引を行う際には特に注意を払うべきです。

Bitdefender Safepay™ は、オンラインバンキングやショッピング、およびその他のオンライン決済を安全に利用できる保護ブラウザです。

Bitdefender パスワードマネージャーは Bitdefender Safepay(TM) に統合されており、オンラインバンキングやオンラインショッピング時にユーザーの個人情報を強力に保護します。 詳細については、「認証情報をパスワードマネージャーで保護」 (p. 137)をご参照ください。

Bitdefender Safepay(TM) には以下の特長があります:

- デスクトップへのアクセスをブロックし、画面のスクリーンショットを撮影されるのを防ぎます。
- パスワードマネージャーにより、ウェブ閲覧時のパスワードを保護します。
- ステルス・キーボードが搭載されており、こちらを使用するとハッカーなどにキーボード操作を盗み取られるのを防げます。
- その他ブラウザからは完全に独立したブラウザです。

- セキュア化されていないWi-Fiネットワークで安全に通信を行なえるように、ホットスポット保護機能が搭載されています。
- ブックマークにも対応しているため、お気に入りのオンライン・ショッピングサイトやオンライン銀行をお気に入り登録することも可能です。
- 使用はオンライン銀行やオンライン・ショッピングサイトに限られていません。 どんなウェブサイトでも Bitdefender Safepay(TM) で開くことができます。

Bitdefender Safepay™ を使用する

デフォルトの設定では、ユーザーがオンラインバンキングやオンラインショップにアクセスすると、 Bitdefender が自動的に検知し、サイトを Bitdefender Safepay™ で開くように促します。

Bitdefender Safepay™ のメイン管理画面には、以下のいずれかの方法でアクセスできます:

- Bitdefender の管理画面から:
  1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
  2. 決済ブラウザ パネルで 決済ブラウザを起動 をクリックします。
- Windows から:
  - Windows 7の場合 :
    1. Windows スタートボタンをクリックして、すべてのプログラムを選択してください。
    2. Bitdefenderをクリックしてください。
    3. Bitdefender Safepay™ をクリックします。
  - Windows 8 および Windows 8.1:

    Windows のスタート画面から Bitdefender Safepay™にアクセスし（スタート画面に ″ Bitdefender Safepay™″ と直接入力する方法も可)、アイコンにクリックします。
  - Windows 10の場合 :

    タスクバーの検索ボックスに「Bitdefender Safepay™」と入力し、アイコンをクリックします。

注記
Adobe Flash Playerのプラグインがインストールされていない、あるいは最新の状態ではない場合、Bitdefenderの警告が表示されます。 該当するボタンを選択して次へお進みください。
インストール処理が完了したら、Bitdefender Safepay™ を手動で起動し直して作業を続行します。

Bitdefender Safepay™ は通常のウェブブラウザと見た目も動作もほぼ同じですので、ウェブブラウザの操作に慣れていれば違和感なく使用できます。

- アドレスバーに開きたいURLを入力します。
- タブを追加し、 をクリックして Bitdefender Safepay™ ウィンドウで複数のウェブサイトを開きます。
- 次の各種ボタンで前へ戻ったり、次へ進んだり、ページを更新することができます
- Bitdefender Safepay™設定 にアクセスするには、 をクリックして 設定 を選択します。
- をクリックして、パスワードマネージャー でパスワードを保護します。
- アドレスバーの隣のをクリックすれば、ブックマークを管理することができます。
- をクリックしてステルス・キーボードを起動します。
- ブサウザのサイズを拡大/縮小するには、キーボードの Ctrl + +/- キーを同時押しします。
- Bitdefender 製品についての情報を表示するには、 をクリックしてこの製品について を選択します。
- をクリックすることで、重要な情報を印刷できます。

注記
Bitdefender Safepay と Windows デスクトップを切り替えるには Alt+Tab キーを押すか、ウィンドウの左上隅にある デスクトップに切り替える オプションをクリックします。

設定を変更する

をクリックし、設定 を選択して Bitdefender Safepay™ を設定:

ドメインリスト
特定のドメインのウェブサイトをドメインリストに追加することで、それらのウェブサイトに通常のブラウザでアクセスした場合の Bitdefender Safepay™ の挙動を選択できます。
- 自動的に Bitdefender Safepay™ で開きます。
- Bitdefenderから警告を出し、操作を促すようにする。
- 通常のブラウザからこのドメインのページにアクセスする際は Bitdefender Safepay™ を使用しない。

ポップアップのブロック
ポップアップをブロックするには、該当するスイッチをクリックします。

ポップアップを許可するウェブサイトのリストを作成することも可能です。 リストには、完全に信頼できるウェブサイトのみを登録してください。

一覧にサイトを追加するには、該当の入力欄にアドレスを入力し、ドメインの追加 をクリックします。

リストからウェブサイトを削除するには、リストに表示された該当のサイトで「X」を選択してください。

プラグインを管理
Bitdefender Safepay™ で特定のプラグインを有効/無効にすることができます。

証明書を管理
証明書をシステムから証明書ストア（セキュリティ証明書が格納されているデータベース）に読み込むことができます。

Bitdefender Safepay™. で証明書を使用するには、証明書を読み込む を選択してウィザードに従います。

パスワード入力欄でステルスキーボードを自動起動
パスワードのフィールドを選択すると、バーチャルキーボードが自動的に表示されます。

該当のスイッチを使って機能を有効または無効にします。

印刷する前に確認を求める
印刷処理を開始する前に確認したい場合は、このオプションを有効にします。

ブックマークを管理する

一部またはすべてのウェブサイトの自動検出を無効にした場合、あるいは Bitdefender が特定のウェブサイトを検出しない場合は、Bitdefender Safepay™ にブックマークを追加することで、お気に入りのウェブサイトを簡単に開けるようになります。

Bitdefender Safepay™ のブックマークに URL を追加するには、次の手順に従ってください:

1. ブックマークページを開くには、アドレスバーの横にある アイコンをクリックします。

   注記
   Bitdefender Safepay™ を起動すると、ブックマークページがデフォルトで開きます。

2. +ボタンをクリックして、ブックマークを追加します。
3. ブックマークの URL とタイトルを入力し、作成 をクリックします。ブックマークしたページを毎回 Bitdefender Safepay™ で開きたい場合は、 Safepay で自動的に開く オプションにチェックを入れます。 URL は設定ページ内のドメインリストにも追加されます。

決済ブラウザの通知をオフにする

オンラインバンキングのサイトが検出されると、 Bitdefender 製品はポップアップウィンドウでその旨を通知するよう設定されています。

決済ブラウザの通知をオフにするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. 決済ブラウザ パネルで 設定 をクリックします。
3. 決済ブラウザの通知 をオフにします。

VPN と Safepay 決済ブラウザを使う

保護されていないネットワークで安全にオンラインバンキングや支払いを行えるよう、 Bitdefender は Safepay 決済ブラウザ実行時に VPN アプリも自動的に起動するよう設定することが可能です。

Safepay 決済ブラウザと VPN アプリの連携と開始するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. 決済ブラウザ パネルで 設定 をクリックします。
3. VPN と Safepay™ 決済ブラウザを使う をオンにします。

4.14. データ保護

ファイルを完全に削除

ファイルを削除すると、通常の方法ではファイルにアクセスすることができなくなります。 ただし新しいファイルで上書きされるまで、ファイルはハードディスクに保存されています。

Bitdefender のファイルシュレッダーは、データを物理的にハードディスクから削除することによって完全に削除します。

以下の手順で、パソコン上のファイルやフォルダをWindowsコンテキストメニューから簡単にかつ素早く完全削除することができます：

1. 完全に削除するファイルまたはフォルダを右クリックしてください。
2. 右クリックメニューからBitdefender > ファイル シュレッダーを選択してください。
3. 完全に削除 をクリックして、削除処理を続行することを確認します。

   Bitdefender がファイル シュレッダーを完了するまでお待ちください。
4. 結果が表示されます。 終了をクリックしてウィザードを終了します。

もしくは、 Bitdefender 管理画面からファイルを消去することも可能です:

1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
2. データ保護ウィンドウで、ファイル シュレッダー をクリックします。
3. ファイル シュレッダー ウィザードの手順に従ってください：
   a. フォルダを追加 ボタンをクリックして、永久に削除したいファイルまたはフォルダを追加します。

      または、これらのファイルまたはフォルダをこのウィンドウにドラッグします。
   b. 完全に削除 をクリックして、削除処理を続行することを確認します。

Bitdefender がファイル シュレッダーを完了するまでお待ちください。

c. 処理結果

結果が表示されます。 終了をクリックしてウィザードを終了します。

4.15. お子様保護

ペアレンタルコントロール機能では、この機能がインストールされているお子様のデバイス上での、インターネットおよび特定のアプリへのアクセスを制御することができます。 ペアレンタルコントロールの設定後は、お子様がデバイスで何をしているかや、過去 24 時間にお子様がいた場所などを簡単に確認できるようになります。 また、お子様の行動をより深く理解できるよう、このアプリケーションはお子様のオンラインでのアクティビティや嗜好についての統計データを提供します。

この機能に必要なものは、インターネット接続ができるコンピュータと、ウェブ ブラウザのみです。

Bitdefender ペアレンタルコントロールを設定することで以下を行えます:

- 不適切なウェブページをブロックします。
- 特定の時間帯 （レッスンの時間など） に、インターネットアクセスをブロックします。
- ゲーム、チャット、ファイル共有プログラムなどのアプリをブロックします。
- 連絡先リストにある連絡先からの通話や SMS メッセージを監視します。この機能は、Android デバイスでのみ利用できます。
- 連絡先リストまたは不明な連絡先からの通話や SMS メッセージをブロックします。
- 制限エリアを設定します。

インターネットに接続されたコンピュータまたはモバイルデバイス上で Bitdefender アカウントにログインすることで、いつでもどこでもお子様のアクティビティをチェックしたり、ペアレンタル コントロールの設定の設定を変更したりできます。

4.15.1. ペアレンタルコントロールにアクセスする - 子供

ペアレンタルコントロールのセクションにアクセスすると、子供 ウィンドウが利用できる状態になります。 ここでは、お子様用に作成したすべての

プロファイルを表示および変更できます。　プロフィールはプロフィールカードとして表示されるため、簡単に管理し、状態をすばやく確認することができます。

お子様のプロファイルを作成した後は、さらに細かい設定をカスタマイズすることで、お子様のアクティビティの監視や、インターネットおよび特定のアプリケーションへのアクセスの制限などを行えます。

ペアレンタルコントロールの設定には、インターネットに接続されているコンピュータまたはモバイルデバイス上の Bitdefender Central からアクセスできます。

Bitdefender アカウントにアクセスします:

- インターネットアクセスがあるデバイスから：
  1. Bitdefender Centralにアクセスします。
  2. メールアドレスとパスワードを使って Bitdefender アカウントにログインします。
  3. ペアレンタルコントロール パネルを選択します。
  4. 表示される 子供 ウィンドウでは、各デバイスのペアレンタルコントロールのプロファイルを管理および設定できます。
- Bitdefenderの製品画面から：
  1. Bitdefender インターフェイスのナビゲーションメニューにある プライバシー をクリックします。
  2. ペアレンタルコントロール パネルで設定をクリックします。

     Bitdefender アカウントの Web ページにリダイレクトされます。 ご自身の認証情報を使ってログインしていることを確認してください。
  3. ペアレンタルコントロール 機能を選択します。
  4. 表示される 子供 ウィンドウでは、各デバイスのペアレンタルコントロールのプロファイルを管理および設定できます。

注記
管理者アカウントで、コンピュータにログオンします。 管理者権限を持ったユーザー（システム管理者）のみが、ペアレンタル コントロール機能を設定することができます。

4.15.2. お子様のプロフィールを追加する

お子様のアクティビティのモニタリングを開始するには、お子様のプロファイルをセットアップし、お子様のデバイスに Bitdefender のペアレンタルコントロールアプリをインストールする必要があります。

お子様のプロフィールをペアレンタルコントロールに追加するには：

1. Bitdefender Central から、ペアレンタルコントロール パネルにアクセスします。
2. 子供 ウィンドウ右側の プロファイルの追加 をクリックします。
3. 対応するフィールドに名前、生年月日などを設定します。 プロフィール画像を追加するには、ファイルを選択リンクをクリックします。 次のステップ をクリックして続行します。

   お子様の生年月日を設定すると、お子様の年齢カテゴリーに適切と判断されたウェブ設定が自動的に読み込まれます。
4. お子様のデバイスに Bitdefender Total Security がすでにインストールされている場合は、リストからデバイスを選択して監視したいアカウントを選択します。 保存 をクリックします。

   お子様が Android または iOS デバイスを使用していて、 Bitdefender ペアレンタルコントロールアプリがまだインストールされていない場合は、デバイスの追加 をクリックします。 お子様が Mac デバイスを使用していて、 Bitdefender Antivirus for Mac がまだインストールされていない場合は同じボタンをクリックします。 アプリをインストールしたいオペレーティングシステムを選択し、次のステップ をクリックして続行します。
5. Bitdefender アプリケーションのダウンロード用リンクを受け取るメールアドレスを入力し、インストール用リンクを送信 をクリックします。

重要項目

Windows ベースのデバイスでは、サブスクリプションに含まれている Bitdefender Total Security をダウンロードしてインストールする必要があります。

macOS デバイスでは、 Bitdefender Antivirus for Mac ダウンロードしてインストールする必要があります。

Android または iOS デバイスでは、 Bitdefender ペアレンタルコントロールアプリをダウンロードしてインストールする必要があります。

複数のデバイスを同じプロファイルに割り当てる

複数のデバイスを 1 つのプロファイルを割り当てて、以下のように同じ制限を適用することができます:

1. Bitdefender Centralにアクセスします。
2. ペアレンタルコントロール パネルを選択します。
3. 任意のプロファイルカード上の ⋮ アイコンをクリックして、 デバイスを選択します。
4. 利用可能なデバイスのリストで、プロファイルを割り当てたいデバイスを選択します。

   お子様が Android または iOS デバイスを使用していて、 Bitdefender ペアレンタルコントロールアプリがまだインストールされていない場合は、デバイスの追加 をクリックします。 お子様が Mac デバイスを使用していて、 Bitdefender Antivirus for Mac がまだインストールされていない場合は同じボタンをクリックします。 アプリをインストールしたいオペレーティングシステムを選択し、次のステップ をクリックして続行します。

   Bitdefender アプリケーションのダウンロード用リンクを受け取るメールアドレスを入力し、インストール用リンクを送信 をクリックします。
5. 新しいデバイス上でインストール処理が完了したら、リストから選択してプロファイルを適用します。
6. 保存 を選択します。

注記
お子様が、割り当てられているデバイスにアクセスすることを一時的にブロックしたいときは、そのお子様のプロファイルを「一時停止」に設定してください。 これを行うには、任意のプロファイルを選択してお子様のプロファイルの写真上の ⏸ をクリックするだけです。

ペアレンタルコントロールにBitdefender Centralをリンクする

Android および iOS 上でお子様のオンラインアクティビティを監視するには、アプリから Bitdefender アカウントにログインし、お子様のデバイスをこのアカウントにリンクする必要があります。

デバイスを Bitdefender アカウントにリンクするには:

- Android の場合:

1. 弊社サーバから送信されるメールに記載されているボタンを選択します。 Google Play ストアにリダイレクトされます。

   Bitdefender アカウントで、お子様のメールアドレス宛てにダウンロード用リンクを送信することを選択しなかった場合は、Google Play で Bitdefender ペアレンタルコントロールアプリを検索してください。

2. Bitdefender ペアレンタルコントロールのウィンドウ内でインストールをタップし、許可を求められた場合は受諾をタップします。 Bitdefender は、お子様のアクティビティ情報を送信するためにアクセス許可を必要とします。拒否された場合、アプリはインストールされません。

3. ペアレンタルコントロールアプリを開きます。

4. アプリの初回起動時には、製品の機能に関する情報を含むイントロウィザードが表示されます。 チュートリアルを続ける場合は 次へ、ウィザードを閉じるには スキップ を選択します。

5. インストールを続行する前に、サブスクリプション契約に同意する必要があります。 サブスクリプション契約には、 Bitdefender を使用する上で守っていただく条件が記載されていますので、必ずよくお読みください。 対応するチェックボックスを選択し、続行 をタップします。

6. 既存の Bitdefender アカウントにログインします。 Bitdefender アカウントをお持ちでない場合は、当該オプションを使って新しいアカウントを作成してください。 また、Facebook、Google、Microsoft アカウントなどでサインインすることもできます。

7. ON にするく をタップすると、アプリのアクセシビリティに関するオプションをオンにできる画面にリダイレクトされます。 画面の指示に従ってアプリを正しくセットアップしてください。

8. 許可 をタップすると、アプリのユーザーアクセス許可に関するオプションをオンにできる画面にリダイレクトされます。 画面の指示に従ってアプリを正しくセットアップしてください。

9. アクティベート をタップすると、アプリの管理者権限の有効化オプションをオンにできる画面にリダイレクトされます。 画面の指示に従ってアプリを正しくセットアップしてください。

   これにより、お子様がペアレンタルコントロールアプリをアンインストールすることはできなくなります。

10. デフォルトの SMS アプリの代わりにペアレンタルコントロールのメッセージアプリを使用するには、変更 をタップしてから「OK」をタップします。 興味がないをタップすると、デフォルトの SMS アプリの使用を継続したまま、次の手順へと進みます。 このオプションは、Android 4.4 以降が動作するデバイスでのみ表示されます。
11. デバイスをお子様のプロファイルに割り当てます。

- iOS の場合:

1. 弊社サーバから送信されるメールに記載されている ボタンを選択してアプリをインストールします。
2. ペアレンタルコントロールアプリを開きます。
3. インストールを続行する前に、サブスクリプション契約に同意する必要があります。 サブスクリプション契約には、 Bitdefender ペアレンタルコントロールを使用する上で守っていただく条件が記載されていますので、必ずよくお読みください。 対応するチェックボックスを選択し、続行 をタップします。
4. 既存の Bitdefender アカウントにログインします。 Bitdefender アカウントをお持ちでない場合は、当該オプションを使って新しいアカウントを作成してください。 また、Facebook、Google、Microsoft アカウントなどでサインインすることもできます。
5. 製品の機能に関する情報を含むイントロウィザードが表示されます。次へ をクリックして続行します。
6. アプリに必要なすべてのアクセス要求を許可することを求められます。許可をタップします。
7. Bitdefender がデバイスの位置情報を特定できるように、デバイスの位置情報へのアクセスを許可してください。
8. アプリによる通知を許可します。
9. デバイスをお子様のプロファイルに割り当てます。
10. デバイスに Bitdefender ペアレンタルコントロールアプリを初めてインストールするときは、MDM（モバイルデバイス管理）プロファイルをインストールする必要があります。 次の手順に進みます。
    a. 許可をタップすると、設定にリダイレクトされます。
    b. Installをタップして、 Bitdefenderがアクティベーションプロセスを続けるために必要なMDM（モバイルデバイス管理）プロファイルをインストールします。

スマートフォンを保護するためにPINコードが設定されている場合は、それを使用する必要があります。

c. CAルート証明書およびモバイルデバイス管理に関連する情報をお読みください。

d. 要約された条件に同意する場合は、インストールをタップします。

e. リモート管理アラート内で信頼をタップし、完了をクリックしてウィンドウを閉じます。

注記
「プロファイルのインストールに失敗しました」というエラーメッセージが出た場合、現在インストールされている MDM プロファイルを一旦削除してから、もう一度インストールする必要があります。 現在の MDM プロファイルを削除するには、設定> 一般 > デバイス管理 > Bitdefender を開きます。 検出されたプロファイルを選択し、管理の削除をタップします。 スマートフォンを保護するためにPINコードが設定されている場合は、それを使用する必要があります。 もう一度管理の削除をタップして選択を確定します。 Bitdefender ペアレンタルコントロールアプリを開き、再インストール をタップして所定の手順を実行してください。 問題が解決しない場合は、bdparental@bitdefender.comで当社チームにメールをお送りください。

お子様のパソコン利用を監視する

Bitdefenderはお子様がインターネット上でどのような行動をとっているのかを把握しやすくします。

これにより、お子様がどのようなウェブサイトやアプリを利用したか、どのようなアクティビティがペアレンタルコントロール機能によってブロックされたかなどを、いつでも細かくチェックできます。

設定によって、レポートには各イベントに関する以下のような詳細情報が含まれます:

- イベントの状況。
- 通知の重要度。
- デバイス名。
- イベントの日付と時間。

インターネットトラフィックやお子様がアクセスしたアプリ、オンラインアクティビティなどを監視するには:

1. Bitdefender Central から、ペアレンタルコントロール パネルにアクセスします。
2. 任意のデバイスカードを選択します。

   「アクティビティ」ウィンドウでは、興味のある情報を表示して確認できます。　もしくは、監視しているデバイスカードの今日のアクティビティを表示 リンクをクリックすると、アクティビティ ウィンドウが開きます。

一般設定の変更方法

初期設定でペアレンタルコントロールが有効の場合、お子様の行動は履歴に記録されます。

メール通知を受け取るには:

1. Bitdefender Central から、ペアレンタルコントロール パネルにアクセスします。
2. 設定 タブを選択します。
3. アクティビティレポートを受け取るには、対応するオプションを有効にします。
4. メール通知を受け取りたいメールアドレスを入力します。
5. 以下の項目についてメール通知を受け取ります :
   - ブロックされたwebサイト
   - ブロックされたアプリケーション
   - 制限されたエリア
   - ブロックされた/不明な電話番号からの着信または SMS
6. 保存 をクリックします。

プロフィールを編集する

既存のファイルを編集するには:

1. Bitdefender Centralにアクセスします。
2. ペアレンタルコントロール パネルを選択します。
3. 任意のプロファイルカードの ⋮ アイコンをクリックし、編集 を選択します。

4. 任意の設定をカスタマイズ後、保存を選択します。

プロフィールを削除する

既存のファイルを削除するには:

1. Bitdefender Centralにアクセスします。
2. ペアレンタルコントロール パネルを選択します。
3. 任意のプロファイルカードの ⋮ アイコンをクリックし、削除 を選択します。
4. 選択内容を確定します。

4.15.3. ペアレンタルコントロールのプロファイルを設定する

お子様のモニタリングを開始するには、 Bitdefender のペアレンタルアドバイザーアプリがインストールされているデバイスにプロファイルを割り当てる必要があります。

お子様のプロファイルを追加した後は、さらに細かい設定を行うことで、お子様のアクティビティの監視や、インターネットおよび特定のアプリケーションへのアクセスの制限などを行えます。

プロファイルの設定を開始するには、子供 ウィンドウで任意のプロファイルカードを選択します。

各タブをクリックして、対応するデバイスのペアレンタルコントロール機能を設定します。

- アクティビティ – 当日のすべてのアクティビティ、興味、場所、友達とのやり取りなどが表示されます。
- アプリケーション– ゲームやメッセージングソフト、ムービーなど、特定のアプリケーションへのアクセスを制限することができます。
- ウェブサイト– ウェブナビゲーションをフィルタリングできます。
- 電話の連絡先 – お子様の連絡先リストの中で、誰がお子様に電話で連絡を取っても良いかを指定できます。
- お子様の場所 – お子様にとって安全な場所、および安全でない場所を設定できます。

- スクリーン時間 - お子様のプロファイルで指定されている、デバイスへのアクセスをブロックできます。

アクティビティ

「アクティビティ」ウィンドウでは、直近 24 時間のお子様のオンラインおよびオフラインでの行動についての詳細な情報を確認できます。 過去からのアクティビティを表示するには、ウィンドウの左上隅にあるカレンダーのアイコンをクリックします。

アクティビティによって、このウィンドウには以下に関する情報が表示されます:

- 場所 - お子様がアクセスしていた場所を確認できます。
- 興味- お子様が訪問したウェブサイトのカテゴリについての情報を確認できます。 不適切なコンテンツを確認 のリンクをクリックして、特定のコンテンツへのアクセスを許可または拒否できます。
- コミュニケーション - お子様がやり取りした連絡先を確認できます。 連絡先の管理 リンクをクリックすると、お子様がやり取りしても良い連絡先と、やり取りすべきでない連絡先を選択できます。
- アプリ- ここには、お子様が使用したアプリが表示されます。 特定のアプリケーションへのアクセスをブロックまたは許可するには、アプリの制限を見直す リンクをクリックします。
- 終日アクティビティ - ここでは、お子様が自分に割り当てられているデバイス上でオンラインだった時間帯と、オンライン時の位置情報を確認できます。 収集される情報は当日のものです。

アプリケーション

「アプリケーション」ウィンドウでは、Windows、macOS、Android、および iOS デバイス上でのアプリ実行をブロックすることができます。 ゲーム、メディア、メッセージング、およびその他カテゴリに属するソフトウェアをこの方法をブロックできます。

さらにここでは、過去 30 日間に最も多く使用された上位アプリと、それらのアプリの使用時間も一緒に表示することができます。 アプリの使用時間に関する情報、Windows、macOS、および Android デバイスからのみ取得できます。

特定のユーザーアカウントに対してアプリケーション制限を設定するには:

1. 割り当てられているデバイスのリストが表示されます。

アプリへのアクセスを制限したいデバイスのカードを選択します。

2. 次のユーザーが使用したアプリを管理... をクリックします。

   インストールされているアプリのリストが表示されます。

3. お子様に使用させたくないアプリの横にある ブロック を選択します。

インストールされているアプリの監視を停止するには、ウィンドウの右上隅にあるアプリの監視オプションをオフにします。

webサイト

「ウェブサイト」ウィンドウでは、好ましくないコンテンツを含むウェブサイトをブロックすることができます。 この方法を使って、ビデオ、ゲーム、メディア、メッセージングソフトウェアなど、危険な可能性のあるコンテンツを含むウェブサイトをブロックすることができます。

この機能は、対応するスイッチを使って有効または無効にできます。

設定したお子様の年齢に応じて、「興味」リストではいくつかのカテゴリーが予め有効になっています。 クリックすることで、特定のカテゴリーへのアクセスを許可または禁止できます。

このチェックマークは、お子様が特定のカテゴリーに関連するコンテンツにアクセスできないことを意味します。

Webサイトを許可またはブロックする

特定のウェブページへのアクセスを許可または制限するには、以下の手順で例外リストに追加します:

1. 管理ボタンをクリックします。
2. 許可またはブロックしたいウェブページを、対応するフィールドに入力します。
3. 許可 または ブロック を選択します。
4. FINISHをクリックして変更を保存します。

注記
ウェブサイトへのアクセス制限は、お子様のプロファイルに割り当てられた Window、Android、および macOS デバイスに対してのみ設定できます。

電話

「電話連絡先」ウィンドウでは、お子様の連絡先リストの中で、誰がお子様に電話で連絡を取っても良いかを指定できます。

連絡先の特定の電話番号を制限するには、まずお子様のプロファイルを使用 Android デバイスに追加する必要があります。

1. Bitdefender Central の ペアレンタルコントロール パネルを選択します。
2. 任意のカードのデバイスにペアレンタルコントロールをインストールのリンクをクリックします。
3. 割り当てたい Android デバイスを選択し、保存 クリックします。 お子様のプロファイルに割り当てたい Android デバイスがリストにない場合は、次の手順に従ってください:
   a. デバイスの追加 をクリックします。
   b. リストから Android を選択し、次のステップ をクリックして続行します。
   c. Bitdefender アプリケーションのダウンロード用リンクを受け取るメールアドレスを入力し、インストール用リンクを送信 をクリックします。
   d. 弊社サーバーから届いたメールに記載されているインストール手順に従って、任意のデバイスにアプリをインストールしてください。
4. Bitdefender Central の電話 タブをタップします。

   カードのリストが表示されます。 カードは、お子様の Android スマートフォン上の連絡先を示しています。
5. ブロックしたい電話番号のカードを選択します。

   表示されるチェックマークは、選択した電話番号ではお子様につながらないことを示しています。

   SMS メッセージは、お子様のデバイス上で Bitdefender ペアレンタルコントロールを設定した際に、デフォルトのアプリの代わりにペアレンタルコントロールのメッセージングアプリの使用を選択した場合のみブロックされます。

不明な電話番号への、あるいは不明な電話番号からの発着信は、不明な「発信者番号なし」のプライベート番号からのコールをブロックします のスイッチを有効にすることでブロックできます。

注記
音声通話に対する制限は、お子様のプロファイルに割り当てられた Android デバイスに対してのみ設定でき、着信と発信の両方に対して適用されます。

元の場所

デバイスの現在地をGoogle Mapsで確認します。 現在地は5秒ごとに再読み込みされ、移動中でも正確に位置を捉えることができます。

位置情報の精度はBitdefenderが認識できるかどうかによって異なります。

- デバイスのGPSが有効になっていて、GPS衛星からの電波が受信出来る状態（例：屋外にいる場合）にある場合は、位置情報は数メートルの範囲にまで絞り込むことができます。
- デバイスが屋内にあり、デバイス側のWi-Fiが有効になっていて、さらに無線通信環境が近くにある場合、位置情報は十数メートルの範囲まで絞り込むことができます。
- それ以外の場合、位置情報はモバイルネットワークの情報のみで判定されるため、絞り込める範囲は数百メートルとなります。

位置情報と到着確認を設定する

お子様が不適切な場所にアクセスしないよう、安全な場所と安全でない場所のリストを作成できます。 あらかじめ定義されたエリアにお子様が単独で入るたびに、お子様が安全であることを確認する通知がペアレンタルコントロールアプリに表示されます。 無事に到着しました をタップすると、Bitdefender アカウントに最終目的地に到着したことを知らせる通知が送られます。

お子様から確認がない場合でも、 Bitdefender アカウント内でお子様のプロフィールを確認することで、お子様の位置情報の履歴をいつでも確認することができます。

場所を設定するには:

1. お子様の場所 ウィンドウのフレーム内の デバイス をクリックします。
2. デバイスの選択 をクリックし、設定したいデバイスを選択します。
3. エリア ウィンドウで エリアの追加 ボタンをクリックします。
4. 場所の種類を 安全 または 制限 のいずれかから選択します。
5. お子様がアクセスできる（またはできない） エリアに付ける名前を入力します。

6. 半径 スライドバーで、モニタリングの適用範囲を設定します。
7. 設定を保存するには エリアを追加 をクリックします。 お子様が一人で行動するのかどうかを尋ねられます。 「はい」または「いいえ」で確認します。

注記
位置情報トラッカーは、 Bitdefender ペアレンタルコントロールアプリをインストールした Android および iOS デバイスの位置情報をモニタリングする目的に使用できます。

利用時間

「スクリーン時間」には、割り当てられたデバイスの今日の使用時間、設定した制限時間までの残り時間、そして選択されているプロファイルの状態 （アクティブ/一時停止） が表示されます。 このウィンドウでは、寝る時間、宿題時間、レッスン時間など、1 日の色々な時間帯に対して時間制限を設定することもできます。

時間制限

時間制限の設定を開始するには:

1. 時間制限の確認をクリックします。
2. 時間制限の設定 エリアで、時間制限を新規追加 をクリックします。
3. 設定する制限に名前を付けてください （たとえば寝る時間、宿題、テニスレッスンなど）。
4. 制限を適用したい日付と時間帯を設定し、追加 をクリックして設定を保存します。

設定した制限を編集するには「スクリーン時間」ウィンドウに移動し、編集したい制限を選ぶと表示される アイコンをクリックします。

制限を削除するには「スクリーン時間」ウィンドウに移動し、編集したい制限を選ぶと表示される アイコンをクリックします。

日ごとの制限

1 日の使用制限は、Android および Windows デバイスに対して適用できます。 制限に達した後にプロファイルを一時停止すると、その設定は Windows、macOS、Android および iOS など割り当てられているすべてのデバイスに対して適用されます。

1 日の使用制限を設定するには:

1. 時間制限の確認をクリックします。
2. 時間制限の設定 エリアで、1 日の時間制限を新規追加 をクリックします。
3. 制限を適用したい日時を設定し、保存 をクリックして設定を保存します。

4.16. デバイス盗難対策

ノートパソコンの盗難は個人レベルのみならず、企業レベルでも大きな問題となります。 ハードウェアを失うダメージ以上に、大切なデータを失ったときの精神的ダメージや経済的ダメージの方が大きい場合もあります。

しかしそれでも多くの人はパソコン紛失・盗難によって大切な個人情報や仕事のデータを失わないための対策を行なわない場合があります。

Bitdefender の窃盗防止機能では、ノートパソコンの位置情報をリモートから確認し、ロックをかけたり、データをすべて消去したりできるため、万が一ノートパソコンが盗難に遭ったり紛失したりした場合に備えることができます。

盗難対策機能を利用するには、以下の条件を満たさなければなりません :

- コマンドは、 Bitdefender アカウントからのみ送信できます。
- コマンドを受信するには、ノートパソコンがインターネットに接続されている必要があります。

盗難対策は次のように機能します :

探す
: デバイスの位置をGoogle Mapsで確認できます。

  位置情報の精度はBitdefenderが認識できるかどうかによります。 パソコンの Wi-Fi が有効になっていて、その範囲内にワイヤレスネットワークがある場合、数十メートル単位で位置情報が確認されます。

  Wi-Fi が利用できない場所で、ノートパソコンが有線 LAN でネットワーク接続されている場合、位置情報には IP アドレスが使用されますが、精度は Wi-Fi よりも大幅に低くなります。

アラート
: デバイスにリモートアラートを送信します。

  この機能はモバイルデバイスでのみ利用できます。

ロックする
ノートパソコンの画面をロックして、アンロック用の 4 桁の PIN 番号を設定します。 ロック コマンドを送信するとシステムが再起動され、設定した PIN 番号を入力しない限り Windows にログインし直すことはできなくなります。

Bitdefender で、お使いのノートパソコンに不正にアクセスしようとした人物の写真を撮影するには、対応するチェックボックスをオンにします。 スナップフォトはフロントカメラで撮影され、タイムスタンプ付きで窃盗防止ダッシュボードに表示されます。 最も新しい 2 枚の写真のみが保存されます。

この機能は、フロントカメラを搭載したノートパソコンでのみ利用できます。

データ消去
システム上のすべてのデータを削除します。 消去 コマンドを送信すると、ノートパソコンが再起動し、ハードディスクのすべてのパーティション上のデータが消去されます。

IPアドレスを表示
選択したデバイスの前回の IP アドレスを表示します。 表示するには IP を表示 をクリックします。

窃盗防止機能はインストール後に有効になり、インターネットに接続されているデバイスから Bitdefender アカウントを経由してアクセスできます。

窃盗防止機能を使う

窃盗防止機能には、以下のいずれかの方法でアクセスできます:

- Bitdefender のメイン管理画面から:
  1. Bitdefender インターフェイスのナビゲーションメニューにある ユーティリティ をクリックします。
  2. 盗難対策機能をチェックする をクリックします。
  3. 表示される Bitdefender Central ウィンドウで任意のデバイスカードをクリックし、窃盗防止 を選択します。
- インターネットアクセスがあるデバイスから :
  1. ウェブブラウザのウィンドウを開いて以下を開きます: https://central.bitdefender.com

2. メールアドレスとパスワードを使って Bitdefender アカウントにログインします。
3. マイデバイス パネルを選択します。
4. 任意のデバイスカードをクリックして 窃盗防止 を選択します。
5. ご利用される機能を選択してください：

   IP を表示 – デバイスの前回の IP アドレスを表示します。
   位置確認– デバイスの位置を Google マップで表示します。
   アラート– デバイスにアラートを送信します。
   ロック – ノートパソコンをロックし、アンロックに必要となる PIN コードを設定します。
   ワイプ – ノートパソコン上のすべてのデータを削除します。

   重要項目
   デバイスをワイプすると、盗難対策の機能も全て機能しなくなります。

4.17. USBメモリ・ワクチンツール

Autorun（自動実行）はWindows OSの標準機能の一つで、接続されたメディア上のファイルを自動起動するための便利な機能です。 例えばこの機能を利用して、ソフトウェアのインストールCDをドライブへ挿入したと同時に自動で実行することができます。

ただし、この機能は脅威などに悪用され、USBメモリや記憶装置から自動で脅威コードを実行させ、パソコンが脅威に感染してしまう場合もあります。ここ数年も、このようにAutorunを悪用した攻撃が数多くみられました。

USBメモリ・ワクチンツールを使用すれば、NTFS、FAT32、FATでフォーマットされたUSBメモリから自動的に脅威を実行されるのを防ぐことができます。 USBにワクチンが投与されると、そのUSBがWindowsパソコンに挿入されたとしても、パソコンを脅威感染させるアプリケーションを自動実行できない状態にします。

USB デバイスを安全にするには:

1. USBメモリをパソコンへ挿入してください。
2. パソコンのエクスプローラーから接続したUSBメモリを探し、アイコンを右クリックします。
3. 右クリックメニュー内のBitdefenderにカーソルを当て、ワクチンを投与するを選択します。

注記
USBメモリにすでにワクチンが投与されている場合は、このUSBメモリはAutorun脅威から保護されていますというメッセージが表示されます。

パソコンがワクチン投与されていないUSBメモリから脅威を自動実行してしまわないようにするには、メディアAutoronの機能を無効にしてください。詳細については、「自動脆弱性監視を使用」（p. 120）をご参照ください。

5. システム最適化

5.1. ユーティリティ

Bitdefender には、システムの完全性を維持するために役立つ「ユーティリティ」セクションが用意されています。 メンテナンス・ツールは、システムの反応性を改善させたり、ハードディスク使用を効率化させるために重要なツールです。

Bitdefender は次のような PC 最適化ツールを提供しています:

- クイック最適化ツール では、シングルクリックで複数のタスクを実行し、システムの速度を向上することができます。
- スタートアップ最適化ツール は、PC の再起動時に不要なアプリケーションを起動させないことで、システムの起動時間を短縮します。
- ディスククリーンアップは、ディスクの容量を圧迫している主な原因のファイルを特定し、そのファイルを削除するかどうかの選択肢を提示します。

5.1.1. シングルクリックでシステムの速度を最適化

ハードディスクの故障、不要なレジストリファイルやブラウザ履歴などのデータは、コンピュータのパフォーマンスを低下させる要因となります。これらをすべて、ボタンのシングルクリックで修復できるようになりました。

ワンクリック オプティマイザは、複数のクリーンアップタスクを同時に実行し、不要なファイルを検出して削除します。

クイック最適化ツールの処理を開始するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある ユーティリティ をクリックします。
2. デバイスを最適化する をクリックします。
   a. 分析中

      Bitdefender によるシステム問題の検出が終了するまで待ちます。

      - ディスククリーンアップ – 不要なファイルやフォルダを検出します。

- レジストリのクリーンアップ - Windows レジストリ内の無効なデータを検出します。
- プライバシークリーンアップ - インターネット一時ファイル、クッキー、ブラウザのキャッシュおよび履歴をクリーンアップします。

見つかった問題が表示されます。 クリーニング処理を実行する前に、詳細を表示 リンクをクリックして内容を確認してください。 OPTIMIZE をクリックしてください。

b. 最適化

Bitdefender によるシステム最適化が完了するのを待ちます。

c. 個別の問題

処理結果を確認することができます。

最適化処理の詳細な情報を確認するには、詳細レポートを表示 リンクをクリックします。

5.1.2. PC の起動時間を最適化する

拡張システム起動は、不要なアプリケーションも起動してしまうのが大きな問題です。 システムが起動するまでに数分間もかかってしまうと、時間の無駄はもちろん、生産性にも大きく影響します。

「起動オプティマイザ」画面では、システム起動時にどのアプリケーションが実行されているかが表示され、各アプリケーションの挙動を管理できます。

スタートアップ最適化ツールの処理を開始するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある ユーティリティ をクリックします。
2. デバイスの起動を最適化 をクリックします。

a. アプリケーションを選択

システム起動時に実行されるアプリケーションのリストが表示されます。 起動時に無効または延期する項目を選択します。

b. コミュニティが選択した設定

他の Bitdefender ユーザーが、あなたが選択したアプリに対して選んだオプションを確認できます。

c. システム起動時間

ウィンドウ上部のスライダーには、システムおよび選択したアプリケーションの起動時間が表示されます。

システムおよびアプリケーションの起動時間に関する情報を取得するには、システムの再起動が必要です。

d. スタートアップの状態

- 有効化. システム起動時にアプリケーションを起動させたい場合、このオプションを選択します。 このオプションはデフォルトで有効になっています。
- 遅延させる. プログラムがシステム起動時に実行されるのを延期する場合、このオプションを選択します。 つまり、選択されたアプリケーションは、ユーザーがシステムにログインしてから 5 分後に起動するということです。 遅延 機能は予め設定済みのため、ユーザーが設定を変更することはできません。
- 無効にする. プログラムがシステム起動時に実行されないようにするには、このオプションを選択します。

e. 結果

起動時に実行するプログラムを延期したり、無効にした後の推定システム起動時間などが表示されます。

これらの情報をすべて表示するには、システムの再起動が必要な場合があります。

OK をクリックすると、変更が保存され、画面が自動で閉じます。

注記
サブスクリプションの有効期限が終了したり、 Bitdefender をアンインストールしたりした場合、起動時に実行を抑制されていたプログラムは、元の起動設定に戻ります。

5.1.3. ディスクを最適化する

不要なファイルやフォルダは、システム速度低下の原因となる場合があります。 そのため、定期的なクリーンアップを実施してシステム速度を向上することをお勧めします。

Bitdefender ディスククリーンアップを使うと、ディスクの容量を圧迫している主な原因のファイルを特定し、簡単にディスクの空き容量を増やすことができます。 また、特定されたファイルに対して実行する操作を選択できます。

システムのクリーンアップを開始するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある ユーティリティ をクリックします。
2. デバイスをクリーンアップ をクリックします。
3. 「ディスククリーンアップ」機能に初めてアクセスすると、機能の紹介が表示されます。 わかりました。 をクリックして続行します。

   a. ドライブとデバイス

      利用可能なディスクの一覧が表示されます。 Windows のシステムディスクに加えて、外付けハードディスクや USB デバイスもスキャンされ、一覧に表示されます。 クリーンアップしたいディスク領域で ドライブを解析 をクリックします。

   b. ドライブの分析中. . .

      選択したドライブの解析を行います。 Bitdefender が大きなファイルやフォルダを検索し終えるまで待ちます。

   c. 個別の問題

      ここで処理結果を確認することができます。 ウィンドウの左側にある、ソート順 ドロップダウンリストから、結果を表示したい順序を選択します。 結果はサイズ（10MB～5GB 超）または種類（ファイルが拡張子ごとに別フォルダにソートされます）でソートすることができます。

      削除したいファイルを選択し、選択内容を確定をクリックして削除処理を開始します。

      システムの動作に関わる保護されたファイルや重要なファイルも特定されますが、選択したり削除したりすることはできません。

      選択したファイルが属しているフォルダにアクセスするには アイコンをクリックします。

   d. 選択内容を確定

      選択したファイルの一覧が表示されます。 これらのファイルが本当に不要かどうかもう一度確認してください。この操作を実行した後にファイルをごみ箱から復元することはできません。 削除をクリックして選択内容を確定します。

   e. 処理結果

      処理の状況が以下のように表示されます:

選択したファイルはすべて削除されました。
選択したファイルのうち 1 つまたは複数を削除できなかったか、あるいは選択したファイルを 1 つも削除できませんでした。

完了をクリックして、ウィンドウを閉じてください。

5.2. プロファイル

仕事、映画鑑賞、ゲームなどのアクティビティは、特に Windows アップデート処理やメンテナンスタスクと同時に実行した場合、システムパフォーマンスの低下を招きやすくなります。 Bitdefender では、任意のプロフィールを選択して適用することで、システム設定を適切に調整し、インストールされている特定のアプリケーションのパフォーマンスを向上します。

Bitdefender には以下のプロファイルが用意されています:

- 仕事プロファイル
- 動画プロファイル
- ゲームプロファイル
- 公共Wi-Fiのプロファイル
- バッテリーモード・プロファイル

プロファイル を使用しない場合は、標準 というプロファイルがデフォルトで有効になり、最適化処理は一切行われません。

アクティビティに基づき、以下の製品設定が仕事、動画再生、およびゲーム プロファイル有効時に適用されます:

- Bitdefender の警告とポップアップ表示がすべて無効になります。
- 自動アップデートを延期します。
- スケジュール設定されているスキャンを延長します。
- サーチ アドバイザを無効にします。
- 特別キャンペーンの通知は無効になっています。

アクティビティに基づき、以下のシステム設定が仕事、動画再生、およびゲーム プロファイル有効時に適用されます:

- Windows 自動更新を延期します。
- Windows アラートおよびポップアップが無効になります。
- 不要なバックグラウンドプログラムは一時停止します。

- 最高のパフォーマンスを得るため、ビジュアル効果を調節します。
- メンテナンスタスクが延期されます。
- 電力設定を調整します。

公共 Wi-Fi プロファイル実行時、 Bitdefender Total Security は自動的に以下のプログラム設定を実行します: ▪

- 高度な脅威に対する防御は有効です
- Bitdefender ファイアウォールがオンになり、以下の設定がワイヤレスアダプタに対して適用されます:
  - ステルスモード - ON
  - ネットワークの種類 - 公共
- オンライン脅威対策の以下の設定がオンになっています:
  - 暗号化 Web スキャン
  - 詐欺サイトからの保護
  - フィッシングサイトからの保護

5.2.1. 仕事プロファイル

メールの送受信、遠くの同僚とのビデオチャット、デザインアプリケーションを使った作業など、複数のタスクを同時に実行すると、システムのパフォーマンス低下につながる可能性があります。 ワークプロファイルは、一部のバックグラウンドサービスやメンテナンスタスクをオフにすることで作業効率の向上をサポートします。

ワークプロファイルを設定する

ワークプロファイル時に実行するアクションを設定するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. プロファイル タブを選択します。
3. 仕事プロファイル エリアにある 設定 ボタンをクリックします。
4. 以下のオプションにチェックを入れて、適用したいシステム調整を選択します:
   - 仕事関連のプログラムのパフォーマンスを向上させる

- 仕事プロファイル用に製品設定を最適化
- バックグラウンド・プログラムの起動やメンテナンスタスクの実行を延期させる
- Windows自動アップデートを延期する

5. 保存 をクリックして変更を保存し、ウィンドウを閉じます。

ワークプロファイルの一覧にアプリケーションを手動で追加する

特定の仕事用アプリケーションを起動した際に、 Bitdefender が自動的に仕事プロファイルに切り替わらない場合は、当該アプリを 仕事アプリケーションリスト に手動で追加できます。

仕事プロファイルのアプリケーションリストに手動でアプリを追加するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. プロファイル タブを選択します。
3. 仕事プロファイル エリアにある 設定 ボタンをクリックします。
4. 仕事プロファイル設定 ウィンドウで アプリケーション リスト をクリックします。
5. 追加 をクリックします。

   新しいウィンドウが表示されます。 アプリケーションの実行ファイルを選択して、OKをクリックしてリストに追加します。

5.2.2. 動画プロファイル

HD 動画などの高品質なビデオコンテンツの再生は、非常に多くのシステムリソースを必要とします。 ムービープロファイルは、ムービーの視聴を快適に行えるように、システムおよび製品の設定を調節します。

ムービープロファイルを設定する

ムービープロファイル時に実行するアクションを設定するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. プロファイル タブを選択します。
3. 動画再生プロファイル エリアにある 設定 ボタンをクリックします。

4. 以下のオプションにチェックを入れて、適用したいシステム調整を選択します:
   - ビデオプレイヤーのパフォーマンスを向上させる
   - 動画プロファイル用に製品設定を最適化
   - バックグラウンド・プログラムの起動やメンテナンスタスクの実行を延期させる
   - Windows自動アップデートを延期する
   - ムービー用に電力設定を調整
5. 保存 をクリックして変更を保存し、ウィンドウを閉じます。

ムービープロファイルのリストにビデオプレイヤーを手動で追加する

特定の動画再生アプリを起動した際に、 Bitdefender が自動的に動画プロファイルに切り替わらない場合は、当該アプリを 動画アプリケーションリスト に手動で追加できます。

動画プロファイルのリストにビデオアプリを手動で追加するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. プロファイル タブを選択します。
3. 動画再生プロファイル エリアにある 設定 ボタンをクリックします。
4. 動画プロファイル設定 ウィンドウで プレイヤーリスト をクリックします。
5. 追加 をクリックします。

   新しいウィンドウが表示されます。 アプリケーションの実行ファイルを選択して、OKをクリックしてリストに追加します。

5.2.3. ゲームプロファイル

システム負荷を軽減し、速度低下を回避することで、快適なゲーム環境を実現します。 Bitdefender は、既知のゲームと挙動ヒューリスティック分析の組み合わせにより動作中のゲームを自動的に検出し、ゲームを快適にプレイできるようにシステムリソースを最適化します。

ゲームプロファイルを設定する

ゲームプロファイル時に実行するアクションを設定するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. プロファイル タブを選択します。
3. ゲームプロファイル エリアにある 設定 ボタンをクリックします。
4. 以下のオプションにチェックを入れて、適用したいシステム調整を選択します:
   - ゲームのパフォーマンスを向上させる
   - ゲームプロファイル用に製品設定を最適化
   - バックグラウンド・プログラムの起動やメンテナンスタスクの実行を延期させる
   - Windows自動アップデートを延期する
   - 電源の設定をゲーム用に調節する
5. 保存 をクリックして変更を保存し、ウィンドウを閉じます。

ゲームを手動でゲームリストに追加する

特定のゲームまたは仕事用アプリを起動した際に、 Bitdefender が自動的にゲームプロファイルに切り替わらない場合は、当該アプリを ゲームアプリケーションリスト に手動で追加できます。

ゲームプロファイルのゲームリストに手動でゲームアプリを追加するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. プロファイル タブを選択します。
3. ゲームプロファイル エリアにある 設定 ボタンをクリックします。
4. ゲームプロファイル設定 ウィンドウで ゲームリスト をクリックします。
5. 追加 をクリックします。

   新しいウィンドウが表示されます。 ゲームの実行可能ファイルを参照して選択し、OK をクリックしてリストに追加します。

5.2.4. 公共Wi-Fiのプロファイル

安全でないワイヤレスネットワークに接続した状態でメールを送信したり、重要な認証情報を入力したり、オンラインショッピングを行ったりすると、個人データを第三者に傍受される危険があります。 公共 Wi-Fi プロファイルは、保護された環境でオンラインでの支払いや重要なデータの送受信を行えるように製品の設定を変更します。

公共 Wi-Fi プロファイルを設定する

Bitdefender が安全でないワイヤレスネットワークへの接続時に自動的に設定を適用するように設定するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. プロファイル タブを選択します。
3. 公共 Wi-Fi プロファイル エリアにある 設定 ボタンをクリックします。
4. 安全でない Wi-Fi ネットワークへの接続時に製品設定を自動的に調整して保護を強化する のチェックボックスはオンのままにしておきます。
5. 保存 をクリックします。

5.2.5. バッテリーモード・プロファイル

バッテリモード プロファイルは、ノートパソコンやタブレット用に設計されているモードです。 この機能は、バッテリーの残り容量がデフォルトまたは選択したレベルよりも低くなった際に、システムおよび Bitdefender による電力消費を最小化します。

バッテリモード プロファイルを設定する

バッテリモード プロファイルを設定するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. プロファイル タブを選択します。
3. バッテリモード プロファイル エリアにある 設定 ボタンをクリックします。
4. 以下のオプションにチェックを入れて、適用するシステム調整を選択します:

- バッテリモード用に製品設定を最適化.
- バックグラウンド・プログラムの起動やメンテナンスタスクの実行を延期する.
- Windows自動アップデートを延期する.
- バッテリモードの電力設定を調整する.
- 外部デバイスやネットワークポートを無効化.

5. 保存 をクリックして変更を保存し、ウィンドウを閉じます。

スピンボックスに有効な値を入力するか、上下いずれかの矢印キーを使って、バッテリモード時におけるシステム動作開始時を指定します。 デフォルトでは、このモードはバッテリー残量が 30% を下回ると有効になります。

Bitdefender のバッテリモード プロファイル動作時には、以下の設定が適用されます:

- Bitdefender の自動アップデートを延期します。
- スケジュール設定されているスキャンを延長します。
- セキュリティ ウィジェット をオフにします。

Bitdefender は、ノートパソコンがバッテリーに切り替わったことを検出し、バッテリーの残量に応じて自動的にバッテリモードに移行します。 同様に、Bitdefender はノートパソコンが電源に接続されたことを検知すると、バッテリモードを自動的に終了します。

5.2.6. リアルタイム最適化

Bitdefender リアルタイム最適化は、プロファイルモード時にシステムパフォーマンスをバックグラウンドでサイレントに向上し、快適なユーザーエクスペリエンスを実現するプラグインです。 このプラグインは CPU 負荷に応じてすべてのプロセスを監視し、負荷の高い処理を必要に応じて調節します。

リアルタイム最適化をオン/オフにするには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. プロファイル タブを選択します。
3. リアルタイム最適化オプションが表示されるまで下にスクロールし、対応するスイッチを使用してオンまたはオフにします。

6. トラブルシューティング

6.1. 一般的な問題を解決する

この章では Bitdefender 使用時に遭遇する問題と、その解決策が記載されています。 これらの問題のほとんどは、製品を適切に構成することで解決できます。

- 「パソコンの動作が遅い」 (p. 182)
- 「検査が開始しない。」 (p. 184)
- 「アプリを使用できなくなった」 (p. 186)
- 「Bitdefender が安全なウェブサイトやオンラインアプリケーションをブロックした場合」 (p. 187)
- 「Bitdefender が安全なアプリケーションをランサムウェアとして誤認識した場合の対処方法」 (p. 188)
- 「インターネット回線速度が遅い環境でBitdefenderをアップデートする方法」 (p. 192)
- 「Bitdefenderサービスが応答していません」 (p. 192)
- 「迷惑メール対策フィルタが正しく動作しない」 (p. 193)
- 「「パスワード管理」の自動入力機能が正しく動作しません。」 (p. 198)
- 「Bitdefender の削除に失敗」 (p. 199)
- 「Bitdefenderをインストール後にパソコンが起動しなくなった」 (p. 200)

ここに該当する問題が記載されていない場合、または、記載されているが問題が解決しない場合は、次の章に表記されている Bitdefender 技術サポート部までお問い合わせください。「サポートを依頼」 (p. 317)

6.1.1. パソコンの動作が遅い

一般的に、セキュリティソフトをインストールした後は、コンピュータの動作が少し遅くなる可能性があります。

パソコンの速度が著しく低下している場合は、以下の原因が考えられます：

- コンピュータ上にBitdefender以外のセキュリティ製品がインストールされている。

Bitdefender は、インストール中に他のセキュリティ製品を検出しますが、 Bitdefender のインストール前に使われていた製品がある場合は、確認の上アンインストールすることをおすすめいたします。 詳細については、「他のセキュリティソフトはどうやって削除するのですか？」 (p. 77)をご参照ください。

- Bitdefenderの使用に必要な、最低動作環境を満たしていないパソコンにインストールした。

  お使いのパソコンが必須動作環境を満たしておらず、複数のアプリケーションを同時に起動している場合は、パソコンの動作が遅くなります。 動作環境についてはパッケージや製品ページをご覧ください。 詳細については、「最低動作条件」 (p. 3)をご参照ください。

- 使用しないアプリがインストールされている場合。

  どのパソコンにも、使用しない不要なプログラムやアプリがインストールされています。 多くの不要プログラムは、知らないうちにバックグラウンドで実行されていたり、メモリを消費し、貴重なディスク容量を使用します。 このように使用しない不要プログラムはアンインストールすることをおすすめします。 こちらはパソコン購入時からプリインストールされていたアプリケーションや、アンインストールし忘れた無料版製品にも有効です。

  ! 重要項目
  プログラムまたはアプリケーションがオペレーティングシステムにとって重要なプログラムだと思われる場合は、アンインストールせずにBitdefenderカスタマーサポートまでお問い合わせください。

- お使いのパソコンはウイルスに感染している可能性があります。

  パソコンのパフォーマンスや通常動作も脅威に影響される可能性があります。 スパイウェア、マルウェア、トロイの木馬やアドウェアはすべてパソコンのパフォーマンスに影響します。 パソコンは定期的に（1週間に一度）ウイルス検査を行うことをおすすめします。 Bitdefenderのシステムスキャンは、システムのセキュリティに影響するあらゆる脅威を検出するため、システムスキャンを実行することをおすすめします。

  システム スキャンを開始:

  1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
  2. アンチウイルスウィンドウで、 システムスキャンをクリックします。

3. ウィザードの手順に随ってください。

6.1.2. 検査が開始しない。

この問題については、主に2つの原因が考えられます：

- 以前のバージョンの Bitdefender が完全に削除されていないか、Bitdefender のインストールが失敗しています。

  この場合、 Bitdefender を再インストールしてください:

  - Windows 7の場合：

    1. スタート ボタンをクリックし、コントロール パネル を開きます。その中にある プログラムおよび機能 をダブルクリックします。
    2. Bitdefender Total Securityを探していただき、削除を選択してください。
    3. 表示されるウィンドウで 再インストール をクリックします。
    4. 再インストール処理が完了するまで待ち、それからシステムを再起動します。

  - Windows 8 および Windows 8.1:

    1. Windowsスタート画面からコントロールパネルを探して（またはスタート画面で「コントロールパネル」と入力して）、アイコンをクリックしてください。
    2. プログラムのアンインストールまたはプログラムと機能をクリックしてください。
    3. Bitdefender Total Securityを探していただき、削除を選択してください。
    4. 表示されるウィンドウで 再インストール をクリックします。
    5. 再インストール処理が完了するまで待ち、それからシステムを再起動します。

  - Windows 10の場合：

    1. 開始 をクリックし、続いて「設定」をクリックします。
    2. 設定エリアの システム アイコンをクリックし、インストールされているアプリケーション を選択します。
    3. Bitdefender Total Securityを探していただき、削除を選択してください。

4. アンインストール をもう一度クリックして選択を確定します。
5. 表示されるウィンドウで 再インストール をクリックします。
6. 再インストール処理が完了するまで待ち、それからシステムを再起動します。

注記
この再インストール手順に従うことで、ユーザー設定が保存され、新たにインストールされた製品で同じ設定が利用可能になります。 その他の設定は、デフォルトの設定に戻すことができます。

- このコンピュータ上に、 Bitdefender 以外のセキュリティ製品がインストールされています。

  この場合の対処方法:

  1. 別のセキュリティ製品を削除してください。 詳細については、「他のセキュリティソフトはどうやって削除するのですか？」 (p. 77)をご参照ください。
  2. Bitdefender を再インストールします:
     - Windows 7の場合 :
       a. スタート ボタンをクリックし、コントロール パネル を開きます。その中にある プログラムおよび機能 をダブルクリックします。
       b. Bitdefender Total Securityを探していただき、削除を選択してください。
       c. 表示されるウィンドウで 再インストール をクリックします。
       d. 再インストール処理が完了するまで待ち、それからシステムを再起動します。
     - Windows 8 および Windows 8.1:
       a. Windowsスタート画面からコントロールパネルを探して（またはスタート画面で「コントロールパネル」と入力して）、アイコンをクリックしてください。
       b. プログラムのアンインストールまたはプログラムと機能をクリックしてください。
       c. Bitdefender Total Securityを探していただき、削除を選択してください。

d. 表示されるウィンドウで 再インストール をクリックします。

e. 再インストール処理が完了するまで待ち、それからシステムを再起動します。

- Windows 10の場合：

a. 開始 をクリックし、続いて「設定」をクリックします。

b. 設定エリアの システム アイコンをクリックし、インストールされているアプリケーション を選択します。

c. Bitdefender Total Securityを探していただき、削除を選択してください。

d. アンインストール をもう一度クリックして選択を確定します。

e. 表示されるウィンドウで 再インストール をクリックします。

f. 再インストール処理が完了するまで待ち、それからシステムを再起動します。

注記
この再インストール手順に従うことで、ユーザー設定が保存され、新たにインストールされた製品で同じ設定が利用可能になります。 その他の設定は、デフォルトの設定に戻すことができます。

解決しなかった場合は、「サポートを依頼」 (p. 317)項に記載されているBitdefenderサポートにお問い合わせください。

6.1.3. アプリを使用できなくなった

Bitdefender のインストール後に特定のアプリケーションが使用できなくなった場合、以下の状況が考えられます。

Bitdefenderをインストールした後、以下のような状況が発生する可能性があります：

- プロクラムがシステムへの変更を行おうとした場合に、Bitdefender がアラートを表示します。拒否を選択するとそのアプリケーションは利用できなくなる場合があります。
- 使用しようとしているアプリケーションからエラーメッセージが出るようになった。

このような状況は、高度な脅威防御は一部のアプリケーションをマルウェアとして誤検出したときに生じます。

高度な脅威防御は、システムで実行中のアプリケーションを常に監視し、不審な挙動を漏らさずレポートする Bitdefender のモジュールです。 この機能はヒューリスティックなシステムに基づいているため、通常のアプリケーションが脅威として誤認識されることがあります。

この状況が発生した際には、該当するアプリを高度な脅威防御によるモニタリング対象から除外できます。

例外リストにプログラムを追加するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. 高度な脅威防御 パネルで 設定 をクリックします。
3. 例外設定 ウィンドウで アプリケーションを例外に追加 をクリックします。
4. 除外したいアプリを選択し、OKをクリックします。

解決しなかった場合は、「サポートを依頼」 (p. 317)項に記載されているBitdefenderサポートにお問い合わせください。

6.1.4. Bitdefender が安全なウェブサイトやオンラインアプリケーションをブロックした場合

Bitdefender は、すべてのウェブトラフィックをフィルタし、悪意のあるコンテンツをブロックして安全にウェブ閲覧ができる環境を提供します。ただし条件・状況によっては、 Bitdefender が安全なウェブサイトやオンラインアプリケーションを危険と判断し、 Bitdefender の HTTP トラフィックスキャンによってブロックしてしまう場合があります。

同じページまたはアプリが繰り返しブロックされる場合は、例外に追加して Bitdefender のエンジンのスキャン対象から除外することで、より快適なウェブ閲覧が可能になります。

例外設定 にウェブサイトを追加するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. オンライン脅威対策 パネルで 例外設定 をクリックします。
3. ブロックするウェブサイトまたはオンラインアプリのアドレスを入力し、追加 をクリックします。
4. 保存 をクリックして変更を保存し、ウィンドウを閉じます。

このリストには、完全に信頼できるウェブサイトおよびアプリケーションのみ追加してください。 これらは、オンライン脅威、フィッシング詐欺、および詐欺サイト用エンジンのスキャンからは除外されます。

解決しなかった場合は、「サポートを依頼」 (p. 317)項に記載されているBitdefenderサポートにお問い合わせください。

6.1.5. Bitdefender が安全なアプリケーションをランサムウェアとして誤認識した場合の対処方法

ランサムウェアは、ユーザーのシステムに勝手にロックをかけて人質にとり、ユーザーに身代金として金銭を要求する悪質なプログラムです。 大切な個人データが盗み出されたり、ランサムウェアの被害にあうことがないよう、 Bitdefender はデータ保護機能を搭載しています。

保護されたファイルを変更または削除しようとするアプリケーションは、安全でないと判断され、 Bitdefender によってブロックされます。

そのようなアプリが、信頼されていないアプリのリストに追加されてしまったが、間違いなく安全だと判断できる場合は以下のステップを実行します:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. 安全なファイル パネルで アプリケーションアクセス をクリックします。
3. 保護フォルダ内のファイルを変更しようとしたアプリケーションがここに表示されます。 間違いなく安全であるアプリの横の 許可 スイッチをクリックします。

6.1.6. インターネットに接続できません。

Bitdefenderをインストール後に特定のプログラムやウェブブラウザからインターネットへアクセスできなかったり、ネットワークサービスを利用できなくなる場合があります。

この場合、最も良い解決策は、自動的にそれぞれのアプリケーション間で接続を許可するよう Bitdefender を設定することです。

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. ファイアウォール パネルで 設定 をクリックします。
3. ルール ウィンドウで ルールを追加 をクリックします。

4. 詳細を追加するための新しいウィンドウが表示されます。 パーミッション のセクションで利用可能なすべてのネットワークタイプを選択し、許可 を選択してください。

Bitdefender を閉じ、ソフトウェアを開いてから再度インターネットへの接続をお試しください。

解決しなかった場合は、「サポートを依頼」 (p. 317)項に記載されているBitdefenderサポートにお問い合わせください。

6.1.7. ネットワーク上のデバイスにアクセスできない。

接続先のネットワークによっては、Bitdefender ファイアウォールはネットワーク プリンタへの接続をブロックする可能性があります。 結果として、ファイルを共有したり印刷できなくなる可能性があります。

この場合、最適な解決策は、 Bitdefender を次のように設定して、当該デバイスとの通信を自動的にを許可する方法です:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. ファイアウォール パネルで 設定 をクリックします。
3. ルール ウィンドウで ルールを追加 をクリックします。
4. 設定 ウィンドウで、このルールをすべてのアプリケーションへ適用 オプションをオンにします。
5. 詳細設定 タブをクリックします。
6. カスタムリモートアドレスボックスに、アクセスを一切制限しないコンピュータまたはプリンタの IP アドレスを入力します。

それでもデバイスへ接続できない場合は、原因はBitdefenderではない可能性があります。

次のような、製品以外の原因がないかご確認ください :

- 他のコンピュータ上のファイアウォールが、このコンピュータと共有しているファイルとプリンタをブロックします。
  - Windowsファイアウォールを使用している場合は、以下の手順でファイルおよびプリンタ共有を許可することができます :
    - Windows 7の場合 :
      1. スタートをクリックしてコントロールパネルを開き、システムとセキュリティを選択してください。

2. Windows ファイアウォール にアクセスし、Windows ファイアウォールを介したアプリまたは機能を許可 をクリックします。
3. ファイルとプリンターの共有チェックボックスにチェックを入れてください。

- Windows 8 および Windows 8.1:
  1. Windowsスタート画面からコントロールパネルを探して（またはスタート画面で「コントロールパネル」と入力して）、アイコンをクリックしてください。
  2. システムとセキュリティをクリックし、Windows ファイアウォールを選択して、Windows ファイアウォールによるアプリケーションの許可を選択してください。
  3. ファイルとプリンタの共有 チェックボックスをオンにし、OK をクリックします。
- Windows 10の場合：
  1. タスクバーの検索ボックスに「Windows ファイアウォールによるプログラムの許可」と入力し、アイコンをクリックします。
  2. 設定の変更 をクリックします。
  3. 許可されているアプリと機能 リストで、ファイルとプリンタの共有 チェックボックスを選択し、 OK をクリックします。
- 別のファイアウォール プログラムを使用している場合は、その説明書あるいはヘルプ ファイルをご参照ください。

- 共有プリンタの使用、または、接続を妨げる可能性がある一般的な条件：
  - Windows の管理者権限が必要な場合。
  - 特定のパソコンやユーザーのみがアクセス許可されている場合。 共有を行なっている場合は、他のユーザー（パソコン）に対してのアクセス許可を確認します。 接続を試みている場合は、プリンタに接続するアクセス許可があるかどうかを、共有を行なっている別のパソコンのユーザーに確認してください。
  - プリンタの共有が設定されていない場合。
  - 共有プリンタがコンピュータに追加されていない場合。

注記
共有プリンタの管理方法（プリンタの共有、プリンタの設定・削除、ネットワーク プリンタ・共有プリンタへ接続)は、Windows ヘルプ及びサポート センター（スタートメニューの ヘルプ&サポート をクリック）に進んでください。

- ネットワークプリンタへのアクセスは、特定のパソコンまたはユーザーにのみ制限することができます。 プリンタへ接続する権限が与えられているか、ネットワーク管理者にご確認ください。

解決しなかった場合は、「サポートを依頼」（p. 317)項に記載されているBitdefenderサポートにお問い合わせください。

6.1.8. インターネットの速度が遅い

この状況は、Bitdefender のインストール後に発生する可能性があります。問題は、Bitdefender ファイアウォール設定内のエラーによって引き起こされます。

この問題を解決するには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. ファイアウォール パネルでスイッチをオフにして機能を無効にします。
3. Bitdefender ファイアウォール機能を無効にした状態で、インターネットの回線速度が改善されるかお確かめください。
   - それでもインターネット速度に遅延がある場合は、原因はBitdefenderではない可能性があります。 ご利用されているプロバイダへご連絡いただき、接続に障害などが発生していないかご確認ください。

     インターネット サービス プロバイダ（ISP）から、接続の問題は彼らの操作によるものであり、まだ解決していないといった内容のメールを受信した場合は、記述の通り Bitdefender に連絡をしてください。「サポートを依頼」（p. 317）
   - Bitdefenderファイアウォールを無効にすることでインターネット接続が改善した場合:
     a. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
     b. ファイアウォール パネルで 設定 をクリックします。

c. ネットワークアダプタタブに移動し、自宅/オフィスでお使いのインターネット接続を設定します。

d. 設定 タブで ポートスキャン保護 をクリックします。

ステルスモードエリアでステルス設定を変更をクリックします。 接続しているネットワークアダプタに対してステルスモードをオンにします。

e. Bitdefender を閉じ、パソコンを再起動後にインターネットの回線速度をご確認ください。

解決しなかった場合は、「サポートを依頼」 (p. 317)項に記載されているBitdefenderサポートにお問い合わせください。

6.1.9. インターネット回線速度が遅い環境でBitdefenderをアップデートする方法

インターネット回線の速度が（ダイヤルアップのように）遅いと、アップデートを行っている間にエラーが発生する可能性があります。

システムの Bitdefender 脅威情報データベースを最新の状態に保つには:

1. Bitdefender インターフェイスのナビゲーションメニューにある 設定 をクリックします。
2. ▪ 更新 タブを選択します。 ▪
3. サイレントアップデート オプションをオフにします。
4. 次にアップデートが利用できるようになった際に、ダウンロードしたいアップデートを選択することを求められるようになります。 定義ファイルのアップデート のみを選択します。
5. Bitdefender は脅威情報データベースの更新分のみをダウンロードし、インストールします。

6.1.10. Bitdefenderサービスが応答していません

この項目では、「Bitdefenderサービスの応答がありません」というエラーに関する解決策を記載しています。 次の内容のエラーが発生するかもしれません：

- タスクトレイ内に表示される Bitdefender アイコンがグレーに表示されている場合、 Bitdefender サービスが応答していないこと表しています。

- Bitdefender 画面に、 Bitdefender サービスが応答していないことを示す表記が出ている。

エラーの原因は以下の状態が考えられます：

- 一時的にBitdefenderサービスへの通信エラーが発生した。
- いくつかのBitdefenderサービスが停止した。
- コンピュータ上で別のセキュリティ対策製品が Bitdefender と同時に実行されている。

このエラーを解決するには、次の対策を行ってください。

1. 一時的なエラーのため、 変更が反映されるまで、しばらくお待ちください。
2. パソコンを再起動し、Bitdefenderが起動するまでお待ちください。 Bitdefenderを開き、状況が改善されたかご確認ください。 コンピュータを再起動することで、通常、問題は解決します。
3. Bitdefender以外に、別のセキュリティ製品がインストールされていないかご確認ください。 他のセキュリティ製品がインストールされていた場合は、その製品を完全にアンインストールした後、再度 Bitdefender をインストールしなおしてください。

   詳細については、「他のセキュリティソフトはどうやって削除するのですか？」 (p. 77)をご参照ください。

エラーが改善されない場合は、「サポートを依頼」 (p. 317)に記載してある通り、サポートまでお問い合わせください。

6.1.11. 迷惑メール対策フィルタが正しく動作しない

この項目は、以下の Bitdefender 迷惑メール対策フィルタの操作に関する問題の解決策を提供しています：

- 問題がない電子メールが次のように区別されました[spam].
- 迷惑メール対策フィルタが、多くの迷惑メール（SPAM）を検出していません。
- 迷惑メール対策フィルタは、迷惑メール（SPAM）を検出しませんでした。

正常なメールが［spam］として区別される

問題がないメッセージが[spam]として区別されました。これは、Bitdefenderの迷惑メール対策フィルタが認識する迷惑メールと類似しているためです。

迷惑メール対策フィルタを正しく設定すると、通常、この問題は解決します。

Bitdefender は電子メール メッセージの宛先を、自動的に友人リストに追加します。 友人リストの連絡先から届くメールは正常のメールと判断されます。 迷惑メール対策フィルタによってチェックされないため、[spam]として迷惑メール扱いされることはありません。

友人リストの設定は、次のような場合に使用し、対象の電子メール　メッセージのアドレスを友人リストに追加することで、解決します。

- 様々なウェブサイトに登録をしているため、多くの勧誘メールを受信してしまう場合。 このような場合は、対象の電子メール メッセージのアドレスを友人リストに追加することで、解決します。
- 問題がない電子メールで、例えば顧客やビジネスパートナー等、電子メールを送信したことがない相手から受信したメールが迷惑メールとして扱われる場合。 この場合他の解決策が必要です。

  Bitdefenderが対応するメールクライアントを使用している場合、誤検出されたメールを移動するをご参照ください。

> **注記**
> Bitdefender は、迷惑メール対策ツールバーを介して、最も共通して使用されるメール クライアントを統合します。 サポートされた全てのメール クライアントの一覧は、「対応メールクライアントとプロトコル」 (p. 106)をご参照ください。

連絡先を友人リストに追加

サポートされたメール　クライアントを使用している場合は、問題がないメッセージの送信者を、簡単に友人リストに追加することができます。 次の手順に従ってください：

1. メール クライアントで、友人リストに追加する送信者からの電子メール メッセージを選択します。
2. Bitdefender 迷惑メール対策ツールバーの 友人を追加 ボタンをクリックします。
3. 友人リストに追加するアドレスについての確認を受けることがあります。 今後このメッセージを表示しません を選択し、OK をクリックします。

このアドレスから届くメール メッセージは、その内容に関わらず、常に受信されます。

別のメール クライアントを使用している場合、連絡先を Bitdefender 管理画面から友人リストに追加することができます。 次の手順に従ってください：

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. 迷惑メール対策 ウィンドウで、友達の管理 をクリックします。

   設定画面が表示されます。
3. 常にメールを受け取りたいメールアドレスを入力し、追加をクリックします。 メールアドレスは制限なく追加することができます。
4. OK をクリックすると、変更が保存され、画面が自動で閉じます。

誤検出されたメールを移動する

対応メールクライアントを使用している場合は、（間違えて[spam]としてマーキングされたメールを選択することで）簡単に迷惑メールフィルタの修正を行うことができます。 これをすることで迷惑メールフィルタの精度を上げることもできます。 次の手順に従ってください：

1. メール クライアントを開きます。
2. SPAM（迷惑）メールが移動された、フォルダを開きます。
3. Bitdefenderが [spam] と誤って区別した、正常なメッセージを選択します。
4. Bitdefender 迷惑メール対策ツールバーの 友人の追加 ボタンをクリックし、送信者を友人リストに追加します。 承認のため、OK のクリックを求められ場合があります。 このアドレスから届くメール メッセージは、その内容に関わらず、常に受信されます。
5. Bitdefender 迷惑メール対策ツールバー（お使いのメールクライアントの上部に表示）の 通常メール ボタンをクリックしてください。 メールは受信トレイへ移動されます。

多くの迷惑メール（SPAM）が検出されていない

[spam] として区別されていない多くの迷惑メールを受信している場合は、効率を良くするため、Bitdefender 迷惑メール対策フィルタを設定する必要があります。

以下の解決策をお試しください：

1. Bitdefenderが対応するメールクライアントを使用している場合、検知されなかった迷惑メールを移動するをご参照ください。

   注記

   Bitdefender は、迷惑メール対策ツールバーを介して、最も共通して使用されるメール クライアントを統合します。 サポートされた全てのメール クライアントの一覧は、「対応メールクライアントとプロトコル」 (p. 106)をご参照ください。

2. 迷惑メール送信者をスパマー リストに追加する。 スパマー リストのアドレスから受信した電子メールは、自動的に [spam] として区別されます。

検出されていない迷惑メールを表示

対応メールクライアントを使用している場合は、迷惑メールとして対処させるメールを簡単に設定することができます。 これをすることで迷惑メールフィルタの精度を上げることもできます。 次の手順に従ってください：

1. メール クライアントを開きます。
2. 受信トレイを開きます。
3. 検出されていない迷惑メール メッセージを選択します。
4. Bitdefender迷惑メールツールバーにある 迷惑メール ボタンを選択します（ツールバーはメールクライアントの上部に表示されます）。[spam]としてマーキングされ、直ちに迷惑メールフォルダへ移動されます。

迷惑メール送信者をスパマー リストに追加

本製品のプラグインが対応したメール クライアントを使用している場合は、迷惑メール メッセージの送信者を簡単にスパマー リストに追加することができます。 次の手順に従ってください：

1. メール クライアントを開きます。
2. SPAM（迷惑）メールが移動された、フォルダを開きます。
3. Bitdefenderが[spam]として判定したメッセージを選択します。
4. Bitdefender 迷惑メール対策ツールバーの スパマー の追加 ボタンをクリックします。

5. スパマー　リストに追加するアドレスの確認を受けることもあります。 今後このメッセージを表示しません を選択し、OK をクリックします。

別のメール クライアントを使用している場合は、 Bitdefenderの管理画面から手動でスパマーをリストに追加することができます。 これは同じメールアドレスから複数の迷惑メールを受けている場合に行うことをおすすめします。 次の手順に従ってください：

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. 迷惑メール対策 ウィンドウで、スパマーの管理 をクリックします。

   設定画面が表示されます。
3. スパムメールの送信元メールアドレスを入力し、追加をクリックします。 メールアドレスは制限なく追加することができます。
4. OK をクリックすると、変更が保存され、画面が自動で閉じます。

迷惑メール対策フィルタが迷惑メール（SPAM）を全く検出しない

迷惑メール メッセージが、[spam] として区別されない場合は、Bitdefender 迷惑メール対策フィルタに問題がある可能性があります。 この問題を解決する前に、次の状態のどれかが原因でないかをご確認ください：

- 迷惑メール対策機能が無効になっている可能性があります。 迷惑メール対策による保護の状態を確認するには、Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。 迷惑メール対策 パネルで、この機能が有効になっているかを確認します。

  迷惑メール対策が無効になっている場合は、これが原因の可能性があります。　該当のスイッチをクリックして、迷惑メール対策をオン/オフにします。
- Bitdefender 迷惑メール対策機能は、POP3 プロトコル経由の電子メール メッセージに対してのみ有効です。 これは以下を意味しています：
  - ウェブ メールから受信したメッセージ（Yahoo!、Gmail、Hotmail 等）に対して、 Bitdefender はスパムのフィルタを行いません。
  - 電子メール クライアントで、POP3 以外のプロトコル（例 IMAP4）で電子メールの受信を設定している場合、 Bitdefender 迷惑メール対策フィルタは、スパムに対するチェックを行いません。

注記

POP3 とは、メール サーバから電子メール メッセージをダウンロードするために最も使用されているプロトコルの 1 つです。 電子メール メッセージをダウンロードするメール クライアントのプロトコルが分からない場合は、電子メールの設定者にご確認ください。

- Bitdefender Total Securityは、Lotus Notes POP3通信をスキャンしません。

製品を再インストールするか、修復インストールすることで改善する可能性があります。 ただし、その前に「サポートを依頼」 (p. 317)で説明されている通り、Bitdefenderへお問い合わせすることをおすすめします。

6.1.12. 「パスワード管理」の自動入力機能が正しく動作しません。

オンライン認証情報は Bitdefender パスワードマネージャーに保存されましたので、自動入力は機能しなくなります。 こちらの現象が発生するときは、多くの場合Bitdefenderパスワード管理の拡張機能がお使いのブラウザに正しくインストールされていないことが原因です。

この問題を修正するには、以下の手順に従ってください：

- Internet Explorerの場合：
  1. Internet Explorer を開きます。
  2. ツールをクリックしてください。
  3. 「アドオンの管理」をクリックしてください。
  4. 「ツールバーと拡張機能」をクリックしてください。
  5. Bitdefender ウォレット にアクセスし、有効化 をクリックします。
- Mozilla Firefoxの場合：
  1. Mozilla Firefoxを開いてください。
  2. ツールをクリックしてください。
  3. 「アドオン」をクリックしてください。
  4. 「拡張機能」をクリックしてください。
  5. Bitdefender ウォレット にアクセスし、有効化 をクリックします。
- Google Chromeの場合：

1. Google Chromeを開いてください。
2. メニューアイコンを選択してください。
3. 「その他ツール」をクリックします。
4. 「拡張機能」をクリックしてください。
5. Bitdefender ウォレット にアクセスし、有効化 をクリックします。

注記
ブラウザを再起動するとアドオンが有効な状態になります。

オンラインアカウントで「パスワード管理」の自動入力機能が正しく動作するかご確認ください。

解決しなかった場合は、「サポートを依頼」 (p. 317)項に記載されているBitdefenderサポートにお問い合わせください。

6.1.13. Bitdefender の削除に失敗

Bitdefenderを削除中に処理が止まってしまった場合は、キャンセルをクリックして操作を中断してください。 改善しない場合は、パソコンを再起動してください。

削除が不完全に終了すると、Bitdefenderのレジストリキーやファイルが残骸としてシステムに残る場合があります。 このような残骸が残ってしまうと、Bitdefenderの新規インストールに影響を及ぼす可能性があります。パソコンのパフォーマンスや、システムの安定性にも影響を及ぼす場合があります。

Bitdefender をシステムから完全に削除するには:

- Windows 7の場合 :
  1. スタート ボタンをクリックし、コントロール パネル を開きます。その中にある プログラムおよび機能 をダブルクリックします。
  2. Bitdefender Total Securityを探していただき、削除を選択してください。
  3. 表示されるウィンドウで 削除 をクリックします。
  4. アンインストール処理が完了するまで待ち、それからシステムを再起動します。
- Windows 8 および Windows 8.1:

1. Windowsスタート画面からコントロールパネルを探して（またはスタート画面で「コントロールパネル」と入力して）、アイコンをクリックしてください。
2. プログラムのアンインストールまたはプログラムと機能をクリックしてください。
3. Bitdefender Total Securityを探していただき、削除を選択してください。
4. 表示されるウィンドウで 削除 をクリックします。
5. アンインストール処理が完了するまで待ち、それからシステムを再起動します。

- Windows 10の場合：

1. 開始 をクリックし、続いて「設定」をクリックします。
2. 設定エリアの システム アイコンをクリックし、インストールされているアプリケーション を選択します。
3. Bitdefender Total Securityを探していただき、削除を選択してください。
4. アンインストール をもう一度クリックして選択を確定します。
5. 表示されるウィンドウで 削除 をクリックします。
6. アンインストール処理が完了するまで待ち、それからシステムを再起動します。

6.1.14. Bitdefenderをインストール後にパソコンが起動しなくなった

Bitdefender をインストールした直後に、パソコンを通常モードで起動できなくなってしまった場合は、様々な原因が考えられます。

この問題の原因は、以前インストールした Bitdefender が正しく削除されなかったか、他のセキュリティソフトウェアがまだパソコンにインストールされていることが考えられます。

各状況の対処方法は下記のとおりです：

- 以前使用していたBitdefenderが正しく削除されていません。

  解決するには:

1. コンピュータを再起動し、セーフ モードで起動します。 これを行う方法については、「セーフモードでパソコンを再起動させる方法は？」(p. 78) を参照してください。
2. パソコンからBitdefenderを削除する：
   - Windows 7の場合：
     a. スタート ボタンをクリックし、コントロール パネル を開きます。その中にある プログラムおよび機能 をダブルクリックします。
     b. Bitdefender Total Securityを探していただき、削除を選択してください。
     c. 表示されるウィンドウで 削除 をクリックします。
     d. アンインストール処理が完了するまで待ち、それからシステムを再起動します。
     e. パソコンを通常モードで再起動してください。
   - Windows 8 および Windows 8.1:
     a. Windowsスタート画面からコントロールパネルを探して（またはスタート画面で「コントロールパネル」と入力して）、アイコンをクリックしてください。
     b. プログラムのアンインストールまたはプログラムと機能をクリックしてください。
     c. Bitdefender Total Securityを探していただき、削除を選択してください。
     d. 表示されるウィンドウで 削除 をクリックします。
     e. アンインストール処理が完了するまで待ち、それからシステムを再起動します。
     f. パソコンを通常モードで再起動してください。
   - Windows 10の場合：
     a. 開始 をクリックし、続いて「設定」をクリックします。
     b. 設定エリアの システム アイコンをクリックし、インストールされているアプリケーション を選択します。
     c. Bitdefender Total Securityを探していただき、削除を選択してください。

d. アンインストール をもう一度クリックして選択を確定します。

e. 表示されるウィンドウで 削除 をクリックします。

f. アンインストール処理が完了するまで待ち、それからシステムを再起動します。

g. パソコンを通常モードで再起動してください。

3. Bitdefenderを再インストールしてください。

- 以前インストールされていた、別のセキュリティ対策ソフトが正しく削除されていません。

  解決するには:

  1. コンピュータを再起動し、セーフ モードで起動します。 これを行う方法については、「セーフモードでパソコンを再起動させる方法は？」（p. 78）を参照してください。
  2. 他のセキュリティシステムをお使いのシステムから削除:
     - Windows 7の場合 :
       a. スタート ボタンをクリックし、コントロール パネル を開きます。その中にある プログラムおよび機能 をダブルクリックします。
       b. 削除するプログラム名を探し、削除 を選択してください。
       c. アンインストール処理が完了するまで待ち、それからシステムを再起動します。
     - Windows 8 および Windows 8.1:
       a. Windowsスタート画面からコントロールパネルを探して（またはスタート画面で「コントロールパネル」と入力して）、アイコンをクリックしてください。
       b. プログラムのアンインストールまたはプログラムと機能をクリックしてください。
       c. 削除するプログラム名を探し、削除 を選択してください。
       d. アンインストール処理が完了するまで待ち、それからシステムを再起動します。
     - Windows 10の場合 :
       a. 開始 をクリックし、続いて「設定」をクリックします。

b. 設定エリアの システム アイコンをクリックし、インストールされているアプリケーション を選択します。

c. 削除するプログラム名を探し、アンインストール を選択してください。

d. アンインストール処理が完了するまで待ち、それからシステムを再起動します。

他社のセキュリティ製品を正しくアンインストールするには、開発元のサイトからその製品の削除ツールを入手するか、開発元のサポートに正しい削除方法についてお問い合わせください。

3. パソコンを通常モードで再起動し、Bitdefender を再インストールしてください。

上記の手順は既に実施したが、状況は改善されなかった。

解決するには:

1. コンピュータを再起動し、セーフ モードで起動します。 これを行う方法については、「セーフモードでパソコンを再起動させる方法は？」（p. 78）を参照してください。
2. Windowsのシステム復元を利用して、Bitdefenderをインストールする前の時点の復元ポイントまでパソコンを復元させてください。
3. パソコンを通常モードで再起動し、「サポートを依頼」（p. 317）に記載されているサポートまでお問い合わせください。

6.2. パソコンから脅威を駆除する

脅威は、多数の異なる方法でコンピュータに影響を及ぼしますが、Bitdefender は脅威攻撃の種類に合わせたアプローチを行います。 しかし、脅威は頻繁にふるまいを変えるため、その活動内容やふるまいをパターン化することは困難です。

そのため、 Bitdefender がコンピュータから自動的に脅威の感染を駆除できない場合があり、こうした場合はユーザーの判断が必要です。 具体的には以下の通りです。

- 「Bitdefender レスキューモード (Windows 10 のレスキュー環境)」（p. 204）
- 「Bitdefender がパソコン上に脅威を検知した場合、どうすればいいのでしょうか？」（p. 208）

- 「アーカイブ内の脅威を駆除するには？」（p. 209）
- 「メールのアーカイブ内にある脅威はどうやって駆除するのですか？」（p. 210）
- 「ファイルが危険だと思った場合はどうすればいいのですか？」（p. 211）
- 「検査ログにある「パスワード保護された項目」とは何ですか？」（p. 212）
- 「検査ログにある「スキップした項目」とは何ですか？」（p. 212）
- 「検査ログにある「多重圧縮項目」とは何ですか？」（p. 212）
- 「なぜ Bitdefender は自動的に感染ファイルを削除するのですか？」（p. 213）

ここに該当する問題が記載されていない場合、または、記載されているが問題が解決しない場合は、次の章に表記されている Bitdefender 技術サポート部までお問い合わせください。「サポートを依頼」（p. 317）

6.2.1. Bitdefender レスキューモード（Windows 10 のレスキュー環境）

レスキューモードは、すべての内蔵および外付けハードドライブのパーティションをスキャンしてウイルスやマルウェアを駆除することのできる Bitdefender の機能です。

Bitdefender Total Security に Windows 7、Windows 8、Windows 8.1 インストールされ、 Bitdefender レスキューイメージファイルのダウンロードが完了すると、Windows を起動できなくなった場合などにも、レスキューモードでシステムを起動できるようになります。

Windows 10では、 Bitdefender レスキュー環境が Windows RE と統合されています。つまり、このオペレーティングシステムではレスキューモードのイメージをダウンロードする必要はありませんが、起動時の問題がある場合は使用できません。 Windowsサービスがロードされる前にシステムをクリーニングするには、 Bitdefender Rescue CDを使用することをおすすめします。

Bitdefender レスキューCD は、脅威の感染が疑われる場合に、コンピュータをスキャンして駆除を行える無料配布ツールです。http://www.bitdefender.co.jp/home-users/ にある Bitdefender Support Center プラットフォームでは、作成および使用方法を詳しく解説した記事を参照できます。

Bitdefender レスキューイメージをダウンロードする

Windows 7、Windows 8、および Windows 8.1 でレスキューモードを使用するには、以下の手順に従ってイメージファイルをダウンロードする必要があります:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. アンチウイルスウィンドウで、 レスキューモードクリックします。
3. 表示される確認ウィンドウで はい をクリックしてコンピュータを再起動します。

   Bitdefender サーバーから Bitdefender レスキューモードのイメージファイルがダウンロードされるまでしばらく待ちます。 ダウンロード処理が終了すると、コンピュータが再起動します。

   オペレーティングシステムを選択するためのメニューが表示されます。このステップでは、システムをレスキューモードまたはノーマルモードのどちらで起動するかを選択できます。

注記
Windows 10 では、Windows RE との統合により、レスキューモードのイメージをダウンロードする必要がありません。

Windows 7、Windows 8、Windows 8.1 のレスキューモードでシステムを起動する

レスキューモードを使用するには、以下の二つの方法があります :

Bitdefender の管理画面から

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
2. アンチウイルスウィンドウで、 レスキューモードクリックします。
3. 表示される確認ウィンドウで はい をクリックしてコンピュータを再起動します。
4. コンピュータの再起動後、オペレーティングシステムの選択を促すメニューが表示されます。 Bitdefender のレスキューモード を選択すると、 Bitdefender 環境でシステムをブートして Windows パーティションのクリーンアップを行うことができます。

5. 選択を求められた場合は、Enterを押して、普段お使いの画面解像度に一番近いものを選択してください。 再度Enterを、押します。

   しばらくするとBitdefender レスキューモードが起動します。

パソコンを直接レスキューモードで起動

Windowsが起動しなくなった場合は、下記の手順でパソコンをBitdefenderレスキューモードから直接起動することができます。

- Windows 7の場合：
  1. 高度な起動オプション画面が表示されるまでF8キーを押します。
  2. 矢印キーで Bitdefender レスキューモードを選択し、 Enterを押します。

     Bitdefender レスキューモードはすぐに起動します。
- Windows 8 および Windows 8.1:
  1. 高度な起動オプション画面が表示されるまでShiftキーを押します。
  2. 別のオペレーティングシステムを使用する オプションを選択し、Bitdefender レスキューモードを選択します。

     Bitdefender レスキューモードはすぐに起動します。

注記

「Bitdefender レスキューイメージをダウンロードする」 (p. 205)で説明されているように、レスキューモードでコンピュータを起動するには、レスキューイメージファイルがダウンロード済みである必要があります。

Windows 10 のレスキューモードでシステムを起動する

レスキュー環境には、 Bitdefender 製品からのみ以下の手順で入ることができます:

1. Bitdefender インターフェイスのナビゲーションメニューにある 保護をクリックします。
2. アンチウイルスウィンドウで、 レスキュー環境をクリックします。
3. 表示されるウィンドウで 再起動 をクリックします。

   しばらくすると Bitdefender のレスキュー環境がロードされます。

レスキューモードでシステムをスキャンする（Windows 10 のレスキュー環境）

レスキューモードでシステムをスキャンするには（レスキュー環境）:

- Windows 7、Windows 8、および Windows 8.1:

  1. 「Windows 7、Windows 8、Windows 8.1 のレスキューモードでシステムを起動する」 (p. 205)で説明されている手順で、パソコンをレスキューモードで起動します。
  2. Bitdefenderロゴが表示され、セキュリティソリューションエンジンのコピーが開始されます。
  3. ようこそ画面が表示されます。 続けるをクリックします。
  4. 脅威情報データベースのアップデートが開始されました。
  5. アップデートが完了すると、Bitdefender のオンデマンド アンチウイルススキャナのウィンドウが表示されます。
  6. 今すぐスキャン をクリックし、表示されるウィンドウでスキャン対象を選択して 開く をクリックするとスキャンが開始します。

     Windowsの全パーティションを検査することをおすすめします。

     注記
     レスキューモードでパソコンを起動した場合、パーティション名はLinuxタイプで表示されます。 ディスクパーティションは、Windowsのパーティション(C:) に対してsda1、(D:)に対して sda2 というように表示されます。

  7. 検査が完了するまでしばらくお待ちください。 脅威が検出された場合は、手順に従って駆除してください。
  8. レスキューモードを終了するには、デスクトップの何もない場所を右クリックして表示されるメニューで 終了 を選択し、コンピュータの再起動またはシャットダウンのいずれかを選択します。

- Windows 10の場合 :

  1. 「Windows 10 のレスキューモードでシステムを起動する」 (p. 206)の手順によりレスキュー環境を起動します。
  2. レスキュー環境にシステムがロードされると、 Bitdefender によるスキャン処理が自動的に開始されます。

3. 検査が完了するまでしばらくお待ちください。 脅威が検出された場合は、手順に従って駆除してください。
4. レスキュー環境を終了するには、スキャン結果が表示されたにウィンドウの閉じるボタンをクリックします。

6.2.2. Bitdefender がパソコン上に脅威を検知した場合、どうすればいいのでしょうか？

パソコン上で脅威が検出されるのは以下のようなケースです。

- コンピュータをスキャンした結果、Bitdefenderが感染した項目を発見した。
- 脅威警告（アラート）が表示され、 Bitdefender がパソコン上の脅威をブロックした。

この場合はBitdefenderをアップデートし、脅威情報データベースファイルを最新の状態にしてから、パソコンの全体検査を行なってください。

システムスキャンが完了しましたら、感染ファイルの処理方法を選択してください（駆除、削除または隔離）。

警告
このファイルが Windows の一部または感染したファイルではないと考えられる場合は、次の手順を行わずに、Bitdefender サポートにご連絡ください。

選択した処理が行われず、スキャン ログで削除できなかった感染項目を確認した場合は、これらのファイルを手動で削除する必要があります。

手動で削除する：

1. Bitdefenderのリアルタイム保護を無効にします。
   a. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。
   b. ウイルス対策 パネルで 隔離フォルダ をクリックします。
   c. シールド ウィンドウで Bitdefender シールド をオフにします。
2. Windows 内で隠し属性のファイルを表示します。 これを行う方法については、「Windows で隠し属性のファイルを表示するには？」（p. 76）を参照してください。
3. 感染したファイル（スキャン ログをご確認ください）の場所を参照し、これを削除します。

4. Bitdefenderのリアルタイム保護をONにしてください。

最初の方法では感染を駆除できなかった場合:

1. コンピュータを再起動し、セーフ モードで起動します。 これを行う方法については、「セーフモードでパソコンを再起動させる方法は？」（p. 78）を参照してください。
2. Windows 内で隠し属性のファイルを表示します。 これを行う方法については、「Windows で隠し属性のファイルを表示するには？」（p. 76）を参照してください。
3. 感染したファイル（スキャン ログをご確認ください）の場所を参照し、これを削除します。
4. システムを再起動して通常のモードで起動します。

解決しなかった場合は、「サポートを依頼」（p. 317）項に記載されているBitdefenderサポートにお問い合わせください。

6.2.3. アーカイブ内の脅威を駆除するには？

アーカイブとは、ディスク上の空きスペースを増やすために、ファイル サイズを小さくする特殊なフォーマットで圧縮されたファイル、もしくは、ファイルの集合体のことです。

オープンフォーマットのものもあるため、内部をスキャンするためのオプションを Bitdefender に提供し、これらを削除するための適切な処理を行ってください。

他のアーカイブは、部分的あるいは完全に閉じられているため、Bitdefenderは、それらの内部にある脅威の存在を検出することはできますが、それ以外の処理を行うことはできません。

Bitdefender がアーカイブの内部から脅威を検出し、有効な処理の手段がないと通知してきた場合は、アーカイブへのアクセス権設定による制限があるため、脅威の駆除が不可能であることを意味します。

アーカイブ内にある脅威の駆除方法：

1. パソコン全体の検査を実行し、脅威を含むアーカイブファイルを特定します。
2. Bitdefenderのリアルタイム保護を無効にします。
   a. Bitdefender インターフェイスのナビゲーションメニューにある 保護をクリックします。

b. ウイルス対策 パネルで 隔離フォルダ をクリックします。

c. シールド ウィンドウで Bitdefender シールド をオフにします。

3. アーカイブのある場所を開き、WinZip のような圧縮・解凍アプリケーションを使って解凍してください。
4. 感染したファイルを特定し、削除してください。
5. 感染を完全に削除するため、元のアーカイブを削除してください。
6. WinZip のような圧縮を行うアプリケーションを使用して、新しいアーカイブ内に、ファイルを再圧縮してください。
7. システム上にそれ以外の感染がないことを確認するには、 Bitdefender のリアルタイム アンチウイルス保護をオンにして、システムスキャンを実行します。

注記
アーカイブ（圧縮ファイル）内にある脅威は、解凍して実行されない限りパソコンへ感染することができないため、アーカイブの状態ではシステムへ直接影響を及ぼすことはありません。

解決しなかった場合は、「サポートを依頼」 (p. 317)項に記載されているBitdefenderサポートにお問い合わせください。

6.2.4. メールのアーカイブ内にある脅威はどうやって駆除するのですか？

Bitdefender は、電子メール データベース内の脅威も、ディスクに保存されている電子メール アーカイブ内の脅威のどちらも、識別することができます。

場合によっては、感染したものを特定するのに、スキャンレポートで表示されている情報が必要になります。そして手動でそれを削除します。

電子メールのアーカイブ内にある脅威の駆除方法：

1. Bitdefender で、電子メールのデータベースをスキャンします。
2. Bitdefenderのリアルタイム保護を無効にします。

a. Bitdefender インターフェイスのナビゲーションメニューにある 保護 をクリックします。

b. ウイルス対策 パネルで 隔離フォルダ をクリックします。

c. シールド ウィンドウで Bitdefender シールド をオフにします。

3. メール内から感染したメッセージを探し出すために、スキャン レポートを開き、このメッセージの個別情報（件名、送信者、宛先）を使用します。
4. 感染したメッセージを削除してください。 殆どのメール ソフトは、そこから復元できるように、削除されたメッセージを復元フォルダに移動します。 この回復フォルダからも、メッセージが削除されます。
5. 感染したメッセージを格納したフォルダを圧縮してください。
   - Microsoft Outlook 2007の場合： ファイル メニューの、データ ファイル管理 をクリックします。 圧縮する個人フォルダ(.pst)ファイルを選択し、設定をクリックします。 「圧縮する」をクリックしてください。
   - Microsoft Outlook 2010 / 2013/ 2016: ファイルメニューで「情報」をクリックし、次に「アカウント設定」をクリックします （アカウントの追加・削除、既存の接続設定の変更)。 次にデータファイルを選択し、圧縮する個人フォルダ（.pst）ファイルを選択して設定をクリックしてください。 「圧縮する」をクリックしてください。
6. Bitdefenderのリアルタイム保護をONにしてください。

解決しなかった場合は、「サポートを依頼」 (p. 317)項に記載されているBitdefenderサポートにお問い合わせください。

6.2.5. ファイルが危険だと思った場合はどうすればいいのですか？

Bitdefenderがウイルスを検知しなかったとしても、システムのファイルが感染の疑いがあると感じるかもしれません。

システムが保護されていることを確認するには:

1. Bitdefenderでパソコン全体の検査を実行してください。 これを行う方法については、「パソコン全体のウイルス検査方法は？」 (p. 53)を参照してください。
2. 検査結果にはウイルス感染がないと表示されても、結果に疑問があり、再確認したい場合は、サポートページよりお問い合せください。

   これを行う方法については、「サポートを依頼」 (p. 317)を参照してください。

6.2.6. 検査ログにある「パスワード保護された項目」とは何ですか？

これは Bitdefender が、パスワードで保護されているか、何らかの暗号化がされているファイルを検出したという通知です。

最も一般的なパスワード保護された項目：

- 別のセキュリティ製品に関するファイルです。
- OS 関連のファイルです。

実際に内容をスキャンするため、これらのファイルは解凍するか、暗号を解除する必要があります。

これらの内容が全て解凍されると、 Bitdefender リアルタイム スキャンは、コンピュータの保護を継続するために、自動的にスキャンを実行します。 Bitdefender で、それらのファイルをスキャンする場合は、ファイルに関して更に詳しい内容を提供してもらうため、製品メーカーに連絡する必要があります。

パソコンに対して脅威とはならないため、これらのファイルはそのままにすることをお勧めいたします。

6.2.7. 検査ログにある「スキップした項目」とは何ですか？

スキャン レポート内で 'スキップ' と表示されているファイルは、全て正常なファイルです。

パフォーマンスを良くするため、Bitdefender は、前回のスキャン時から変更されていないファイルはスキャンしません。

6.2.8. 検査ログにある「多重圧縮項目」とは何ですか？

'多重圧縮'に分類されるものは、スキャン エンジンによって解凍できない、もしくは、解読に要する時間が長過ぎるため、システムを不安定にすることが考えられるものを指します。

過剰圧縮と表示されるものは、解凍するにはシステムのリソースを大幅に消費するため、Bitdefenderが検査を省略したものです。 必要な場合は、アーカイブにアクセスした際にリアルタイム保護が検査します。

6.2.9. なぜ Bitdefender は自動的に感染ファイルを削除するのですか？

感染したファイルが検出されると、Bitdefender は自動的に駆除を試みます。 駆除が失敗した場合は、'隔離領域'に移動されます。

脅威の種類によっては、ファイルの一部が感染しているのではなく、ファイル全体が悪意あるコードで書かれているため、駆除できないものもあります。 このような場合、感染したファイルはディスクから完全に削除されます。

信頼できないWEBサイトからダウンロードされたインストールファイルにおいて、よくあるケースです。 そのような場合、インストールファイルを製造元、また他の信頼できるウェブサイトからダウンロードしてください。

ANTIVIRUS FOR MAC

7. インストールと削除

この章は以下のトピックで構成されています:

7.1. システム要件

Bitdefender Antivirus for Mac は、OS X Mavericks (10.9.5)、OS X Yosemite (10.10.5)、 OS X El Capitan (10.11.6)、macOS Sierra (10.12.5 以降)、macOS High Sierra (10.13.0 以降) が動作する、Intel ベースの Macintosh コンピュータにのみインストールできます。

お使いの Mac には 600 MB 以上のハードディスク空き容量が必要です。

Bitdefender Antivirus for Mac の登録とアップデートにはインターネット接続が必要です。

お使いの macOS のバージョンと Mac のハードウェア情報の確認方法

画面左下隅の Apple アイコンをクリックし、この Mac についてを選択します。 表示されるウィンドウで、オペレーティングシステムのバージョンやその他の有用な情報を確認できます。 ハードウェア情報の詳細については追加情報 をクリックします。

7.2. Bitdefender Antivirus for Macをインストールしています

Bitdefender Antivirus for Mac アプリは、お客様の Bitdefender アカウントからインストールすることができます:

1. 管理者としてログインします。
2. 次のサイトへアクセスします : https://central.bitdefender.com
3. メールアドレスとパスワードを使って Bitdefender アカウントにログインします。
4. マイデバイス パネルを選択し、保護をインストール をクリックします。
5. 以下のいずれかのオプションを選択します:

- このデバイスを保護

  このオプションを選択するとインストールファイルを保存できます。

- 他のデバイスを保護

  このオプションを選択してから、ダウンロードリンクを送信 をクリックします。 当該フィールドにメールアドレスを入力してメールを送信をクリックします。 ダウンロードリンクは、以後 24 時間のみ有効です。 リンクの有効期限が切れた場合は、同じ手順を実行して新しいリンクを生成する必要があります。

- Bitdefender をインストールしたいデバイス上で、登録したメールアドレスの受信トレイを開き、届いたメールに記載されているダウンロードボタンをクリックしてください。

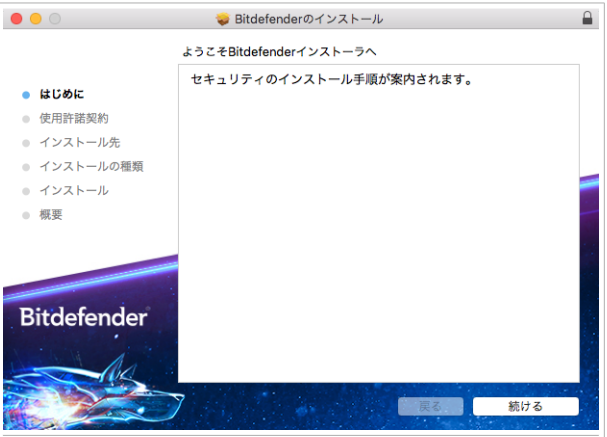
6. ダウンロードした Bitdefender 製品を実行します。
7. インストールを完了する。

7.2.1. インストール処理

Bitdefender Antivirus for Mac をインストールするには:

1. ダウンロードしたファイル をクリックします。 するとインストーラが起動し、インストール処理の案内を開始します。
2. インストール ウィザードに従います。

手順 1 - はじめに



はじめに

続けるをクリックします。

ステップ 2 - サブスクリプション契約を読む

サブスクリプション契約を読む

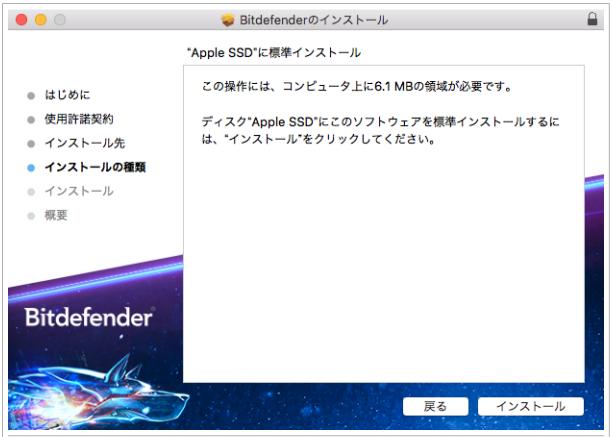
インストールを続行する前に、サブスクリプション契約に同意する必要があります。 サブスクリプション契約には、 Bitdefender Antivirus for

Mac を使用する上で守っていただく条件が記載されていますので、必ずよくお読みください。

続行 をクリックしてから同意 をクリックします。

重要項目
これらの条件に同意しない場合は、続行 をクリックしてから同意しない をクリックし、インストールをキャンセルしてインストーラを終了してください。

手順 3 - インストール開始

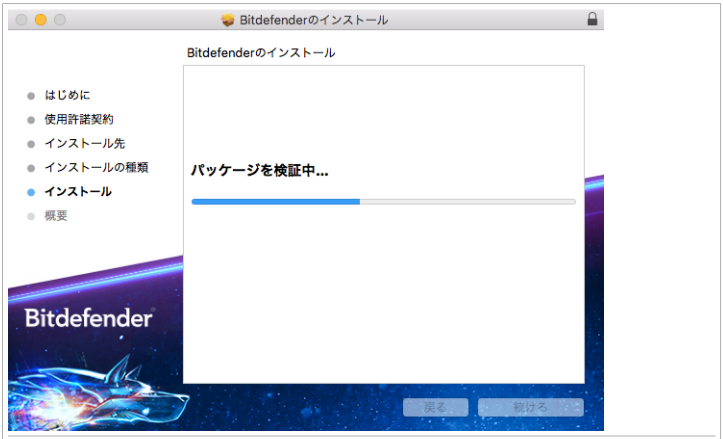


インストール開始

Bitdefender Antivirus for Mac はMacintosh HD/Library/Bitdefender にインストールされます。 インストールパスは変更できません。

インストールを開始するには、インストールをクリックします。

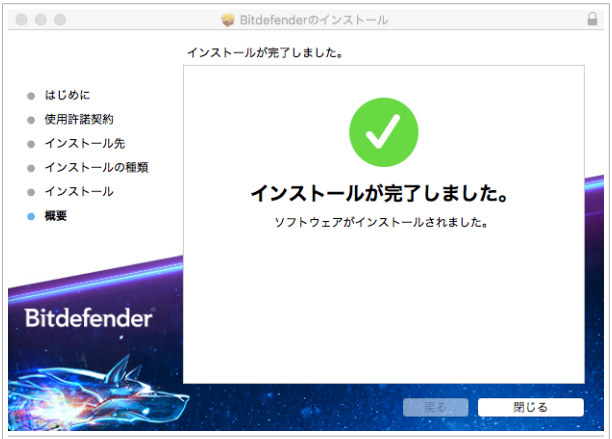
ステップ 4 - Bitdefender Antivirus for Mac をインストールする



Bitdefender Antivirus for Macをインストールしています

インストールが完了するのを待ってから続行 をクリックします。

手順 5 - 完了



終了

閉じる をクリックしてインストーラのウィンドウを閉じます。

インストール処理はこれで完了です。

重要項目
MacOS High Sierra 10.13.0以降に Bitdefender Antivirus for Mac をインストールしている場合、 システム拡張がブロックされている という通知が表示されます。 Bitdefender の機能拡張がブロックされているため、手動で有効にする必要があります。 OK をクリックしてください。 表示された Bitdefender Antivirus for Mac ウィンドウで、セキュリティとプライバシーのリンクをクリックします。 リストから Bitdefender チェックボックスを選択し、 OK をクリックします。

7.3. 保護を設定する

このステップでは、 Bitdefender Antivirus for Mac に含まれている最も重要な機能を紹介しています。 これらのうち一部の機能は自動的にインストールされ、一部は手動で有効にする必要があります。

- Bitdefender シールド - は、すべての新しいファイルと変更されたファイルをリアルタイムでスキャンし、様々な脅威からシステムを保護するために、自動的に有効になります。 インストールしたアプリや、アップデートされたアプリもすべてスキャン対象となります。
- 自動操作の推奨事項 - デバイスのセキュリティとパフォーマンスを改善するためのさまざまな推奨事項を表示します。
- Web 保護 - すべての Web トラフィックをフィルタリングし、悪意のあるコンテンツを遮断します。 使用しているブラウザを選択して TrafficLight をインストールし、ウェブブラウジングを安全に保護してください。
- ランサムウェア保護機能では、個人データを 安全なファイル に追加することで、信頼できないアプリによってアクセスされることを回避できます。 安全なファイル機能を有効にするには、設定 をクリックして該当するボタンをクリックします。

  Time Machine 保護 は自動的に有効になり、お使いのバックアップドライブを保護します。
- プライバシー保護 - VPN アプリは自動的にインストールされ、安全でないワイヤレスネットワークへの接続時にお客様のデータを保護します。

7.4. Bitdefender Antivirus for Mac を削除する

Bitdefender Antivirus for Mac は複雑なアプリケーションのため、アプリケーションのアイコンをアプリケーション フォルダからゴミ箱にドラッグするだけでは削除できません。

Bitdefender Antivirus for Mac を削除するには、次の手順に従ってください:

1. Finderウインドウを開いてApplicationsに移します。
2. Bitdefender フォルダを開いてBitdefenderUninstallerをダブルクリックしします。
3. アンインストールをクリックし、プロセスが完了するのを待ちます。
4. 閉じる をクリックして終了します。

> **重要項目**
> エラーが発生した場合は、「サポートを依頼」（p. 317）に記載されている Bitdefender カスタマーケアまでご連絡ください。

8. セットアップ

この章は以下のトピックで構成されています:

8.1. Bitdefender Antivirus for Mac について

Bitdefender Antivirus for Mac は、以下を含むあらゆるタイプの悪意のあるソフトウェア （「脅威」） を検出・駆除できる強力なアンチウイルススキャナです:

- ランサムウェア
- アドウェア
- ウィルス
- スパイウェア
- トロイの木馬
- キーロガー
- ワーム

このアプリは Mac だけでなく Windows の脅威も検知・駆除できるため、感染したファイルをうっかり家族や友達、同僚に送ってしまうことを完全に防げます。

8.2. Bitdefender Antivirus for Macを開く

Bitdefender Antivirus for Mac はいくつかの方法で開くことができます。

- Launchpad で Bitdefender Antivirus for Mac アイコンをクリックします。
- メニューバーの アイコンをクリックし、メインウィンドウを開く を選択します。
- Finder ウィンドウから アプリケーション に移動し、Bitdefender Antivirus for Mac アイコンをダブルクリックします。

8.3. アプリメイン画面

メインウィンドウでは、セキュリティの状態を確認したり、自動操作機能の推奨事項に従ってコンピュータのセキュリティを向上したりできます。また、システムスキャンを実行したり、ブラウジングを保護したり、Bitdefender アカウントにログインしたりすることもできます。

アプリメイン画面

Bitdefender　自動操作機能は、色々な作業やアクティビティをより効率的かつ安全に行うための、パーソナルセキュリティアドバイザーとして役立ちます。 Bitdefender 自動操作は、仕事、オンラインバンキング、映画鑑賞、ゲームなど、デバイス上で実行しているアクティビティの種類に応じて、各種設定を最適化します。 これにより、 Bitdefender Antivirus for Mac　アプリに含まれている機能による様々なメリットを把握し、それらを最大限に活用することができます。

ウィンドウ上部のステータスバーには、システムのセキュリティ状態がメッセージと色を使って表示されます。 Bitdefender Antivirus for Mac で警告が発生していない場合、ステータスバーは緑色で表示されます。 セキュリティ上の問題が検出されると、ステータスバーが赤に変わります。 問題の詳細とその修復方法については、「問題を修正」 (p. 230)を参照してください。

ステータスバーの下に、お使いの Mac のスキャンする際に使用するボタンが配置されています:

- クイックスキャン – システム上で最も脆弱な場所に対して脅威スキャンを実行します（たとえば文書、ダウンロードファイル、メール、各ユーザーの一時ファイルなど）。
- フルスキャン – システム全体に対して脅威のスキャンを実行します。接続済みのマウントもすべてスキャンされます。
- カスタムスキャン – 特定のファイル、フォルダ、またはボリュームの脅威スキャンを実行できます。

詳細については、「Mac をスキャンする」（p. 227）をご参照ください。

スキャンボタンのほかにも、いくつかの追加オプションが利用可能です:

- Web 保護 – すべての Web トラフィックをフィルタリングし、悪意のあるコンテンツを遮断して Web ブラウジングを保護します。 詳しくは「webからの防御」（p. 231）を参照してください。
- Bitdefender アカウントに移動します – メインインターフェイスの右下部分にある アカウントに移動 のリンクをクリックして Bitdefender アカウントにアクセスします。 詳しくは「Bitdefender Central」（p. 247）を参照してください。
- 残り日数 – サブスクリプションの有効期限の残り日数が表示されます。有効期限の終了後は、リンクをクリックすることでサブスクリプション更新ページにアクセスできます。
- フィードバック – デフォルトのメールクライアントで新しいウィンドウが開き、弊社へのお問い合わせを送信できます。

8.4. アプリ Dock アイコン

Bitdefender Antivirus for Mac のアイコンは、アプリケーションを開くとすぐに Doc に表示されます。 Dock に表示されているアイコンから、ファイルやフォルダの脅威スキャンを簡単に実行できます。 ファイルまたはフォルダを Dock アイコンにドラッグ＆ドロップするだけで、スキャンが直ちに開始します。

Dock アイコン

9. 悪意のあるソフトウェアから保護する

この章は以下のトピックで構成されています:

9.1. 最良事例

お使いのシステムを脅威から保護し、また他のシステムを感染してしまうことを防ぐには、以下のベストプラクティスに従ってください:

- Bitdefender Antivirus for Mac がシステムファイルを自動的にスキャンできるよう、Bitdefender シールドを有効のままにしてください。
- Bitdefender Antivirus for Mac 製品に最新の脅威情報と製品アップデートを適用して、常に最新の状態に保ちましょう。
- Bitdefender Antivirus for Mac によって報告される問題を、定期的にチェックして修正しましょう。 詳細は「問題を修正」 (p. 230)を参照してください。
- ユーザーのコンピュータ上で実行された、 Bitdefender Antivirus for Mac のアクティビティの詳細なログを確認してください。 システムまたはデータのセキュリティに影響を与えるイベントが発生すると、新しいメールが受信箱に届くのと同じように Bitdefender の履歴に新しいメッセージが追加されます 詳しくは「履歴」 (p. 240) にアクセスしてください。
- また、以下のベストプラクティスに従ってください:
  - 外部ストレージ (USB メモリや CD) からダウンロードしたファイルは、特にソースが不明なには必ずスキャンする習慣を付けましょう。

- DMG ファイルをお持ちの場合は、イメージをマウントしてから内容のスキャンを実行します（マウントしたボリューム/イメージ内のファイル）。

ファイル、フォルダ、またはボリュームをスキャンする最も簡単な方法は、 Bitdefender Antivirus for Mac のウィンドウまたは Dock のアイコン上にスキャンしたいファイル、フォルダ、またはボリュームをドラッグアンドドロップする方法です。

それ以外の設定やアクションは必要ありませんが、 必要に応じてアプリケーションの各種設定を変更することが可能です。 詳細については、「環境設定を変更する」 (p. 235)をご参照ください。

9.2. Mac をスキャンする

コンピュータ上で実行されているアプリを常時監視し、脅威に似た挙動を検知して予防するBitdefender シールド機能に加えて、Mac 全体または特定のファイルをいつでもスキャンすることができます。

ファイル、フォルダ、またはボリュームをスキャンする最も簡単な方法は、Bitdefender Antivirus for Mac のウィンドウまたは Dock のアイコン上にスキャンしたいファイル、フォルダ、またはボリュームをドラッグアンドドロップする方法です。 スキャンウィザードが表示され、スキャン処理をガイドします。

スキャンは以下の手順でも開始できます:

1. Bitdefender Antivirus for Mac を開きます。
2. 3 つのうちいずれかのスキャンボタンをクリックして、任意のスキャンを開始します。
   - クイックスキャン – システム上で最も脆弱な場所に対して脅威スキャンを実行します （たとえば文書、ダウンロードファイル、メール、各ユーザーの一時ファイルなど）。
   - フルスキャン – システム全体に対して脅威のスキャンを実行します。接続済みのマウントもすべてスキャンされます。

> **注記**
>
> ハードディスクのサイズによっては、システム全体のスキャンにしばらくの時間がかかる場合があります（最大 1 時間以上）。 パフォーマンス向上のため、このタスクはリソースを多く消費する他のタスク（ビデオ編集など）とは同時に実行しないことをお勧めします。

また、マウント済みのボリュームを環境設定ウィンドウの例外 リストに追加することで、そのボリュームをスキャン対象から除外することもできます。

- カスタムスキャン - 特定のファイル、フォルダ、またはボリュームの脅威スキャンを実行できます。

9.3. Bitdefender Shield（リアルタイム保護）

Bitdefender は、インストールされているすべてのアプリ、それらのアップデート後バージョン、および新規ファイル/変更されたファイルをスキャンすることで、様々な脅威に対するリアルタイム保護を提供します。

リアルタイム保護を無効にするには:

1. Bitdefender Antivirus for Mac を開きます。
2. メニューバーで Bitdefender Antivirus for Mac をクリックし、環境設定 を選択します。
3. 保護タブを選択してから、Bitdefender シールドチェックボックスをオフにします。

警告
これは緊急レベルのセキュリティ問題です。 リアルタイム保護を無効にする場合は、期間をなるべく短めにすることをおすすめします。 リアルタイム保護が無効になっていると、パソコンは脅威から保護されません。

9.4. Time Machine Protection

すべてのエクスターナルソースのアクセスをブロックすることによって、それにすべてのファイルを格納するという決定を含めて Bitdefender タイムマシンプロテクションはお客様のバックアップドライバにとって追加のセキュリティレイヤとして機能します。 お客様のタイムマシンのドライブからのファイルはランサムウェアによって暗号化される場合、尋ねた身代金を支払うことなく、それらを回復することができるようになります。

Time Machine のバックアップから項目を復元する必要がある場合は、Apple のサポートページで手順を確認してください。

タイムマシンプロテクションを有効または無効にする

Time Machine 保護をオン/オフにするには:

1. Bitdefender Antivirus for Mac を開きます。
2. メニューバーで Bitdefender Antivirus for Mac をクリックし、環境設定 を選択します。
3. 保護 タブを選択します。
4. タイムマシンプロテクションのチェックボックスをオンにするかまたはオフにします。

9.5. スキャンウィザード

スキャンを開始すると、 Bitdefender Antivirus for Mac スキャンウィザードが必ず表示されます。

検査しています

各スキャン中に検出および解決された脅威に関するリアルタイムの情報。

Bitdefender Antivirus for Mac がスキャンを完了するまでお待ちください。

注記
スキャンの内容によっては処理に時間がかかる場合があります。

9.6. 問題を修正

Bitdefender Antivirus for Mac は、システムおよびデータのセキュリティに影響を及ぼす可能性のある問題を自動的に検出して通知します。 これにより、セキュリティ上のリスクを簡単かつすばやく修復できます。

Bitdefender Antivirus for Mac が指摘する問題を修復することで、システムおよびデータのセキュリティを最適な状態に保つことができます。

検出された問題の例:

- 新しい脅威情報アップデートが弊社サーバーからダウンロードされていません。
- 脅威がシステム上で検出されましたが、自動的に駆除することができませんでした。
- リアルタイム保護が無効です。

検出された問題を確認・修復するには:

1. Bitdefender Antivirus for Mac を開きます。
2. Bitdefender で警告が発生していない場合、ステータスバーは緑色で表示されます。 セキュリティ上の問題が検出されると、ステータスバーが赤に変わります。
3. 詳しくは説明をご覧ください。
4. 問題が検出された場合は、該当するボタンをクリックして問題に対処してください。

「未解決の脅威」ウィンドウ

未解決の脅威の一覧は、スキャンがバックグラウンドで自動的に行われたか、ユーザーが手動で実行したかに関係なく、システムスキャンを実行するたびに更新されます。

未解決の脅威に対しては、以下の処理を選択できます:

- 手動で削除します。 感染を手動で駆除するにはこのアクションを実行します。
- 例外リストに追加. この処理は、アーカイブ内で検出された脅威に対しては実行できません。

9.7. webからの防御

Bitdefender Antivirus for Mac は TrafficLight 拡張機能を使って Web ブラウジングを完全に保護します。 TrafficLight はすべての Web トラフィックを処理およびフィルタリングし、悪意のあるコンテンツをすべて遮断します。

拡張機能は Mozilla Firefox、Google Chrome、および Safari と連携して利用できます。

TrafficLight 拡張機能を有効にする

TrafficLight 拡張機能を有効にするには、次の手順に従ってください:

1. Bitdefender Antivirus for Mac を開きます。
2. 今すぐ修復 をクリックして Web 保護を有効にします。
3. Bitdefender Antivirus for Mac はシステムにインストールされている Web ブラウザを自動的に検出します。 TrafficLight 拡張機能をお使いのブラウザにインストールするには拡張機能を入手 をクリックします。
4. オンラインのこの場所にリダイレクトされます:

   http://bitdefender.com/solutions/trafficlight.html
5. 無料ダウンロード を選択します。
6. ステップを実行して、お使いの Web ブラウザに適した TrafficLight 拡張機能をインストールします。

拡張機能設定の管理

搭載された多彩な機能が、Webブラウジング中に遭遇する可能性があるあらゆる脅威からお守りします： その機能アクセスするには、ブラウザの設定

の横にあるトラフィックライトアイコンにクリックしてから設定にクリックする：

- Bitdefender トラフィックライト設定
  - 高度な脅威フィルター - マルウェア、フィッシング、詐欺サイトなどのウェブサイトへのアクセスを防ぎます。
  - トラッカー検出器 - 訪問したウェブページ上のトラッカーを検出し、その存在について通知を表示します。
  - 検索結果アナライザー：検索結果内の危険なWebサイトを事前に検知してお知らせします。

    すべての設定がオフになっている場合、ウェブサイトはスキャンされません。
- 許可リスト

  Bitdefenderエンジンでスキャンされないようにwebサイトを除外することができます　対応するフィールドに、ホワイトリストに追加するWebサイトの名前を入力し、追加にクリックします。

  除外されたページに脅威が存在する場合、警告は表示されません。 このため、完全に信頼できるWebサイトのみをこのリストに追加することを強くお勧めします。

ページのレーティングおよびアラート

現在表示中の Web ページを TrafficLight がどのように区分するかによって、以下のいずれかのアイコンがエリア内に表示されます:

このページは安全です。 作業を続行できます。
このページには危険なコンテンツが含まれている可能性があります。ページを開く場合はご注意ください。
Webページには、マルウェアやその他の脅威が含まれているため、すぐにWebページを閉じる必要があります。

Safariでは、トラフィックライトアイコンの背景は黒です。

9.8. アップデート

新しい脅威を日々発見し、対応しています。 それに対処するにはBitdefender Antivirus for Macを最新の脅威情報アップデートで更新することが非常に重要です。

脅威情報アップデートはオンザフライ（=ファイルが累進的に置換される）で更新されます。 これにより、アップデート処理は製品の動作に影響を与えず、また脆弱性も除外されます。

- Bitdefender Antivirus for Mac が最新バージョンになっていれば、最新の脅威でも検出し、感染したファイルを駆除することができます。
- Bitdefender Antivirus for Mac が最新の状態でない場合、 Bitdefender Labs が発見した最新の脅威を駆除できません。

9.8.1. アップデートを要求

アップデートをいつでも手動で要求することができます。

利用可能なアップデートの確認とダウンロードにはインターネット接続が必要です。

アップデートを手動で要求するには:

1. Bitdefender Antivirus for Mac を開きます。
2. メニューバーの アクション ボタンをクリックします。
3. 脅威情報データベースの更新 を選択します。

また、CMD + U を押すことでアップデートをいつでも手動で要求できます。

アップデートの進捗状況とダウンロードされたファイルを確認できます。

9.8.2. プロキシサーバ経由でアップデートを入手する

Bitdefender Antivirus for Mac は、認証不要のプロキシサーバ経由でのみアップデートできます。 プログラムの設定を変更する必要はありません。

認証が必要なプロキシサーバーを経由してインターネットに接続している場合、定期的にプロキシサーバーなしで直接インターネットに接続し、脅威情報アップデートを更新する必要があります。

9.8.3. 新しいバージョンにアップグレード

弊社は、製品に新たな機能を追加したり、問題を修正したりするためのアップデートを定期的に公開します。 これらのアップデートは、新しいファイルをインストールするためにシステムの再起動が必要な場合があります。 デフォルトの設定では、アップデートがシステムの再起動を必要とする場合、 Bitdefender Antivirus for Mac はシステムが再起動されるまでは古

いファイルを利用し続けます。 この場合、アップデート処理はユーザーの作業に一切干渉しません。

製品のアップデートが完了すると、システムの再起動を促すポップアップウィンドウが表示されます。 この通知を逃した場合は、メニューバーから再起動してアップグレード を選択するか、システムを手動で再起動してください。

9.8.4. Bitdefender Antivirus for Mac についての情報を見つける

インストールされている Bitdefender Antivirus for Mac のバージョンを確認するには、バージョン情報 ウィンドウを開いてください。 さらにこのウィンドウでは、サブスクリプション契約、プライバシーポリシー、およびオープンソースライセンスなども確認できます。

「この製品について」を開くには:

1. Bitdefender Antivirus for Mac を開きます。
2. メニューバーで Bitdefender Antivirus for Mac をクリックし、Antivirus for Mac について を選択します。

10. 環境設定を変更する

この章は以下のトピックで構成されています:

10.1. 環境設定にアクセスする

Bitdefender Antivirus for Mac の環境設定ウィンドウを開くには:

1. Bitdefender Antivirus for Mac を開きます。
2. 次の操作が行えます :
   - メニューバーで Bitdefender Antivirus for Mac をクリックし、環境設定 を選択します。
   - メニューバーの アイコンをクリックし、環境設定 を選択します。
   - Command + コンマ (,) を押します。

10.2. アカウント情報

アカウント情報ウィンドウは、サブスクリプションと Bitdefender アカウントについての情報を提供します。

別のBitdefender アカウントでログインしたいときは、 アカウントの切り替え ボタンをクリックしてください。 Bitdefenderアカウントアプリケーションウィンドウに新しいメールアドレスとパスワードを入力しサインイン をクリックします。

このウィンドウでは、マイオファーオプションを設定することもできます。このオプションを許可すると、 Bitdefender からのスペシャルオファーがあるたびに通知が表示されます。

10.3. 保護の設定

保護の環境設定ウィンドウでは、全体のスキャン方針を設定できます。 感染したファイルや、疑わしいファイルに対して実行する処理を選択したり、その他の設定を変更したりできます。

保護の設定

- Bitdefender シールド. Bitdefender シールドは、インストールされているすべてのアプリ、それらのアップデート後バージョン、および新規ファイル/変更されたファイルをスキャンすることで、様々な脅威に対するリアルタイム保護を提供します。 Bitdefender シールドを無効にすることは推奨されません。無効にする必要がある場合は、無効にする時間をできるだけ短くすることをお勧めします。 Bitdefender シールドが無効になっていると、システムを脅威から自動的に保護できなくなります。
- 感染ファイルに対する処理：. 脅威を検出すると、 Bitdefender Antivirus for Mac は、感染したファイルから自動的に悪意のあるコードを取り除き、元のファイルに再構成しなおします。 この操作は、'駆除' と呼ばれます。 駆除ができないファイルについては、感染の可能性があるため、隔離領域 に移動されます。

  推奨はされませんが、感染ファイルに対して一切アクションを実行しないことも可能です。 削除されたファイルはログにのみ記録されます。

  Bitdefender シールドは、システムパフォーマンスへの影響を最小限に抑えつつ、個の脅威。 未解決の脅威がある場合には、それを表示して個別にアクションを選択できます。

- 疑わしい項目に対する処理. ヒューリスティック分析により疑いあるものとして検出されたファイルです。 疑わしいファイルに対しては、駆除する方法がないため、駆除を行うことができません。

  デフォルトでは、疑わしいファイルは隔離領域へ移動されます。 隔離領域にある脅威を実行したり読み出したりすることはできないため、脅威が被害を及ぼすことはありません。

  疑わしいファイルを無視するよう選択することもできます。 削除されたファイルはログにのみ記録されます。

- 新規および変更ファイルのみ検査. Bitdefender Antivirus for Mac に、これまでスキャンしたことがないファイル、および前回のスキャン後に変更されたファイルのみをスキャンさせたい場合はこのチェックボックスを選択します。

  当該チェックボックスを選択することで、ドラッグアンドドロップのスキャンに対してこの設定を適用しないこともできます。

- バックアップしたファイルは検査しない. バックアップファイルをスキャン対象から除外するには、このチェックボックスをオンにしてください。感染したファイルが後で復元された場合、 Bitdefender Antivirus for Mac はそれらを自動的に検出して適切なアクションを実行します。

- Time Machine Protection. タイムマシンに保存されたファイルを保護するには、このチェックボックスをクリックします、 お客様の Time Machine ドライブのファイルがランサムウェアによって暗号化された場合、要求された身代金を支払うことなく、ファイルを復元することができます。

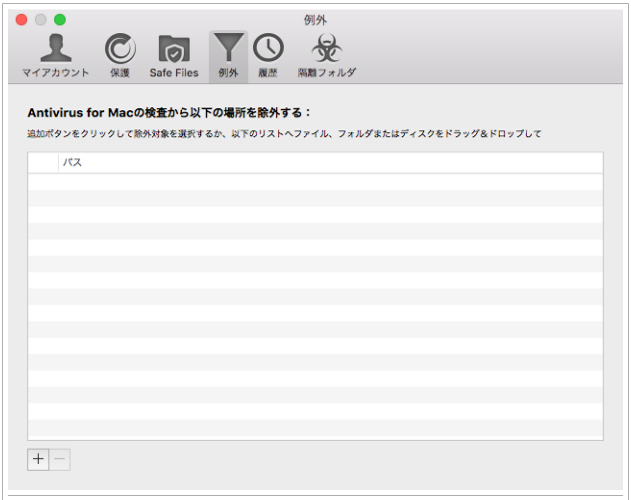
- 自動操作通知. 通知センターで自動操作機能からの通知を受け取りたくない場合は、このチェックボックスをオフにします。

- プライバシー保護. 設定ウィザード で VPN アプリのインストールに失敗した場合、ここから Bitdefender VPN をインストール をクリックしてインストールできます。

10.3.1. スキャン例外

また、 Bitdefender Antivirus for Mac に特定のファイルやフォルダ、あるいはボリューム全体をスキャンさせないようにすることもできます。 たとえば、以下のような項目をスキャンから除外した場合が考えられます:

- 感染済みとして誤認識されるファイル（フォールスポジティブ）
- スキャンエラーを引き起こすファイル
- バックアップボリューム



スキャン例外

例外リストには、スキャンから除外されたパスが含まれています。

スキャンに例外を設定するには 2 通りの方法があります:

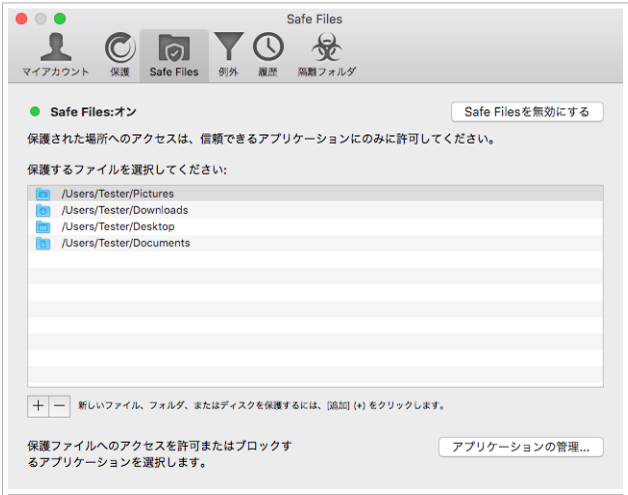
- 例外リストの上にファイル、フォルダ、またはボリュームをドラッグアンドドロップします。
- 例外リストの下にある、プラス（+）の付いたボタンをクリックします。次に、スキャンから除外するファイル、フォルダ、またはボリュームを選択します。

スキャン例外から項目を削除するには、当該項目をリストで選択し、例外リストの下にあるマイナス（-）の付いたボタンをクリックします。

10.4. Safe Files

ランサムウェアは、脆弱性のあるシステムを攻撃してシステムにロックをかけ、ロックを解除する見返りに金銭を要求する悪意のあるソフトウェアです。　この悪意のあるソフトウェアは、偽のメッセージを表示してユーザーをパニックに陥れ、金銭を早く支払うように促します。

最新のテクノロジーを駆使することで、 Bitdefender はシステムに余計な負荷をかけることなく、重要なシステムエリアをランサムウェアの攻撃から守ります。 また、文書や写真、動画などの個人データに信頼できないアプリがアクセスすることも防ぐ必要があります。 Bitdefender のセーフファイル機能では、重要な個人ファイルを保護エリアとして設定し、どのアプリにそのエリアへのアクセスを許可するかを細かく設定できます。



Safe Files

保護環境にファイルを後から追加するには 2 つの方法があります:

- 「セーフファイル」ウィンドウの上にファイル、フォルダ、またはボリュームをドラッグアンドドロップします。
- 保護ファイルの下にある、プラス (+) の付いたボタンをクリックします。 次に、ランサムウェア攻撃から保護したいファイル、フォルダ、またはボリュームを選択します。

システム速度の低下を防ぐため、フォルダ数は 30 個以内におさめるか、あるいは複数のファイルを 1 つのフォルダに保存することをお勧めします。

デフォルトの設定では「ピクチャ」、「デスクトップ」、「ドキュメント」および「ダウンロード」フォルダがマルウェアに対して保護されます。

注記
カスタムフォルダは、現在のユーザーに対してのみ保護可能です。 外部ドライブ、システムファイル、アプリケーションファイルを保護環境に追加することはできません。

不審な挙動を持つ不明なアプリが、追加されたファイルにアクセスしようと試みるたびに通知が届きます。 許可またはブロックをクリックすることで、アプリケーションの管理リストに追加できます。

10.4.1. アプリケーションを管理する

保護されたファイルを変更または削除しようとするアプリケーションは、安全でないと判断され、ブロック中のアプリケーションのリストに追加される場合があります。 そのようなアプリケーションがブロックされたが、問題のないアプリケーションであることが確かな場合は、アプリケーションの管理 ボタンをクリックし、ステータスを「許可」に変更することで許可できます。

「許可」に設定されているアプリは、「拒否」に設定することもできます。

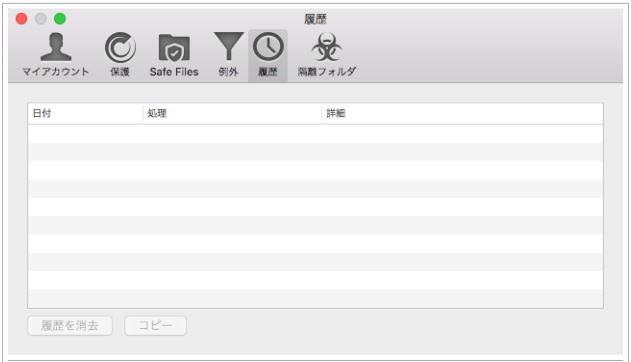
ドラッグ&ドロップか、プラス記号 (+) をクリックして、リストにアプリを追加します。

10.5. 履歴

Bitdefenderは、パソコン上で行なった操作や、各種イベントの詳細ログを作成します。 システムまたはデータのセキュリティに影響を与えるイベントが発生すると、新しいメールが受信箱に届くのと同じように Bitdefender Antivirus for Mac の履歴に新しいメッセージが追加されます。

イベントはBitdefenderの保護を監視・管理するために非常に重要なツールです。 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脅威が発見されましたか、不正なアプリがお使いのタイムマシンのドライブにアクセスしようとしたなど、これらの全部を簡単に確認できます。

製品のアクティビティについての詳細が表示されます。



履歴

履歴ログを削除したいときは、履歴のクリア ボタンをクリックします。

コピー ボタンを使うと、この情報をクリップボードにコピーできます。

10.6. 隔離フォルダ

Bitdefender Antivirus for Mac では、マルウェアに感染したファイルや疑わしいファイルを、隔離領域と呼ばれる安全な領域に隔離することができます。 隔離領域にある脅威を実行したり読み出したりすることはできないため、脅威が被害を及ぼすことはありません。

隔離したファイル

隔離領域セクションでは、隔離フォルダに隔離された全てのファイルを見ることができます。

ファイルを隔離領域から削除するには、当該ファイルを選択して 削除 をクリックします。 隔離されたファイルを元の場所に戻す場合は、復元 をクリックします。

11. VPN

この章は以下のトピックで構成されています:

11.1. VPN について

Bitdefender VPN を使用すると、空港、ショッピングセンター、カフェ、ホテルなどの安全でないワイヤレスネットワークに接続する際に、個人データを安全に保護することができます。 それにより、個人情報の盗難やデバイスの IP アドレスがハッキングされてしまうなどの危険な事態を避けることができます。

VPNは、デバイスとネットワークとの間の安全なトンネルとして機能し、銀行と同等レベルの暗号化を使用してデータを暗号化することで、常に IP アドレスを隠すことができます。 トラフィックは別のサーバーを経由してリダイレクトされます。 そのため、弊社のサービスを利用している他の多数のデバイスの中から、お客様のデバイスを識別することはほぼ不可能です。 さらに、 Bitdefender VPN を経由してインターネットに接続すると、通常は特定の地域からしかアクセスできないコンテンツも楽しむことができます。

注記

一部の国ではインターネット検閲が行われているため、法律によって VPN の使用が禁止されています。 法的な問題を回避するため、 Bitdefender VPN アプリの初回起動時に警告メッセージが表示される場合があります。 このアプリを引き続き使用することで、該当される法律や条例と、生じうるリスクを理解したことになります。

11.2. VPN を開く

BitdefenderVPNアプリを開くには、メニューバーの アイコンにクイックします。 さらに、Applicationsフォルダに移動し、Bitdefenderフォルダを開き、Bitdefender VPNアイコンをダブルクリックします。

11.3. インターフェース

VPN インターフェイスには、アプリの状態（接続・切断）が表示されます。無料バージョンの場合、接続するサーバーの場所は Bitdefender によって最適なサーバーに自動的に設定されますが、プレミアムユーザーは 場所を選択 リストから接続したいサーバーを自由に選択できます。 VPN サブスクリプションの詳細については、「サブスクリプション」 (p. 264)を参照してください。

接続または切断するには、画面上部に表示されている状態をクリックします。 VPN 接続時はメニューバーのアイコンが黒く表示され、VPN 切断時には白いアイコンが表示されます。

VPN インターフェース

接続している間インタフェースの下部に経過時間が表示されます。 さらに多くのオプションにアクセスするには、右上の ⚙ アイコンをクリックします。

- マイアカウント - Bitdefender アカウントと、VPN サブスクリプションについての詳細が表示されます。 別のアカウントでサインインしたいときはアカウントの切り替えをタップします。
- 設定 - 必要に応じて、製品の挙動をカスタマイズできます:
  - VPN をシステム起動後に実行する
  - VPN が自動的に接続または切断したときに通知を受け取る
- Premium にアップグレードする - 無料版の製品を使用している場合は、ここからプレミアムプランにアップグレードできます。 今すぐアップグレード をクリックすると、サブスクリプション購入ページにリダイレクトされます。
- ヘルプ - サポートセンターのプラットフォームにリダイレクトされ、BitdefenderVPNの使用方法に関する参考資料をご覧いただけます。
- アプリ情報 - インストールされているバージョンに関する情報が表示されます。
- 終了 - アプリを終了します。

11.4. サブスクリプション

Bitdefender VPN では、デバイスごとに毎日 200MB のトラフィックを無料で使用できます。最適なサーバーに自動的に接続するため、必要なときにいつでも接続を保護することが可能です。

サーバーの場所を自由に選択して無制限のトラフィックおよび無制限のコンテンツへアクセスを利用したい場合は、プレミアムバージョンにアップグレードする必要があります。

製品のインターフェース内に表示されている 無制限トラフィックを入手ボタンをタップすることで、いつでも Bitdefender VPN のプレミアムバージョンにアップグレードできます。

Bitdefender VPN プレミアムサブスクリプションは、 Bitdefender Antivirus for Mac のサブスクリプションとは独立しているため、VPN はセキュリティのサブスクリプションの状態とは関係なく常に利用可能です。 Bitdefender VPN プレミアムサブスクリプションの有効期限が終了したが、 Bitdefender

Antivirus for Mac のサブスクリプションがまだ有効な場合、自動的に無料プランへと切り替わります。

Bitdefender VPN はクロスプラットフォームの製品であり、Windows、macOS、Android、および iOS に対応した Bitdefender 製品で利用することができます。 プレミアムプランにアップグレードすると、同じ Bitdefender アカウントでログインするだけで、お使いのすべての製品でサブスクリプションを利用することができます。

12. BITDEFENDER CENTRAL

この章は以下のトピックで構成されています:

12.1. Bitdefender Centralについて

Bitdefender Central は、製品のオンライン機能およびサービスにアクセスしたり、 Bitdefender がインストールされているデバイス上でリモートタスクを実行したりできるプラットフォームです。 インターネットに接続しているコンピュータまたはモバイルデバイスから https://central.bitdefender.com にアクセスして Bitdefender アカウントにログインするか、Android または iOS デバイスの Bitdefender Central アプリから直接ログインすることができます。

お使いのスマートフォンに Bitdefender Central アプリをインストールするには:

- Android デバイス - Google Play で Bitdefender Central アプリを検索し、ダウンロードしてインストールします。 必要なステップを実行して、インストールを完了してください。
- iOS デバイス - App Store で Bitdefender Central アプリを検索し、ダウンロードしてインストールします。 必要なステップを実行して、インストールを完了してください。

ログインすると、以下の操作が可能になります:

- Bitdefender を Windows、macOS、iOS、および Android オペレーティングシステムにダウンロードしてインストールします。 ダウンロードできる製品は以下の通りです:
  - Bitdefender Antivirus for Mac
  - BitdefenderWindows製品ライン
  - Bitdefender Mobile Security for Android
  - Bitdefender Mobile Security for iOS
  - Bitdefender ペアレンタル コントロール

- Bitdefender のサブスクリプションを管理・更新します。
- ネットワークに新しいデバイスを追加して、いつでもどこでも管理できます。
- ペアレンタルコントロール を設定することで、お子様のデバイスの設定を行ったり、いつでも好きな場所でお子様のオンラインアクティビティを監視したりできます。

12.2. Bitdefender Centralにアクセス

Bitdefender Central にアクセスする方法はいくつか用意されています。実行したいタスクによって、以下の選択肢があります:

- Bitdefender Antivirus for Mac のメインインターフェイスから:
  1. 画面の右下部分にある アカウントに移動 のリンクをクリックします。
- ウェブブラウザから:
  1. インターネットに接続しているデバイスで、ウェブブラウザを起動します。
  2. 次のサイトへアクセスします : https://central.bitdefender.com
  3. メールアドレスとパスワードを使ってアカウントにログインします。
- お使いの Android または iOS デバイスから:

  インストールした Bitdefender Central アプリを開きます。

> **注記**
> この資料には、Web インターフェイス上で見つけることのできるオプションが含まれています。

12.3. サブスクリプション

Bitdefender Central 管理画面では、すべてのデバイスのサブスクリプションを簡単に管理することができます。

12.3.1. サブスクリプションの有効化

サブスクリプションは、 Bitdefender アカウントを使ってインストール中に有効化できます。 有効化の実行と同時に、サブスクリプションの有効期限のカウントダウンが開始します。

アクティベーションコードを弊社リセラーから購入した場合やプレゼントとして入手した場合は、その内容をアカウント内の Bitdefender のサブスクリプションに追加することが可能です。

アクティベーション　コードを使ってサブスクリプションを有効化するには、次の手順に従ってください:

1. Bitdefender Centralにアクセスします。
2. ウィンドウの左上隅にある ☰ アイコンをクリックし、マイ サブスクリプション パネルを選択します。
3. アクティベーション コード ボタンをクリックし、該当の入力欄にコードを入力します。
4. 続行するにはACTIVATEにクリックします。

サブスクリプションが有効になりました。

デバイスへの製品のインストールを開始するには、「Bitdefender Antivirus for Macをインストールしています」（p. 215）を参照してください。

12.3.2. サブスクリプションを購入

以下の手順を実行することで　Bitdefender　アカウントからサブスクリプションを直接購入できます:

1. Bitdefender Centralにアクセスします。
2. ウィンドウの左上隅にある ☰ アイコンをクリックし、マイ サブスクリプション パネルを選択します。
3. 今すぐ購入リンクをクリックすると、 購入用の Web ページに移動します。

処理を完了すると、サブスクリプションの利用状況が製品のメインインターフェイスの右下隅に表示されます。

12.4. マイ・デバイス

Bitdefender アカウントの マイデバイス エリアでは、管理しているデバイスにインストールされている Bitdefender 製品のインストール、管理、リモート操作などが可能です（デバイスの電源が入っていて、インターネットに接続されている必要があります）。 デバイスカードには、デバイス名、保護状態、および保護状態に影響があるセキュリティリスク （存在する場合）が表示されます。

12.4.1. デバイスをカスタマイズする

デバイスを簡単に識別できるように、デバイス名をカスタマイズすることが可能です:

1. Bitdefender Centralにアクセスします。
2. マイデバイス パネルを選択します。
3. 任意のデバイスカードをクリックし、ウィンドウの右上隅にある アイコンをクリックします。
4. 設定を選択します
5. デバイス名フィールドに新しい名前を入力して 保存 をクリックします。

各デバイスに所有者を作成して割り当てることで、より効率的な管理が可能です。

1. Bitdefender Centralにアクセスします。
2. マイデバイス パネルを選択します。
3. 任意のデバイスカードをクリックし、ウィンドウの右上隅にある アイコンをクリックします。
4. プロファイルを選択します。
5. オーナーを追加 をクリックし、該当するフィールドに入力します。 プロフィールをカスタマイズするには生年月日を設定し、写真、メールアドレス、電話番号を追加します。
6. プロファイルを保存するには 追加 をクリックします。
7. デバイスの所有者 リストから任意の所有者を選択し、割り当て をクリックします。

12.4.2. リモート処理

リモートデバイス上の Bitdefender をアップデートするには:

1. Bitdefender Centralにアクセスします。
2. マイデバイス パネルを選択します。
3. 任意のデバイスカードをクリックし、ウィンドウの右上隅にある アイコンをクリックします。

4. アップデートを選択します。

デバイスカードをクリックすると、以下のタブが利用可能になります:

- ダッシュボード. このウィンドウでは、選択したデバイスの詳細を表示したり、保護状態をチェックしたり、 テータスや過去7日間にブロックされた脅威の件数を確認したりできます。 保護ステータスは、製品に問題がないときには緑、対処が必要な問題があるときには黄色、デバイスが危険に晒されているときには赤で表示されます。 製品に影響する問題が発生している場合は、上部のステータスエリアにあるドロップダウンの矢印をクリックして詳細を確認します。 ここで、お使いのデバイスのセキュリティに影響を与えている問題を手動で修正することができます。
- 保護. このウィンドウでは、デバイスに対してクイックスキャンまたはシステムスキャンをリモートから実行できます。 スキャン ボタンをクリックして処理を開始します。 また、デバイス上で前回スキャンが実行された日時を確認したり、重要な情報を含む最新スキャンのレポートを確認したりできます。 これら 2 つのスキャン処理の詳細については「Mac をスキャンする」 (p. 227) を参照してください。

13. よくある質問

Bitdefender Antivirus for Mac のサブスクリプションを購入する前に試用するには？

あなたは Bitdefender の新規ユーザーであるため、製品を購入する前に試用することが可能です。 試用期間は 30 日間で、 Bitdefender のサブスクリプションを購入すれば試用期間が過ぎた後も製品を使い続ける事ができます。 Bitdefender Antivirus for Mac を使用するには:

1. 以下の手順を実行して Bitdefender アカウントを作成します:
   - 次のサイトへアクセスします : https://central.bitdefender.com
   - 該当する欄に必要な情報を入力してください。 入力いただいたデータは機密情報として扱われます。
   - 続行する前に、使用条件に同意する必要があります。 サブスクリプション契約には、 Bitdefender を使用する上で守っていただく条件が記載されているため、必ずよくお読みください。

     また、プライバシーポリシーにアクセスして参照することもできます。
   - アカウント作成をクリックします。
2. Bitdefender Antivirus for Mac を以下の手順でダウンロード:
   - マイデバイス パネルを選択し、保護をインストール をクリックします。
   - 以下のいずれかのオプションを選択します:
     - このデバイスを保護

       このオプションを選択するとインストールファイルを保存できます。
     - 他のデバイスを保護

       このオプションを選択してから、ダウンロードリンクを送信 をクリックします。 当該フィールドにメールアドレスを入力してメールを送信 をクリックします。 ダウンロードリンクは、以後 24 時間のみ有効です。 リンクの有効期限が切れた場合は、同じ手順を実行して新しいリンクを生成する必要があります。

- Bitdefender をインストールしたいデバイス上で、登録したメールアドレスの受信トレイを開き、届いたメールに記載されているダウンロードボタンをクリックしてください。
- ダウンロードした Bitdefender 製品を実行します。

アクティベーション・コードを持っています。 サブスクリプションに追加するにはどうすれば良いですか？

アクティベーションコードを弊社リセラーから購入した場合やプレゼントとして入手した場合は、その内容をアカウント内の Bitdefender のサブスクリプションに追加することが可能です。

アクティベーション コードを使ってサブスクリプションを有効化するには、次の手順に従ってください:

1. Bitdefender Centralにアクセスします。
2. ウィンドウの左上隅にある アイコンをクリックし、マイ サブスクリプション パネルを選択します。
3. アクティベーション コード ボタンをクリックし、該当の入力欄にコードを入力します。
4. 続行するにはACTIVATEにクリックします。

拡張機能が Bitdefender アカウントと、画面右下に表示されているインストール済み Bitdefender Antivirus for Mac 製品に表示されます。

スキャンログに、まだ未解決の項目が残っています。 どうやって削除できますか？

スキャンログの未解決項目の例:

- アーカイブへの制限アクセス（xar、rar など）

  解決方法:Finder で表示 オプションで手動でファイルを探して削除します。 削除後はゴミ箱を必ず空にしてください。

- アクセスの制限されたメールボックス（Thunderbird など）

  解決方法: アプリケーションを使って、感染ファイルが含まれるエントリを削除します。

- バックアップのコンテンツ

  解決方法: 保護環境設定のバックアップコンテンツのスキャニングをしません オプションを有効にするか、検出されたファイルを 例外に追加します。

感染したファイルが後で復元された場合、 Bitdefender Antivirus for Mac はそれらを自動的に検出して適切なアクションを実行します。

注記
アクセス制限ファイルとは、 Bitdefender Antivirus for Mac が開くことができても、変更を加えることはできないファイルを指します。

製品のアクティビティについての詳細はどこで確認できますか？

Bitdefender ▪ は、すべての重要なアクション、ステータス変化、およびアクティビティに関連する重要なメッセージのログを保存します。 ▪ ログにアクセスするには、 Bitdefender Antivirus for Mac の環境設定のウィンドウを開いてください。

1. Bitdefender Antivirus for Mac を開きます。
2. 次の操作が行えます：
   - メニューバーで Bitdefender Antivirus for Mac をクリックし、環境設定 を選択します。
   - メニューバーの アイコンをクリックし、環境設定 を選択します。
   - Command + コンマ（,）を押します。
3. 履歴 タブを選択します。

   製品のアクティビティについての詳細が表示されます。

Bitdefender Antivirus for Mac はプロキシサーバ経由でアップデートできますか？

Bitdefender Antivirus for Mac は、認証不要のプロキシサーバ経由でのみアップデートできます。 プログラムの設定を変更する必要はありません。

認証が必要なプロキシサーバーを経由してインターネットに接続している場合、定期的にプロキシサーバーなしで直接インターネットに接続し、脅威情報アップデートを更新する必要があります。

Bitdefender Antivirus for Macをアンインストール（削除）するには？

Bitdefender Antivirus for Mac を削除するには、次の手順に従ってください:

1. Finderウインドウを開いてApplicationsに移します。

2. Bitdefender フォルダを開いてBitdefenderUninstallerをダブルクリックしします。
3. アンインストールをクリックし、プロセスが完了するのを待ちます。
4. 閉じる をクリックして終了します。

重要項目
エラーが発生した場合は、「サポートを依頼」（p. 317）に記載されている Bitdefender カスタマーケアまでご連絡ください。

Web ブラウザから TrafficLight 拡張機能を削除するには？

- TrafficLight 拡張機能を Mozilla Firefox から削除するには、次の手順に従ってください:
  1. Mozilla Firefox ブラウザを開きます。
  2. ツール を開いて アドオン を選択します。
  3. 左側の 拡張機能 を選択します。
  4. 拡張機能を選択して、削除をクリックします。
  5. ブラウザを再起動して、削除処理を完了します。
- TrafficLight 拡張機能を Google Chrome を削除するには、次の手順に従ってください:
  1. Google Chrome ブラウザを開きます。
  2. 右上にある詳細 をクリックします。
  3. その他ツールを開いて拡張機能を選択します。
  4. 削除する拡張機能の横にあるChromeから削除  アイコンをクリックします。
  5. 削除処理を確定するにはアンインストール をクリックしてください。
- Safari から Bitdefender TrafficLight を削除するには、次の手順に従ってください:
  1. Safari ブラウザを開きます。
  2. ブラウザのツールバーの  をクリックして、環境設定をクリックします。

3. 拡張機能 タブを選択し、Bitdefender TrafficLight on Safari 拡張機能を参照します。
4. 拡張機能を選択して アンインストール をクリックします。
5. 削除処理を確定するにはアンインストール をクリックしてください。

Bitdefender VPN を使うべき理由

インターネット上のコンテンツにアクセスしたり、ダウンロードやアップロードを行うときには注意が必要です。 ウェブブラウジング時には、Bitdefender VPN を使って安全な接続を確保することをお勧めします。

- 公衆 Wi-Fi ネットワークに接続したい
- 自宅や海外など自分の現在いる場所に関係なく、特定の地域でしかアクセスできないコンテンツを利用したい
- 個人データのプライバシーを守りたい（ユーザー名、パスワード、クレジットカード情報など）
- IP アドレスを隠したい

Bitdefender VPN を使うとデバイスのバッテリーの減りが早くなりますか?

Bitdefender VPN は、お客様の個人情報を保護し、セキュリティ保護されていないワイヤレスネットワークへの接続時に IP アドレスを隠し、特定の国の制限されたコンテンツにもアクセスできるように設計されています。 デバイスのバッテリー浪費を避けるため、必要なときにだけ VPN を有効にして、オフライン時は接続を切断することをお勧めします。

Bitdefender VPN で接続すると、インターネットが遅くなるのはどうしてですか?

Bitdefender VPN は、快適なウェブブラウジングを提供できるように設計されていますが、利用しているインターネット接続の速度や、サーバーまでの距離によっては、接続速度が低下する恐れがあります。 この場合、現在位置から遠くのサーバー（たとえば米国から中国など）に接続する必要がない場合は、 Bitdefender VPN が自動的に選択する最寄りのサーバーに接続することを許可するか、あるいは現在位置に最も近いサーバーを接続することをお勧めします。

MOBILE SECURITY FOR IOS

14. BITDEFENDER MOBILE SECURITY FOR IOS とは？

公共料金の支払い、旅行の予約、商品・サービスの購入などをオンラインで行うことは非常に便利で簡単です。 しかし、インターネットを経由する性質上、これらには一定のリスクが付きまといます。特に、適切なセキュリティ措置を講じない場合、個人データの漏洩や、ハッキングなどの脅威の危険性はさらに高くなります。 オンラインアカウントや、スマートフォンに記録されている個人データを保護することは、この時代に最も重要な事柄の１つだといえます。

Bitdefender Mobile Security for iOS では以下が行えます:

- 保護されていない無線ネットワークへの接続時に個人データを保護。.
- インターネット上で使用しているアカウントが、データ漏えいの被害にあっていないか確認。
- 紛失または盗難に遭ったデバイスの位置情報確認、ロック、データ消去。

Bitdefender Mobile Security for iOS は無料でインストールできますが、Bitdefender アカウントを使ったアクティベーションが必要です。

15. セットアップ

デバイス 要件

Bitdefender Mobile Security for iOS は iOS 10 以上が動作するすべてのデバイスで利用できます。アクティベーションやオンラインアカウントのデータ漏えい検出には、インターネット接続が必要です。

Bitdefender Mobile Security for iOSをインストールしています

- Bitdefender Centralからインストールできます
  - iOS の場合
    1. 次のサイトへアクセスします：https://central.bitdefender.com
    2. お客様の Bitdefender アカウントでログインしてください
    3. ウィンドウの左上隅にある ☰ アイコンをクリックし、マイデバイス を選択します。
    4. 保護をインストールをタップしてから、このデバイスを保護をタップします。
    5. App Store アプリにリダイレクトされます。 App Store 画面で、インストールオプションを選択してください。
  - Windows、macOS、および iOS 上:
    1. 次のサイトへアクセスします：https://central.bitdefender.com
    2. お客様の Bitdefender アカウントでログインしてください
    3. ウィンドウの左上隅にある ☰ アイコンをクリックし、マイデバイス を選択します。
    4. 保護をインストールを押してから、他のデバイスを保護を押します。
    5. ダウンロードリンクを送信を押します。
    6. 当該フィールドにメールアドレスを入力してメールを送信 をクリックします。 ダウンロードリンクは、以後 24 時間のみ有効です。リンクの有効期限が切れた場合は、同じ手順を実行して新しいリンクを生成する必要があります。

7. Bitdefender をインストールしたいデバイス上で、登録したメールアドレスの受信トレイを開き、届いたメールに記載されているダウンロードボタンを押してください。

- App Store

  Bitdefender Mobile Security for iOS を検索してアプリをインストールします。 ▪

インストール処理を開始するには、サブスクリプション契約に同意する必要があります。 サブスクリプション契約には、 Bitdefender Mobile Security for iOS を使用する上で守っていただく条件が記載されていますので、必ずよくお読みください。

続行をタップして次のウィンドウに進みます。

Bitdefender アカウントにログイン

Bitdefender Mobile Security for iOS を使用するには、Facebook、Google、または Microsoft アカウントにアプリからサインインし、いずれかのアカウントと Bitdefender デバイスをリンクする必要があります。 アプリの初回起動時には、アカウントへのサインインを促されます。

デバイスをBitdefenderアカウントに紐付ける方法

1. 対応するフィールドに Bitdefender アカウントのメールアドレスとパスワードを入力します。 Bitdefender アカウントをまだ持っていない場合は、当該リンクを選択して作成してください。
2. ▪サインイン をタップします。 ▪

Facebook、Google、または Microsoft アカウントを使用してログインするには、利用したいサービスを または次でサインイン エリア内でタップします。 選択したサービスのログイン画面へリダイレクトされます。 手順に従ってアカウントを Bitdefender Mobile Security for iOS へリンクさせてください。

注記
Bitdefenderはお客様のアカウントのパスワードや、お友達の連絡先など、機密情報へアクセスすることはできません。

ウィザード

アプリの初回起動時には、製品の機能に関する情報を含むイントロウィザードが表示されます。 次へ をタップしてガイドを続けるあるいはスキップをタップしてウイザードを閉じます。

ダッシュボード

デバイスのアプリー覧画面にある ▪ Bitdefender Mobile Security for iOSのアイコンをタップして、アプリケーションのWEB管理画面を開きます。 ▪

アプリ初回起動時には Bitdefenderから通知が表示されるように求められます。 Bitdefenderがアプリに関連する何かを伝える必要があるたびにできるように、許可をタップして通知を許可してください。 Bitdefender通知を管理するには、設定>通知>モバイルセキュリティをアクセスします。

必要な情報にアクセスするには、画面下部にある機能名が書かれたアイコンをタップします。

VPN
通信の暗号化を行うことで、セキュア化されていないネットワーク上でも安全に通信を行なえるようにします。 詳細については、「VPN」 (p. 263)をご参照ください。

アカウントプライバシー
お客様のメールアカウントが漏洩していないか調べましょう。 詳細については、「アカウントプライバシー」 (p. 266)をご参照ください。

盗難対策
紛失したデバイスの位置を特定し、ロックをかけて個人データが第三者に漏洩することを防ぎましょう。 詳細については、「デバイス盗難対策機能」 (p. 268)をご参照ください。

追加のオプションを表示するには、デバイス上のアプリホーム画面にある ••• アイコンをクリックします。 以下のオプションが表示されます:

- 購入情報の復元 - ここでは、iTunes アカウントで購入した VPN プレミアムサブスクリプションを復元することができます。
- はじめる - こちらから製品のクイックツアーが表示されます。
- フィードバック - こちらからデフォルトのメールクライアントが起動し、アプリに関するフィードバックを送信することができます。

- この製品について - こちらからインストールされている製品のバージョン、サブスクリプション契約、プライバシーポリシー、オープンソースライセンスのコンプライアンスに関する情報にアクセスできます。

16. VPN

Bitdefender VPN を使用すると、空港、ショッピングセンター、カフェ、ホテルなどの安全でないワイヤレスネットワークに接続する際に、個人データを安全に保護することができます。 それにより、個人情報の盗難やデバイスの IP アドレスがハッキングされてしまうなどの危険な事態を避けることができます。

VPNは、デバイスとネットワークとの間の安全なトンネルとして機能し、銀行と同等レベルの暗号化を使用してデータを暗号化することで、常に IP アドレスを隠すことができます。 トラフィックは別のサーバーを経由してリダイレクトされます。 そのため、弊社のサービスを利用している他の多数のデバイスの中から、お客様のデバイスを識別することはほぼ不可能です。 さらに、 Bitdefender VPN を経由してインターネットに接続すると、通常は特定の地域からしかアクセスできないコンテンツも楽しむことができます。

注記
一部の国ではインターネット検閲が行われているため、法律によって VPN の使用が禁止されています。 法的な結果を避けるために、 BitdefenderVPN機能を初めて使用すると警告メッセージが表示されることがあります。 この機能を引き続き使用することにより、国の適用される規制およびお客様がさらされている可能性のあるリスクを認識していることを確認したことになります。

Bitdefender VPN をオンにするには:

1. 画面下部にある アイコンをタップします。
2. 安全でないワイヤレスネットワークへの接続時に、保護を有効したい場合に 接続 をタップします。

   接続を無効にしたいときは 切断 をタップします。

注記
初めてVPNをオンにすると、 Bitdefenderがネットワークトラフィックを監視するVPN設定をセットアップできるようにするプロンプトが表示されます。 許可をタップして続行する。 スマートフォンを保護するための認証方法（指紋またはPINコード）が設定されている場合は、あれを使用する必要があります。

VPN が有効になると、ステータスバーに VPN アイコンが表示されます。

バッテリーの消費を抑えるため、不要なときはVPN をオフにすることをおすすめします。

プレミアムサブスクリプションを購入済みで、任意のサーバーに自由に接続したい場合は、VPN インターフェイスで サーバーの場所 をタップし、接続したいサーバーの場所を選択します。 VPN サブスクリプションの詳細については、「サブスクリプション」 (p. 264)を参照してください。

VPN

16.1. サブスクリプション

Bitdefender VPN では、デバイスごとに毎日 200MB のトラフィックを無料で使用できます。最適なサーバーに自動的に接続するため、必要なときにいつでも接続を保護することが可能です。

サーバーの場所を自由に選択して無制限のトラフィックおよび無制限のコンテンツへアクセスを利用したい場合は、プレミアムバージョンにアップグレードする必要があります。

VPN ウィンドウにある プレミアム VPN を有効にするボタンをタップすることで、いつでも Bitdefender VPN プレミアムバージョンにアップグレードできます。 サブスクリプションには、年額タイプと月額タイプの 2 種類が用意されています。

Bitdefender プレミアムVPNサブスクリプションは、 Bitdefender Mobile Security for iOS無料サブスクリプションとは独立しています。つまり、プレミアムVPNサブスクリプションはサブスクリプション有効期間内に利用できるようになります。 Bitdefenderプレミアム VPN契約の有効期限が切れた場合、自動的に無料プランに戻ります。

Bitdefender VPN はクロスプラットフォームの製品であり、Windows、macOS、Android、および iOS に対応した Bitdefender 製品で利用することができます。 プレミアムプランにアップグレードすると、同じ Bitdefender アカウントでログインするだけで、お使いのすべての製品でサブスクリプションを利用することができます。

17. アカウントプライバシー

Bitdefender アカウントのプライバシーは、オンライン決済、オンラインショッピング、またはアプリやウェブサイトにサインインする際に使用するアカウントで、データ漏洩が発生していないかを検出します。 各種アカウントには、お客様のパスワード、クレジットカード情報、銀行口座情報などが保存されている可能性があり、それらが適切に保護されていない場合、個人情報の窃盗やプライバシーの侵害が発生する恐れがあります。

確認後に、各アカウントのプライバシー状態が表示されます。

アカウントの漏えいの有無を確認したい場合は、漏えいをスキャン をタップします。

個人情報を安全に保つために:

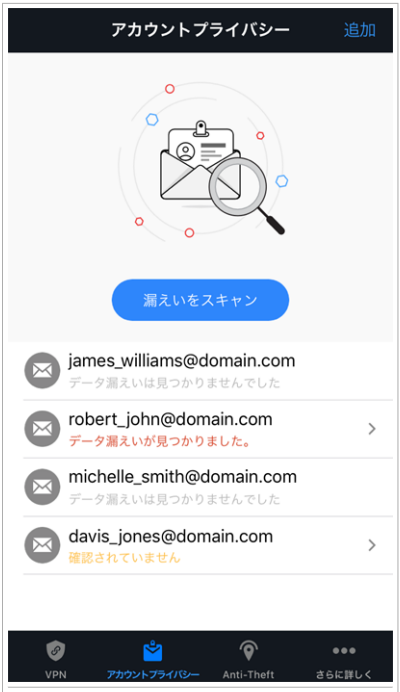
1. 画面下部にある アイコンをタップします。
2. 画面右上の 追加 をタップします。
3. 入力欄にメールアドレスを入力し、次へをタップします。

   Bitdefender では、個人情報を表示する前にこのアカウントの確認を実施する必要があります。 したがって、確認コードが記載されたメールが、指定されたメールアドレス宛てに送信されます。
4. 受信トレイを確認し、受け取ったコードをアプリの アカウントのプライバシー エリアに入力します。 受信トレイに確認メールが届かない場合は、迷惑メールフォルダを確認してください。

   確認済みアカウントのプライバシー状態が表示されます。

アカウント情報の漏洩が発覚した場合には、直ちにパスワードを変更することを強く推奨します。 強力で安全なパスワードを作成するには、次のヒントを参考にしてください:

- 8文字以上で設定してください。
- 大文字や小文字を使用してください。
- 数字および#、@、%、!などの記号を最低1つ使用してください。



アカウントプライバシー

18. デバイス盗難対策機能

Bitdefender ▪ は、紛失したデバイスの位置を特定し、個人データが第三者に漏えいすることを防ぎます。

デバイスから盗難対策を有効にし、必要なときにウェブブラウザからBitdefender Centralにアクセスするだけです。

Bitdefender Mobile Security for iOS ▪ は、以下のデバイス盗難対策機能を提供します: ▪

リモートロケーション
デバイスの位置を地図で確認できます。

位置情報の精度はBitdefenderが認識できるかどうかによって異なります。

- デバイスのGPSが有効になっていて、GPS衛星からの電波が受信出来る状態（例：屋外にいる場合）にある場合は、位置情報は数メートルの範囲にまで絞り込むことができます。
- デバイスが屋内にあり、デバイス側のWi-Fiが有効になっていて、さらに無線通信環境が近くにある場合、位置情報は十数メートルの範囲まで絞り込むことができます。
- それ以外の場合、位置情報はモバイルネットワークの情報のみで判定されるため、絞り込める範囲は数百メートルとなります。

リモートロック
デバイスの画面を遠隔からロックできます。

リモートワイプ
紛失したデバイス上の個人データをすべて削除します。

デバイス盗難対策を有効にする

デバイス盗難対策機能をオンにする方法:

1. 画面下部にある  アイコンをタップします。
2. スイッチをオンにします。
3. デバイスの盗難・紛失時に Bitdefender がデバイスの位置情報を特定できるように、デバイスの位置情報へのアクセスを許可してください。 この通知は、 Bitdefenderの盗難対策を初めて有効にした場合にのみ表示

されます。 Bitdefenderアクセスを管理するには、[設定]> プライバシー>ロケーションサービス>モバイルセキュリティに移動します。

4. デバイスで初めて盗難対策機能を有効にした時、MDM（Mobile Device Management）プロファイルもインストールする必要がありますので、 次の手順に進みます。

   a. 許可をタップすると、設定にリダイレクトされます。

   b. Installをタップして、 Bitdefenderがアクティベーションプロセスを続けるために必要なMDM（モバイルデバイス管理）プロファイルをインストールします。

      スマートフォンを保護するためにPINコードが設定されている場合は、それを使用する必要があります。

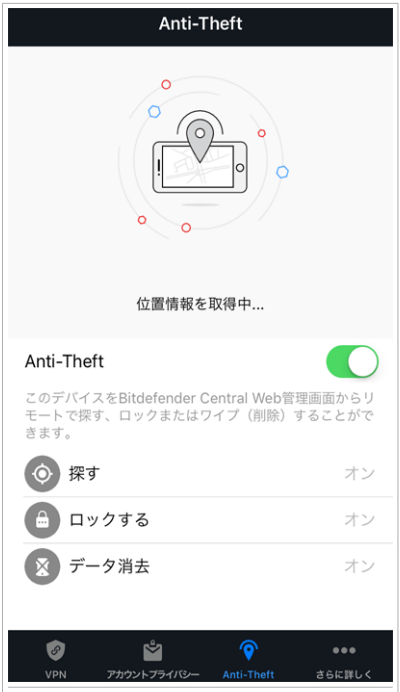
   c. CAルート証明書およびモバイルデバイス管理に関連する情報をお読みください。

   d. 要約された条件に同意する場合は、インストールをタップします。

   e. リモート管理アラート内で信頼をタップし、完了をクリックしてウィンドウを閉じます。

注記

現在のBitdefenderMDMプロファイルのインストールが失敗した場合、古いMDMプロファイルがすでにインストールされているため削除する必要があります。 それゆえ、設定> 一般設定 > デバイス管理> Bitdefenderに移動します。 検出されたプロファイルを選択し、管理の削除をタップします。 スマートフォンを保護するためにPINコードが設定されている場合は、それを使用する必要があります。 もう一度管理の削除をタップして選択を確定します。 再度盗難対策機能を有効にしてください。 問題が解決しない場合は、bdios@bitdefender.comで当社チームにメールをお送りください。



盗難対策

Bitdefender Central (Web コントロール)▪ からデバイス盗難対策機能を使用する

Bitdefenderアカウントで盗難対策機能を使用するには：

1. 次のサイトへアクセスします：https://central.bitdefender.com
2. お客様の Bitdefender アカウントでログインしてください
3. ウィンドウの左上隅にある ☰ アイコンをクリックし、マイデバイス を選択します。
4. 設定したいデバイスをタップして選択し、盗難対策　タブをタップします。▪
5. ウィンドウの下部フィールドで、使用する機能のアイコンをタップします。

IPアドレスを表示 – 選択したデバイスの前回のIPアドレスを表示します。
位置確認- デバイスの位置を 地図で表示します。
ロック – デバイスをロックし、ロック解除に必要となる PIN コードを設定します。 ▪
ワイプ – デバイス上のすべてのデータを削除します。 ▪

重要項目
デバイスをワイプすると、盗難対策の機能も全て機能しなくなります。

19. BITDEFENDER アカウント

Bitdefender アカウントは、 Bitdefender Mobile Security for iOS をアクティベートするために必要です。 製品のオンライン機能およびサービスにアクセスしたり、 Bitdefender がインストールされているデバイス上でリモートタスクを実行したりしたいときは、 https://central.bitdefender.com にアクセスすることで、インターネットに接続されているあらゆるコンピュータまたはモバイルデバイスからお客様アカウントにログインできます。

マイ・デバイス

Bitdefender アカウントの マイデバイス エリアでは、管理しているデバイスにインストールされている Bitdefender 製品のインストール、管理、リモート操作などが可能です（デバイスの電源が入っていて、インターネットに接続されている必要があります）。 デバイスカードには、デバイス名、保護状態、および保護状態に影響があるセキュリティリスク （存在する場合）が表示されます。

デバイスを簡単に識別できるように、デバイス名をカスタマイズして、それぞれのデバイスに所有者を作成・割り当てることが可能です:

1. ウィンドウの左上隅にある ☰ アイコンをクリックし、マイデバイス を選択します。
2. 目的のデバイスカードをタップし、画面の右上にある ⋮ アイコンをタップします。 以下のオプションを利用できます：
   - 設定 - ここで、選択したデバイスの名前を変更することができます。
   - プロファイル - ここで、選択したデバイスに対してプロファイルを割り当てることができます。 所有者を追加 をクリックして対応するフィールドに入力し、名前、メールアドレス、電話番号、性別、生年月日、プロフィール画像などを設定します。
   - 削除- ここでは、割り当てられたデバイスと一緒に、 Bitdefender アカウントからプロファイルが削除されます。

別のBitdefenderアカウントでログインする

別のBitdefenderアカウントでログインするには：

1. 画面下部にある ••• アイコンをタップします。

2. ログアウトをタップします。
3. 対応するフィールドに Bitdefender アカウントのメールアドレスとパスワードを入力します。
4. ▪ サインイン をタップします。 ▪

MOBILE SECURITY FOR ANDROID

20. 保護機能

Bitdefender Mobile Security ▪ は以下の機能によって Android デバイスを保護します: ▪

- ウイルススキャン
- アカウントプライバシー
- webからの防御
- VPN
- ▪ 盗難対策、以下を含む: ▪
  - リモートロケーション
  - リモートデバイスロック
  - リモートデバイス消去
  - リモートデバイスアラート
- アプリロック
- レポート
- WearON

製品の各機能を 14 日間無料でお試しいただけます。 有効期限の終了後もモバイルデバイスの保護を継続するには、製品版をご購入ください。

21. セットアップ

デバイス 要件

Bitdefender Mobile Security ▪ は Android 4.0.3 以上のすべてのデバイスで動作します。 ▪ クラウドベースの脅威スキャンにはインターネット接続が必要です。

Bitdefender Mobile Securityをインストールしています

- Bitdefender Centralからインストールできます
  - Android 上
    1. 次のサイトへアクセスします：https://central.bitdefender.com
    2. お客様の Bitdefender アカウントでログインしてください
    3. ウィンドウの左上隅にある ☰ アイコンをクリックし、マイデバイス を選択します。
    4. 保護をインストールをタップしてから、このデバイスを保護をタップします。
    5. ▪ Google Play アプリにリダイレクトされます。 ▪ Google Play 画面で、インストールオプションを選択してください。
  - Windows、MacOS、および iOS 上
    1. 次のサイトへアクセスします：https://central.bitdefender.com
    2. お客様の Bitdefender アカウントでログインしてください
    3. ウィンドウの左上隅にある ☰ アイコンをクリックし、マイデバイス を選択します。
    4. 保護をインストールを押してから、他のデバイスを保護を押します。
    5. ダウンロードリンクを送信を押します。
    6. 当該フィールドにメールアドレスを入力してメールを送信 をクリックします。 ダウンロードリンクは、以後 24 時間のみ有効です。リンクの有効期限が切れた場合は、同じ手順を実行して新しいリンクを生成する必要があります。

7. Bitdefender をインストールしたいデバイス上で、登録したメールアドレスの受信トレイを開き、届いたメールに記載されているダウンロードボタンを押してください。

- Google Play から

  Bitdefender Mobile Security を検索してアプリをインストールします。 ▪

  または QR コードをスキャンします:

QRコード

アクティベーションを続行する前に、サブスクリプション契約に同意する必要があります。 サブスクリプション契約には、 Bitdefender Mobile Security を使用する上で守っていただく条件が記載されていますので、必ずよくお読みください。

続行をタップして次のウィンドウに進みます。

Bitdefender アカウントにログイン

Bitdefender Mobile Security を使用するには、Facebook、Google、または Microsoft アカウントにアプリからサインインし、いずれかのアカウントと Bitdefender デバイスをリンクする必要があります。 アプリの初回起動時には、アカウントへのサインインを促されます。

Bitdefender Mobile Security をBitdefender をインストールした場合、アプリは自動的にそのアカウントにログインしようとします。 ▪

デバイスをBitdefenderアカウントに紐付ける方法

1. ▪ Bitdefender Mobile Security を開きます。 ▪

2. 対応するフィールドに Bitdefender アカウントのメールアドレスとパスワードを入力します。 Bitdefender アカウントをまだ持っていない場合は、当該リンクを選択して作成してください。
3. ▪サインイン をタップします。▪

Facebook、Google、または Microsoft アカウントを使用してログインするには、利用したいサービスを または次でサインイン エリア内でタップします。 選択したサービスのログイン画面へリダイレクトされます。 手順に従ってアカウントを Bitdefender Mobile Security へリンクさせてください。

注記
Bitdefenderはお客様のアカウントのパスワードや、お友達の連絡先など、機密情報へアクセスすることはできません。

保護を設定する

アプリにサインインすると、保護を設定する ウィンドウが開きます。 デバイスを保護するため、以下の手順を実行することをお勧めします:

- サブスクリプションの状態。Bitdefender Mobile Security による保護を受けるには、製品を使用できる期間を定めたサブスクリプションを使って製品をアクティベートする必要があります。 サブスクリプションの有効期限が終了すると、アプリは動作を停止し、デバイスは保護されなくなります。▪

  アクティベーションコードをお持ちの場合は、コードを持っています をタップしてから アクティベート をタップします。

  新しい Bitdefender アカウントでサインインした場合、製品の各機能を 14 日間無料でお試しいただけます。

- Web 保護 。 お使いのデバイスで Web 保護を有効にするためにアクセシビリティの許可が必要な場合は 有効化をタップします。 するとアクセシビリティメニューが開きますので Bitdefender Mobile Security をタップして、該当するスイッチをオンにしてください。

- マルウェアスキャナ。 デバイス上に脅威がないことを確認するため、このスキャンを 1 回実行してください。 スキャン処理を開始するには 今すぐスキャン をタップします。

  スキャンが開始すると、すぐにダッシュボードが表示されます。 ここでは各デバイスのセキュリティ状態を確認することができます。

ダッシュボード

デバイスのアプリー覧画面にある ▪ Bitdefender Mobile Securityのアイコンをタップすると、アプリケーションの管理画面が開きます。▪

ダッシュボードでは、デバイスのセキュリティ状態が表示されるほか、自動操作機能がデバイスのセキュリティを向上するための推奨事項を提案します。

ウィンドウ上部のステータスカードには、デバイスのセキュリティ状態がメッセージと色を使って表示されます。 Bitdefender Mobile Security で警告が発生していない場合、ステータスバーは緑色で表示されます。 セキュリティ上の問題が検出されると、ステータスバーが赤に変わります。

Bitdefender 自動操作機能は、色々な作業やアクティビティをより効率的かつ安全に行うための、パーソナルセキュリティアドバイザーとして役立ちます。 Bitdefender の自動 操作は、仕事、オンラインバンキング、映画鑑賞、ゲームなど、デバイス上で実行しているアクティビティの種類に応じて、各種設定を最適化します。 これにより、 Bitdefender Mobile Security アプリに含まれている機能による様々なメリットを把握し、それらを最大限に活用することができます。

実行中のプロセスや、入力が必要な機能がある場合、さらに多くの情報と、実行可能なアクションがダッシュボードに表示されます。

画面の左上隅にある メニュー ボタンから、 Bitdefender Mobile Security 機能にアクセスしたり、セクション間を簡単に移動したりできます:▪

ウイルススキャン
: オンデマンドスキャンを起動したり、ストレージスキャンを有効/無効にすることができます。 詳細については、「ウイルススキャン」 (p. 281)をご参照ください。

アカウントプライバシー
: オンラインアカウントでデータ漏洩が発生していないかどうかを確認します。 詳細については、「アカウントプライバシー」 (p. 284)をご参照ください。

webからの防御
: Web保護機能のオン/オフを切り替えることができます。 詳細については、「webからの防御」 (p. 286)をご参照ください。

VPN
通信の暗号化を行うことで、セキュア化されていないネットワーク上でも安全に通信を行なえるようにします。 詳細については、「VPN」 (p. 288)をご参照ください。

盗難対策
盗難対策機能のオン/オフを切り替えたり、盗難対策機能の設定を変更することができます。 詳細については、「デバイス盗難対策機能」 (p. 292)をご参照ください。

アプリロック
PIN アクセスコードを設定することで、インストール済みのアプリケーションを保護できます。 詳細については、「アプリロック」 (p. 297)をご参照ください。

レポート
すべての重要なアクション、ステータス変化、およびアクティビティに関連する重要なメッセージのログを保存します。 詳細については、「レポート」 (p. 302)をご参照ください。

WearON
お使いのスマートウォッチと通信し、スマートフォンを紛失したときに現在位置を確認することができます。 詳細については、「WearON」 (p. 303)をご参照ください。

22. ウイルススキャン

Bitdefenderは、インストール時スキャンおよびオンデマンドスキャンにより、あなたのデバイスとデータを悪意のあるアプリから保護します。

注記
モバイルデバイスがインターネットに接続されていることを確認してください。 デバイスがインターネットに接続されていない場合、スキャン処理は開始されません。

- インストール時スキャン

  アプリをインストールすると、 Bitdefender Mobile Security はクラウドサーバを使って自動的にスキャンします。 インストール済みアプリがアップデートされるたびに同じスキャン処理が開始されます。

  悪意のあるアプリが見つかった場合には、アンインストールを推奨するアラートが表示されます。 ▪アンインストール をクリックすると、アプリのアンインストール画面に移動します。▪

- オンデマンドスキャン（手動スキャン）

  デバイスにインストールしたアプリが安全かどうかを確認するには、オンデマンドスキャンを起動してください。

  オンデマンドスキャンを開始するには、ダッシュボードのマルウェアスキャナの ▪スキャン開始 ボタンをタップします。▪

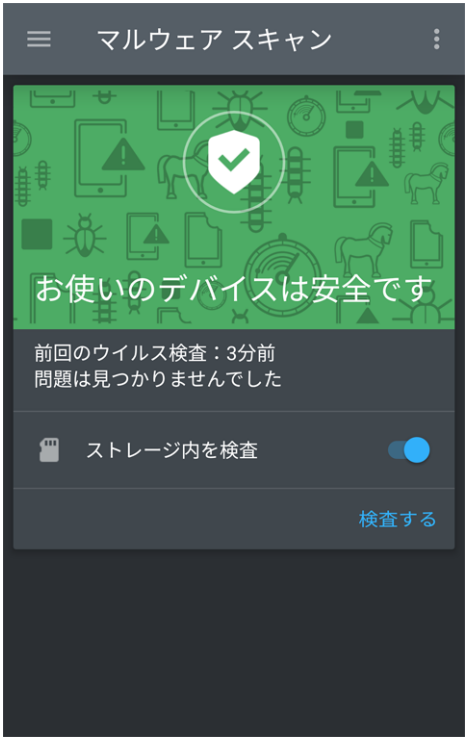
  または以下の手順でスキャンを実行することもできます:

  1. ▪ Bitdefender Mobile Security を開きます。▪
  2. ▪メニュー ボタンをタップして、リストから マルウェアスキャナ を選択します。▪
  3. ▪スキャン開始 をタップします。▪

  注記
  Android 6 でマルウェアスキャナ機能を使用するには追加のパーミッションが必要です。 ▪スキャン開始 ボタンをタップした後、以下に対して Allow を選択します:▪

  - ▪アンチウイルス による通話の発信と管理を許可しますか？▪
  - ▪アンチウイルス による写真、メディアおよびファイルへのアクセスを許可しますか？▪

スキャンの進行状況が表示され、処理はいつでも停止することが可能です。



マルウェアスキャン

デフォルトの設定では、▪ Bitdefender Mobile Security はデバイスの内部ストレージと、マウントされている SD カードをスキャンします。そのため危険性のあるアプリは、デバイス上でダメージを引き起こす前に確実に検知されます。▪

スキャンストレージ設定を有効/無効にするには:

1. ▪ Bitdefender Mobile Security を開きます。▪
2. ▪メニュー ボタンをタップして、リストから マルウェアスキャナ を選択します。▪
3. 該当するスイッチをタップします。

ストレージスキャンは、▪設定 エリアで  ボタンをタップして、該当するスイッチをタップすることでも有効/無効を切り替えられます。▪

悪意のあるアプリが検出された場合、そのアプリについての情報が表示され、▪アンインストール ボタンをタップして削除できます。 ▪

マルウェアスキャナ カードは、お使いのデバイスの現在のセキュリティ状態を表示します。 デバイスが安全な状態であれば、カードは緑色で表示されます。 デバイスをスキャンする必要があったり、ユーザーによるアクションが必要な状態になると、カードの色が赤に変わります。

23. アカウントプライバシー

Bitdefender アカウントのプライバシーは、オンライン決済、オンラインショッピング、またはアプリやウェブサイトにサインインする際に使用するアカウントで、データ漏洩が発生していないかを検出します。 各種アカウントには、お客様のパスワード、クレジットカード情報、銀行口座情報などが保存されている可能性があり、それらが適切に保護されていない場合、個人情報の窃盗やプライバシーの侵害が発生する恐れがあります。

確認後に、各アカウントのプライバシー状態が表示されます。

自動再チェックがバックグラウンドで実行されるように設定されていますが、毎日手動でスキャンを実行することも可能です。

確認済みメールアカウントを含む、新しい漏洩が検出されるたびに通知が表示されます

個人情報を安全に保つために:

1. ▪ Bitdefender Mobile Security を開きます。 ▪
2. ▪メニュー ボタンをタップして、リストから アカウントのプライバシーを選択します。 ▪
3. 画面の右下にある青い丸をタップします
4. 対応するフィールドにメールアドレスを入力し、次へをクリックします。

   Bitdefender では、個人情報を表示する前にこのアカウントの確認を実施する必要があります。 したがって、確認コードが記載されたメールが、指定されたメールアドレス宛てに送信されます。
5. 受信トレイを確認し、受け取ったコードをアプリの アカウントのプライバシー エリアに入力します。 受信トレイに確認メールが届かない場合は、迷惑メールフォルダを確認してください。

   確認済みアカウントのプライバシー状態が表示されます。

アカウント情報の漏洩が発覚した場合には、直ちにパスワードを変更することを強く推奨します。 強力で安全なパスワードを作成するには、次のヒントを参考にしてください:

- 8文字以上で設定してください。
- 大文字や小文字を使用してください。
- 数字および#、@、%、!などの記号を最低1つ使用してください。

プライバシー侵害されたアカウントを確保したら、特定されたリークを解決済みとしてマークして、変更を確認することができます。 有効にすることもできます:

1. ▪ Bitdefender Mobile Security を開きます。 ▪
2. ▪ メニュー ボタンをタップして、リストから アカウントのプライバシーを選択します。 ▪
3. 保護したばかりのアカウントをタップします。
4. データ漏えいエリアではアカウントを確保したリークを左にスワイプします。
5. アイコンをタップします。
6. 解決済みにするオプションが表示されます。

   確認をタップすると、アカウントが保護されていることを確認できます。

検出されたすべての漏えいが解決済みとしてマークされると、新しい漏えいが検出されるまで、アカウントはリークされたとして表示されなくなります。

24. WEBからの防御

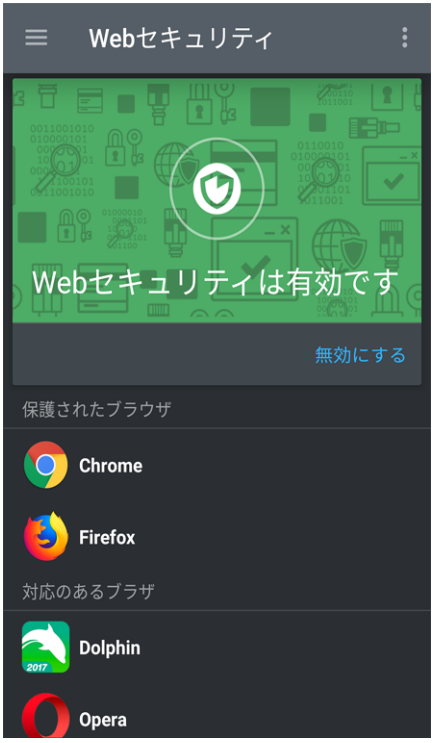
ウェブセキュリティ機能は、 Bitdefender のクラウドサービスを使って、デフォルトの Android ブラウザ、Google Chrome、Firefox、Opera、Opera Mini、Dolphin。 サポートされているブラウザの完全なリストはウェブセキュリティのセクションで確認できます。

もしURLの接続先が既知のフィッシング詐欺や偽装サイト、またはスパイウェアやウイルスなどの悪意のあるコンテンツの場合、それらのサイトは一時的にブロックされアラートが表示されます。

アラートを無視してWebページを開くか、安全なページに戻ることができます。

注記

Android 6でWebセキュリティ機能を使用するには追加の許可設定が必要です。アクセシビリティ サービスとして登録する権限を許可し、要求された際には ▪オンにする をタップします。 アンチウイルス をタップしてスイッチを有効にし、 デバイスのパーミッションへのアクセスに同意することを確認します。 ▪


Webセキュリティ
Webセキュリティは有効です
無効にする
保護されたブラウザ
Chrome
Firefox
対応のあるブラザ
Dolphin
Opera

webからの防御

25. VPN

Bitdefender VPN を使用すると、空港、ショッピングセンター、カフェ、ホテルなどの安全でないワイヤレスネットワークに接続する際に、個人データを安全に保護することができます。 それにより、個人情報の盗難やデバイスの IP アドレスがハッキングされてしまうなどの危険な事態を避けることができます。

VPNは、デバイスとネットワークとの間の安全なトンネルとして機能し、銀行と同等レベルの暗号化を使用してデータを暗号化することで、常に IP アドレスを隠すことができます。 トラフィックは別のサーバーを経由してリダイレクトされます。 そのため、弊社のサービスを利用している他の多数のデバイスの中から、お客様のデバイスを識別することはほぼ不可能です。 さらに、 Bitdefender VPN を経由してインターネットに接続すると、通常は特定の地域からしかアクセスできないコンテンツも楽しむことができます。

注記
一部の国ではインターネット検閲が行われているため、法律によって VPN の使用が禁止されています。 法的な結果を避けるために、 BitdefenderVPN機能を初めて使用すると警告メッセージが表示されることがあります。 この機能を引き続き使用することにより、国の適用される規制およびお客様がさらされている可能性のあるリスクを認識していることを確認したことになります。

Bitdefender VPN をオン/オフにする方法は 2 つあります:

- ダッシュボードの VPN カード内の電源ボタンをタップします。

  Bitdefender VPN の状態が表示されます。

- メニュー ボタンをタップして、リストから VPN を選択します。

  安全でないワイヤレスネットワークへの接続時に保護を有効したい場合に毎回 接続 をタップします。

  接続を無効にしたいときは 切断 をタップします。

注記
VPNを初めてオンにするときは、 BitdefenderでVPNトラフィックを監視するVPN接続を設定するように求められます。 OKをタップして続行します。

Bitdefender VPN が有効になると、ステータスバーに アイコンが表示されます。

バッテリーの消費を抑えたいときは、VPN 機能が必要のないときにオフにすることをお勧めします。

プレミアムサブスクリプションを購入済みで、任意のサーバーに自由に接続したい場合は、VPN 機能で 場所を選択 をタップし、接続したいサーバーの場所を選択します。 VPN サブスクリプションの詳細については、「サブスクリプション」（p. 290）を参照してください。

VPN

ダッシュボードから VPN カードの 詳細 をクリックすると、次のような機能を利用できます:

- 毎日の残りトラフィック量を確認したり、プレミアムバージョンにアップグレードしたりできます - これらの情報は VPN の無料版で利用可能です。

- 接続したいサーバーを選択し、サブスクリプションの残り時間を表示 – 情報は プレミアムVPN バージョンで確認できます。

VPN設定

VPN機能メニューの  ボタンをタップし、設定を選択して、VPNの詳細設定を行います。

VPN設定に次のオプションが設定できます：

- クイックアクセス VPN 通知 – デバイスのステータスバーに、VPN をすばやくオンにできる通知が表示されます。
- 保護されていない Wi-Fi への接続時の通知 – 保護されていない Wi-Fi に接続するたびに、デバイスのステータスバーに VPN を使用することを推奨する通知が表示されます。
- オンラインバンキング利用時の通知 – 銀行のサイトなどオンラインバンキングにアクセスするたびに、デバイスのステータスバーに VPN を使用することを推奨する通知が表示されます。

サブスクリプション

Bitdefender VPN では、デバイスごとに毎日 200MB のトラフィックを無料で使用できます。最適なサーバーに自動的に接続するため、必要なときにいつでも接続を保護することが可能です。

サーバーの場所を自由に選択して無制限のトラフィックおよび無制限のコンテンツへアクセスを利用したい場合は、プレミアムバージョンにアップグレードする必要があります。

ダッシュボードまたはVPNウィンドウで利用できるプレミアムVPNを有効にするボタンをタップすると、いつでも Bitdefenderプレミアム VPNバージョンにアップグレードできます。

Bitdefender VPN プレミアムサブスクリプションは、 Bitdefender Mobile Security のサブスクリプションとは独立しているため、VPN はセキュリティのサブスクリプションの状態とは関係なく常に利用可能です。Bitdefender VPN プレミアムサブスクリプションの有効期限が終了したが、Bitdefender Mobile Security のサブスクリプションがまだ有効な場合、自動的に無料プランへと切り替わります。

Bitdefender VPN はクロスプラットフォームの製品であり、Windows、macOS、Android、および iOS に対応した Bitdefender 製品で利用することができ

ます。 プレミアムプランにアップグレードすると、同じ Bitdefender アカウントでログインするだけで、お使いのすべての製品でサブスクリプションを利用することができます。

26. デバイス盗難対策機能

Bitdefender ▪ は、紛失したデバイスの位置を特定し、個人データが第三者に漏えいすることを防ぎます。

デバイスから盗難対策を有効にし、必要なときにウェブブラウザからBitdefender Centralにアクセスするだけです。

インターネットにアクセスできない場合でも、通常のテキストメッセージを使って携帯電話からスマートフォンに ▪SMS コマンド を送信することで、デバイスおよびデータを保護できます。 ▪

Bitdefender Mobile Security ▪ は、以下のデバイス盗難対策機能を提供します: ▪

リモートロケーション
: デバイスの位置を Google マップで表示します。 現在地は5秒ごとに再読み込みされ、移動中でも正確に位置を捉えることができます。

  位置情報の精度はBitdefenderが認識できるかどうかによって異なります。

  - デバイスのGPSが有効になっていて、GPS衛星からの電波が受信出来る状態（例：屋外にいる場合）にある場合は、位置情報は数メートルの範囲にまで絞り込むことができます。
  - デバイスが屋内にあり、デバイス側のWi-Fiが有効になっていて、さらに無線通信環境が近くにある場合、位置情報は十数メートルの範囲まで絞り込むことができます。
  - それ以外の場合、位置情報はモバイルネットワークの情報のみで判定されるため、絞り込める範囲は数百メートルとなります。

IPアドレスを表示
: 選択したデバイスの前回の IP アドレスを表示します。 IPアドレス表示をタップしてからそれを見ることができます。

リモートワイプ
: 紛失したデバイス上の個人データをすべて削除します。

リモートロック
: デバイスの画面をロックして、ロック解除用の PIN 番号を設定します。

デバイスにアラートを送信（スクリーム）

デバイスに表示するメッセージをリモートから送信したり、デバイスのスピーカーで大音量で再生するサウンドをリモートから発信させることができます。

デバイスを紛失してしまった場合は、デバイスの画面にリモートからメッセージを表示して、デバイスを拾った人に返却方法を知らせることができます。

デバイスが見つからないが、おそらく近くにあると思われる場合（たとえば家やオフィスの中など）には、デバイス上で大音量のサウンドを鳴らす方法が非常に有効です。 音はデバイスがサイレントモードになっていても再生されます。

デバイス盗難対策を有効にする

盗難対策機能を有効にするには、ダッシュボードの盗難対策カードの設定を完了してください。

または以下の手順で盗難対策を有効にすることもできます:

1. ▪ Bitdefender Mobile Security を開きます。 ▪
2. ▪ メニュー ボタンをタップして、リストから 盗難対策 を選択します。 ▪
3. ON にする をタップします。
4. この機能をするために以下の手順を開始します:

> **注記**
> Android 6 で盗難対策機能を使用するには追加のパーミッションが必要です。 有効にするには、以下の手順を実行します:
>
> - ▪ 盗難対策を有効化 をタップしてから ON にする をタップします。 ▪
> - 以下のパーミッションを許可します:
>   a. ▪ アンチウイルス による SMS メッセージの送信および表示を許可しますか？ ▪
>   b. ▪ アンチウイルス によるデバイスの位置情報へのアクセスを許可しますか？ ▪
>   c. ▪ アンチウイルス による連絡先へのアクセスを許可しますか？

a. 管理者権限を付与する

これらの権限は窃盗防止モジュールの動作に必要なため、許可しないと続行できません。

b. アプリの暗証番号を設定する

窃盗防止機能の設定が不正に変更されることを防ぐには、PIN コードを設定するのが有効です。 窃盗防止機能の設定を変更しようとすると、毎回 PIN コードを入力を求められ、入力しないと変更は適用されません。 もしくは、指紋認証に対応したデバイスであれば、PIN コードの代わりに指紋認証を使用することができます。

注記
同じ PIN コードがアプリロックでも使われるので、インストールされているアプリの保護に役立ちます。

c. スナップフォトを有効にする

スナップフォト機能が有効になっている状態で、誰かがお客様のアプリへのアクセスを試みると、 Bitdefender は自動的にその人物の写真を撮影します。 この機能についての詳細は、 「スナップショット」(p. 299)を参照してください。

d. 盗難対策用に信頼する番号を設定

SMS 制御 タブを選択し、信頼できる電話番号を入力するか連絡先から選択し、番号を保存 をタップします。 信頼できる電話番号には、お客様がよく知っている人物の電話番号や、お客様が所有する別の電話番号を使用できます。

デバイスに別の SIM カードがデバイスに挿入されると、 Bitdefender Mobile Security は新しい電話番号を含むテキストメッセージを、信頼できる番号に自動的に送信します。

そのため、デバイスの SIM カードが差し替えられて、電話番号が変わってしまっていても、デバイスに SMS コマンドを送信することができます。

重要項目
このステップでは必須ではありませんが、初回セットアップ時に信頼できる番号を設定しておくことを推奨します。 ワイプコマンドは、事前に設定した信頼できる番号から送られた場合以外は動作しません。

窃盗防止を有効にすると、窃盗防止画面から Web コントロールおよび SMS コントロールボタンをタップすることで、個別にオン/オフを切り替えることができます。

Bitdefender Central（Web コントロール）からデバイス盗難対策機能を使用する

注記
すべての盗難対策機能を使用するには、デバイスのデータ使用設定の バックグラウンドデータ のオプションが有効になっている必要があります。

Bitdefenderアカウントで盗難対策機能を使用するには：

1. Bitdefender Centralにアクセスします。
2. ウィンドウの左上隅にある アイコンをクリックし、マイデバイス を選択します。
3. マイデバイス ウィンドウで設定したいデバイスを選択します。
4. 盗難対策 タブをタップします。
5. 画面下部にある アイコンをタップし、使用したい機能のボタンをタップします。

   位置確認- デバイスの位置を Google マップで表示します。
   アラート -デバイスの画面に表示するメッセージを入力したり、デバイス上で音を再生したりできます。
   ロック - デバイスをロックし、ロック解除に必要となる PIN コードを設定します。
   ワイプ - デバイス上のすべてのデータを削除します。

   重要項目
   デバイスをワイプすると、盗難対策の機能も全て機能しなくなります。

   IPアドレス表示は選択したデバイスの最後のIPアドレスを表示します。

SMS コマンドを使って盗難対策機能を使用する（SMS コントロール）

SMS コマンドを有効にすると、どのモバイルデバイスからでも SMS 経由でスマートフォンに以下のコマンドを送信できます:

- LOCATE – コマンドを送信した電話番号に、デバイスの位置情報を含むメッセージを送信します。 メッセージには、モバイルデバイスのブラウザで開くことのできる、Google マップのリンクが含まれています。
- SCREAM – デバイスのスピーカーでサウンドを大音量で再生
- LOCK – デバイスの画面を設定した PIN コードでロックします。
- WIPE – デバイス上のすべてのデータを削除

> **重要項目**
> ワイプコマンドは、事前に設定した信頼できる番号から送られた場合以外は動作しません。

- CALLME – コマンドが送信された電話番号に、スピーカーがオンの状態で電話をかけます。 これにより、あなたのデバイスを持っている人物をこっそりとチェックすることができます。
- HELP – コマンドを送信した電話番号に、利用可能なすべてのコマンドを含むメッセージを送信します。
- SIM Change – お客様がデバイスの SIM カードを交換すると、新しい番号を通知する SMS が設定した信頼できる番号に届きます。 友人の電話番号をセットアップするには、信頼できる番号 をタップし 、国コードを含めた友人の電話番号を入力するか、連絡先リストから友人のカードを選択します。

すべての SMS コマンドは以下の形式で送信する必要があります。

bd-▪ <PIN> <コマンド>▪

> **注記**
> 括弧は変数を示しており、コマンドには含めません。

たとえば、設定したセキュリティ PIN コードが ▪123456 で、デバイスの位置情報を含むメッセージを受け取りたい場合には、お客様の電話番号宛てに以下のテキストメッセージを送信します:▪

BD-123456 LOCATE

27. アプリロック

メール、写真、メッセージなどのアプリには通常、第三者によるアクセスを制限したい個人データが含まれています。

アプリロックは、アプリにセキュリティ PIN コードを設定することで第三者に起動できないようにする機能です。 PIN コードは 4 ～ 8 桁の数字で設定し、ロックしたアプリを開くたびに入力する必要があります。

もしくは、指紋認証に対応したデバイスであれば、PIN コードの代わりに指紋認証を使用することができます。

アプリロックを有効にする

選択したアプリへのアクセスを制限するには、盗難対策機能の起動後にダッシュボードに表示されるアプリロックを設定してください。

または以下の手順でアプリロックを起動することもできます:

1. ▪ Bitdefender Mobile Security を開きます。▪
2. ▪メニュー ボタンをタップして、リストから アプリロック を選択します。▪
3. オンにする をタップしてから、該当するチェックボックスにチェックを入れ、 Bitdefender による使用状況データへのアクセスを許可します。

   注記
   Android 6 でスナップフォト機能を使用するには追加の許可設定が必要です。
   有効にするには、▪アンチウイルス による写真およびビデオの撮影を許可します。▪

4. アプリに戻り、アクセスコードを設定して PIN 設定 をタップします。

   注記
   このステップは、盗難対策機能の PIN が未設定の場合にのみ表示されます。

5. スナップフォト オプションを有効にすると、お客様のデバイスの個人情報を盗み見ようとする人物を突き止めることができます。
6. 保護するアプリを選択してください。

間違った PIN または指紋が 5 回連続で入力されると、30 秒間のタイムアウトセッションが発生し、 保護されているアプリに侵入するそれ以上の試みをブロックします。

注記
同じPIN コードを窃盗対策でも使用しますので、デバイスの位置情報の確認に役立てることができます。

アプリロック

ロックモード

ここでは、アプリロック機能がデバイスにインストールされているアプリをどのようにして保護するかを選択できます。

以下のいずれかのオプションを選択できます:

- 毎回ロックする - ロックされているアプリにアクセスするには、設定した PIN コードまたは指紋を毎回使用する必要があります。
- 画面オフまでアンロック - 画面がオフになるまで、ロックされているアプリにアクセスすることができます。
- 短時間の移動を許可 - 30 秒以内であれば、アンロック状態のアプリの外に移動した後に、同じ状態でアプリに戻ることができます。
- スマートアンロックを有効にする - このオプションを有効にして信頼できるネットワークに接続すると、他の設定は利用不可になります。 つまり、ロックされたアプリに PIN コードや指紋認証なしでアクセスできるようになります。

アプリ・ロック設定

アプリロック機能の詳細な設定を行うには、「アプリロック」機能メニューの ▪ ボタンをタップし、設定 を選択します。 ▪

アプリロック ▪ 設定 では以下の設定を行うことができます: ▪

- ロック解除に3 回失敗したときにスナップフォト機能を起動します。
- 新たにインストールしたアプリのロック通知.
- PIN コードの変更

スナップショット

Bitdefender のスナップフォト機能があれば、友達や家族などの身近な人たちを含む第三者が、あなたの個人データや、あなたが使っているアプリをこっそり覗き見たりすることができなくなります。 あなたのデバイスを持っている人物をこっそりとチェックすることができます。

機能の仕組みは簡単です:アプリを保護するために設定されている PIN コードまたは指紋認証が 3 回連続で誤って入力されると、フロントカメラを使って操作者の写真を撮影します。 撮影した写真には、タイムスタンプと状況情報が記録され Bitdefender Mobile Security を開いてアプリロック機能にアクセスすることで確認できます。

注記
この機能は、フロントカメラを搭載したカメラでのみ利用できます。

スナップフォト機能の設定方法:

1. ▪ Bitdefender Mobile Security を開きます。▪
2. ▪メニュー ボタンをタップして、リストから アプリロック を選択します。▪
3. 「アプリロック」機能メニューの ▪  ボタンをタップし、設定 を選択します。▪
4. ▪アンロックが 3 回失敗したときにスナップフォト機能を起動▪ スイッチを有効にします。

間違った PIN を入力したときに撮影した写真は「アプリロック」メニューに表示され、フルスクリーンで表示することができます。

またBitdefenderアカウントでもご確認いただけます：

1. 次のサイトへアクセスします：https://central.bitdefender.com
2. Bitdefenderアカウントでログインします。
3. ウィンドウの左上隅にある  アイコンをクリックし、マイデバイス を選択します。
4. マイデバイス ウィンドウでデバイスを選択し、盗難対策 タブを選択します。

   写真が表示されます。

直近の画像3枚のみが保存されています。

かんたん解除

保護されたアプリにアクセスするたびに、アプリロック機能に PIN コードまたは指紋認証の入力を求められないようにするには、スマートアンロックを有効にしてください。

スマートアンロックでは、普段接続する Wi-Fi ネットワークが信頼できるネットワークとして設定され、保護されたアプリに対するアプリロックのブロック設定が無効になります。

スマートロック解除を有効にするには：

1. ▪ Bitdefender Mobile Security を開きます。▪
2. ▪メニュー ボタンをタップして、リストから アプリロック を選択します。▪
3. ロックモード タブを選択してから、該当するスイッチを有効にします。

接続中のワイヤレスネットワークが表示されます。

現在接続中の Wi-Fi 接続を信頼できるネットワークとして設定するには、⊕ アイコンをタップします。

注記
この設定はスマートアンロック機能が有効になっている場合にのみ利用できます。

設定を変更したい場合は、いつでも機能を無効にできます。無効にすると、信頼できるネットワークとして設定した Wi-Fi ネットワークが、信頼できないネットワークに変更されます。

28. レポート

レポート機能は、コンピュータ上のアクティビティの詳細なイベントログを記録します。

システムまたはデータのセキュリティに影響を与えるイベントが発生すると、レポートに新しいメッセージが追加されます。

レポートを確認するには：

1. ▪ Bitdefender Mobile Security を開きます。▪
2. ▪メニュー ボタンをタップして、リストから レポート を選択します。

レポートウィンドウでは以下のタブが利用可能です:

- 週次レポート - ここから、今週および前週のセキュリティステータスおよび実行タスクにアクセスできます。 今週のレポートは、毎週日曜日に生成され、レポート作成時に通知が届きます。

  毎週新しいヒントがここに表示されます。アプリを最大限に活用できるよう、ぜひ定期的にチェックしてください。

- アクティビティログ - ここでは、 Bitdefender Mobile Security アプリをお使いの Android デバイスにインストールしてからの、このアプリのアクティビティに関する詳細な情報を確認できます。

  アクティビティログを削除するには、画面の右上隅にある  アイコンをクリックし、アクティビティログをクリア を選択します。

29. WEARON

▪ Bitdefender WearON を使うと、スマートフォンをオフィスや会議室に置き忘れたときや、枕・ソファの下に入れたまま場所が分からなくなったときに、簡単に見つけることができます。 デバイスがマナーモードになっていても問題ありません。 ▪

スマートフォンの紛失を防ぐには、この機能を有効にしてください。

注記
この機能は Android 4.3 および Android Wear で動作します。

ウェアオンを有効にする

ウェアオンを使用するには、スマートウォッチを Bitdefender Mobile Security アプリに接続し、以下の音声コマンドで機能を有効にします: ▪

Start:<Where is my phone>

Bitdefender ▪ ウェアオン には 2 つのコマンドがあります: ▪

1. 電話アラート

   電話アラート機能を使うと、自分のスマートフォンから一定以上の距離を離れたときにすばやく見つけることができます。

   スマートウォッチをお持ちの場合は、デバイス上のアプリを自動的に検出し、デバイスから離れてデバイスの Bluetooth 接続が失われるとバイブレーションで通知します。

   この機能は、 ▪ Bitdefender Mobile Security を開いてメニューからグローバル設定 をタップし、WearON のセクションから該当するスイッチを選択します。 ▪

2. 警報を鳴らす

   紛失したモバイルデバイスを見つけるのは簡単です。 モバイルデバイスをどこかに置き忘れてしまったときは、スマートウォッチの「スクリーム」コマンドをタップすると、モバイルデバイス上でサウンドを大音量で再生できます。

30. 設定

設定では、次のオプションを変更することができます:

- セキュリティPINコード - アプリあるいは盗難対策コマンドのロックを解除するため設定されたPINコードを変更することができます。
- マルウェアスキャナー - ストレージをスキャンするかどうかを決めることができます。
- クラウド内検出 - クラウド検出の改善を目的にし、当社にレポートを送信するかどうかを決定できます。
- アカウントプライバシー - アカウントに関するデータ漏えいが検出される場合通知を受けるかどうかを設定できます。
- アプリロック - 新たにインストールされたアプリのロック通知を表示するかどうかを設定できます。
- スナップショット - アプリへのアクセスに 3 回失敗したときに、使用者の写真を撮影するかどうかを設定します。
- 盗難対策 - デバイスが紛失された場合に、信頼する電話番号として設定した番号を変更することができます。
- レポート - レポート通知を受信するかどうかを決定できます。
- 匿名レポートを送信する - 製品の使用しかたに関する情報を含むレポートを送信するかどうかを決定できます。 この情報は製品の改良のために重要であり、より良い製品のご提供に役立てられます。

31. この製品について

インストールしたBitdefender Mobile Securityのバージョンに関する情報をアクセスするためこの製品についてをご覧ください。 そこからサブスクリプション契約、プライバシーポリシーとオープンソースライセンスをアクセスして読むことができるし、サポートチームまでご連絡も可能です。

32. BITDEFENDER CENTRAL

Bitdefender Central は、製品のオンライン機能およびサービスにアクセスしたり、 Bitdefender がインストールされているデバイス上でリモートタスクを実行したりできるウェブプラットフォームです。 インターネットに接続しているコンピュータまたはモバイルデバイスから https://central.bitdefender.com にアクセスして Bitdefender アカウントにログインするか、Android または iOS デバイスの Bitdefender Central アプリから直接ログインすることができます。

お使いのスマートフォンに Bitdefender Central アプリをインストールするには:

- Android デバイス – Google Play で Bitdefender Central アプリを検索し、ダウンロードしてインストールします。 必要なステップを実行して、インストールを完了してください。
- iOS デバイス – App Store で Bitdefender Central アプリを検索し、ダウンロードしてインストールします。 必要なステップを実行して、インストールを完了してください。

ログインすると、以下の操作が可能になります:

- Bitdefender を Windows、macOS、iOS、および Android オペレーティングシステムにダウンロードしてインストールします。 ダウンロードできる製品は以下の通りです:
  - Bitdefender Mobile Security
  - Bitdefender Mobile Security for iOS
  - Bitdefender Antivirus for Mac
  - BitdefenderWindows製品ライン
  - Bitdefender ペアレンタルコントロール
- Bitdefender のサブスクリプションを管理・更新します。
- ネットワークに新しいデバイスを追加して、いつでもどこでも管理できます。
- 盗難防止 機能を使って、ネットワーク機器やデータを窃盗や損失から保護できます。

Bitdefender アカウントにアクセスする

Bitdefender Central にアクセスする方法は 2 通りあります:

- ウェブブラウザから:
  1. インターネットに接続しているデバイスで、ウェブブラウザを起動します。
  2. 次のサイトへアクセスします : https://central.bitdefender.com
  3. メールアドレスとパスワードを使ってアカウントにログインします。
- お使いの Android または iOS デバイスから:

  インストールした Bitdefender Central アプリを開きます。

> **注記**
> この資料では、Web インターフェイス上で見つけることのできるオプションと指示が提供されています。

マイ・デバイス

Bitdefender アカウントの マイデバイス エリアでは、管理しているデバイスにインストールされている Bitdefender 製品のインストール、管理、リモート操作などが可能です（デバイスの電源が入っていて、インターネットに接続されている必要があります)。 デバイスカードには、デバイス名、保護状態、および保護状態に影響があるセキュリティリスク （存在する場合）が表示されます。

デバイスを簡単に識別できるように、デバイス名をカスタマイズすることが可能です:

1. Bitdefender Centralにアクセスします。
2. ウィンドウの左上隅にある ☰ アイコンをクリックし、マイデバイス を選択します。
3. 目的のデバイスカードをタップし、画面の右上にある ⋮ アイコンをタップします。
4. 設定を選択します
5. デバイス名 フィールドに新しい名前を入力し、保存ボタンにクリックします。

各デバイスに所有者を作成して割り当てることで、より効率的な管理が可能です。

1. Bitdefender Centralにアクセスします。
2. ウィンドウの左上隅にある ☰ アイコンをクリックし、マイデバイス を選択します。
3. 目的のデバイスカードをタップし、画面の右上にある ⋮ アイコンをタップします。
4. プロファイルを選択します。
5. オーナーを追加 をクリックし、該当するフィールドに入力します。 プロフィールをカスタマイズするには、写真を追加し、生年月日を設定します。
6. 追加 をクリックしてプロファイルを保存します。
7. デバイスの所有者 リストから任意の所有者を選択し、割り当て をクリックします。

特定のデバイス上の Bitdefender に対してリモート操作を行ったり情報を確認したりするには、該当するデバイスカードをクリックします。

デバイスカードをクリックすると、以下のタブが利用可能になります:

- ダッシュボード. このウィンドウでは、選択したデバイスの詳細を表示したり、保護状態をチェックしたり、 Bitdefender VPNのステータスや過去7日間にブロックされた脅威の件数を確認したりできます。 保護ステータスは、製品に問題がないときには緑、対処が必要な問題があるときには黄色、デバイスが危険に晒されているときには赤で表示されます。製品に影響する問題が発生している場合は、上部のステータスエリアにあるドロップダウンの矢印をクリックして詳細を確認します。 ここで、お使いのデバイスのセキュリティに影響を与えている問題を手動で修正することができます。
- 保護. このウィンドウでは、デバイスに対してクイックスキャンをリモートから実行できます。 処理を開始するにはスキャン ボタンをクリックします。 また、デバイス上で前回スキャンが実行された日時を確認したり、重要な情報を含む最新スキャンのレポートを確認したりできます。
- 盗難対策. デバイスを紛失してしまった場合、窃盗防止機能を使ってデバイスの位置を確認し、リモートから操作することができます。 位置確認 をクリックすると、デバイスの現在位置を確認できます。 最後に把握されていた位置が、日付・時間とともに表示されます。 この機能につ

いての詳細は、 「デバイス盗難対策機能」 (p. 292)を参照してください。

サブスクリプション

Bitdefender Central 管理画面では、すべてのデバイスのサブスクリプションを簡単に管理することができます。

利用可能なサブスクリプションの確認

利用可能なサブスクリプションを確認するには:

1. Bitdefender Centralにアクセスします。
2. ウィンドウの左上隅にある ▪ ☰ アイコンをクリックし、サブスクリプション パネルを選択します。 ▪

ここでは、所有しているサブスクリプションの状態と、サブスクリプションを使用しているデバイス数を確認できます。

サブスクリプションカードを選択すると、サブスクリプションに新しいデバイスを追加したり、サブスクリプションを更新することができます。

新しいデバイスを追加する

お持ちのサブスクリプションが 1 つ以上のデバイスをカバーしている場合、 ▪ 「Bitdefender Mobile Securityをインストールしています」 (p. 276) の手順を実行することで、新しいデバイスを追加して Bitdefender Mobile Security をインストールできます。 ▪

サブスクリプションの更新

サブスクリプションの有効期限の残り期間が30日を下回っていて、サブスクリプションの自動更新を有効にしていない場合は、以下の手順に従って手動で更新することができます:

1. Bitdefender Centralにアクセスします。
2. ウィンドウの左上隅にある ▪ ☰ アイコンをクリックし、サブスクリプション パネルを選択します。 ▪
3. 該当のサブスクリプション カードを選択します。
4. 続行するには 更新 をクリックします。

Bitdefender のサブスクリプションを更新するためのページが開きます。

33. よくある質問

Bitdefender Mobile Security にはどうしてインターネット接続が必要なのですか？▪.

窃盗防止機能を使用する際に、このアプリはスキャン対象のアプリや接続したWebページのセキュリティ状態をチェックしたり、 Bitdefender アカウントからコマンドを受け取るために Bitdefender サーバと通信する必要があるためです。

▪ Bitdefender Mobile Security にはどうしてインターネット接続が必要なのですか？▪.

- インターネットアクセス –▪> クラウドとの通信に必要です。▪
- 電話の状態と識別情報の読み取り ▪– > デバイスがインターネットに接続しているかどうかの確認や、 Bitdefenderクラウドとの通信に必要なデバイス固有の ID の作成に使用します。▪
- ブラウザブックマークの読み取り・書き込み –> Web保護モジュールは、ブラウジングの履歴から悪意のあるサイトを削除します。
- ログデータの読み取り –> Bitdefender Mobile Securityは、Androidデバイスのログに脅威が動作した形跡がないかを検査します。
- SMS、連絡先、アカウントデータ、外部ストレージの読み取り・書き込み –▪> リモートワイプ機能に必要です。▪
- 場所 –▪> リモート位置の確認に必要です。▪
- カメラ –▪> スナップフォト機能に必要です。▪
- ストレージ –▪> マルウェアスキャナが SD カードをスキャンするために必要です。▪

アプリのアクティビティの詳細はどこで確認できますか？.

Bitdefender Mobile Security▪ は、すべての重要なアクション、ステータス変化、およびアクティビティに関連する重要なメッセージのログを保存します。▪ この情報にアクセスするには、▪ Bitdefender Mobile Security を開いて メニュー ボタンをタップし、リストから レポート を選択します。▪

アプリを保護するために設定した PIN コードを忘れてしまいました。 どうすればよいですか？.

1. Bitdefender Centralにアクセスします。

2. ウィンドウの左上隅にある アイコンをクリックし、マイデバイス を選択します。
3. 目的のデバイスカードをタップし、画面の右上にある アイコンをタップします。
4. 設定を選択します
5. ▪ アプリケーション PIN フィールドから PIN コードを取得します。 ▪

▪ Bitdefender Mobile Security はデバイスのパフォーマンスやバッテリーの持ちにどのような影響を与えますか？.

弊社の製品はデバイスのパフォーマンスに負荷をかけません。 アプリをインストールした後、アプリのインターフェースをブラウズしたとき、またはセキュリティチェックをしたいとう必須の場合にのみ実行されます。 Bitdefender Mobile Security▪ はあなたが友達に電話したり、メッセージを入力したり、ゲームで遊んでいる間はバックグラウンドで動作しません。

アプリロック機能をオフするには？.

アプリロック機能を「オフにする」オプションはありませんが、設定した PIN または指紋で認証した後に、選択したアプリの横にあるチェックボックスをオフにすることで機能を簡単に無効にできます。

別のワイヤレスネットワークを信頼できるネットワークとして設定するには？.

別のワイヤレスネットワークを信頼できるネットワークとして設定する場合:

1. ▪ Bitdefender Mobile Security を開きます。 ▪
2. ▪ メニュー ボタンをタップして、リストから アプリロック を選択します。 ▪
3. ロックモード タブを選択してから、 アイコンをタップします。
4. PIN コードまたは指紋認証で選択を確定します。
5. 信頼できるネットワークとして設定したいネットワークの横にある アイコンをタップします。

デバイス上で撮影したスナップフォトが表示されないようにするには？.

デバイス上で撮影したスナップフォトが表示されないようにするには:

1. Bitdefender Centralにアクセスします。
2. 画面の右上にある アイコンをタップします。
3. スライドメニューでマイ・アカウントをタップします。
4. 設定 タブを選択します。
5. デバイス上で撮影された写真を表示する/しない オプションを無効にします。

オンラインショッピングを安全にするはどうすればいいですか？.

セキュリティを軽視すると、オンラインショッピングの危険性は高まります。 詐欺の被害者になることを防ぐために以下を推奨します:

- セキュリティアプリを更新しておいてください。
- オンラインでの支払いは、バイヤー保護がある場合のみ実行しましょう。
- 公共および保護されていないワイヤレスネットワークからインターネットに接続する際には VPN を使用してください。
- オンラインアカウントに設定したパスワードにご注意ください。 大文字と小文字、数字、および記号 (@、!、%、#など) を含む強力なパスワードを設定してください。
- 情報を送信するネットワークがセキュアな接続であることを確認してください。 ウェブサイトのプロトコルは、HTTP://ではなく、HTTPS://である必要があります。

Bitdefender VPN を使うべき理由.

インターネット上のコンテンツにアクセスしたり、ダウンロードやアップロードを行うときには注意が必要です。 ウェブブラウジング時には、Bitdefender VPN を使って安全な接続を確保することをお勧めします。

- 公衆 Wi-Fi ネットワークに接続したい
- 自宅や海外など自分の現在いる場所に関係なく、特定の地域でしかアクセスできないコンテンツを利用したい
- 個人データのプライバシーを守りたい (ユーザー名、パスワード、クレジットカード情報など)
- IP アドレスを隠したい

Bitdefender VPN を使うとデバイスのバッテリーの減りが早くなりますか?

Bitdefender VPN は、お客様の個人情報を保護し、セキュリティ保護されていないワイヤレスネットワークへの接続時に IP アドレスを隠し、特定

の国の制限されたコンテンツにもアクセスできるように設計されています。デバイスのバッテリー浪費を避けるため、必要なときにだけ VPN を有効にして、オフライン時は接続を切断することをお勧めします。

Bitdefender VPN で接続すると、インターネットが遅くなるのはどうしてですか?

Bitdefender VPN は、快適なウェブブラウジングを提供できるように設計されていますが、利用しているインターネット接続の速度や、サーバーまでの距離によっては、接続速度が低下する恐れがあります。 この場合、現在位置から遠くのサーバー（たとえば米国から中国など）に接続する必要がない場合は、 Bitdefender VPN が自動的に選択する最寄りのサーバーに接続することを許可するか、あるいは現在位置に最も近いサーバーを接続することをお勧めします。

デバイスに紐付いている ▪ Bitdefender アカウントを変更できますか？.

デバイスに接続しているBitdefenderアカウントを簡単に変えるには：

1. ▪ Bitdefender Mobile Security を開きます。 ▪
2. メニューボタンをタップし、リストからアカウント情報を選択します。
3. ログアウトをタップしてお客様の選択した内容を確認します。
4. 対応するフィールドにアカウントのメールアドレスとパスワードを入力し、サインイン をタップします。

デバイス管理者とは.

デバイス管理者は、 Bitdefender Mobile Security が一部のタスクをリモートから実行するために必要なパーミッションを与える Android 機能です。 これらの権限がないとリモートロックは機能せず、またリモートワイプ機能も完全にデータを消去できません。 アプリを削除したい場合は、アンインストールを実行する前に、「設定」>「セキュリティ」>「デバイス管理者を選択」で必ずこれらの権限を無効にしてください。

信頼できる番号は何に使われますか？.

もしあなたのモバイルデバイスを手にした人物が、デバイスをあなたに返却する意思を持たない場合、すぐに SIM カードが抜き取られてしまう可能性が高くなります。 Bitdefender Mobile Security は、あなたのモバイルデバイスから SIM カードが差し替えられたことを検知すると、新しい SIM カードの電話番号が記載されたテキストメッセージがあなた宛てに自動的に送信されます。 そのため、デバイスの SIM カードが差し替えられて、電話番号が変わってしまっていても、デバイスに SMS コマンドを送信する

ことができます。 この番号にはお客様が信頼できる人の電話番号、あるいはお客様が所有する別の電話番号を指定できます。

信頼できる番号を設定後に変更することはできますか？.

別の信頼できる番号を設定するには:

1. ▪ Bitdefender Mobile Security を開きます。 ▪
2. ▪メニュー ボタンをタップして、リストから 設定 を選択します。
3. ▪盗難対策 セクションの 信頼する番号 をタップします。 ▪

   信頼できる番号の変更の前に PIN の入力を求められます。

SMS コマンドを送信するにはどのくらいの料金がかかりますか？.

SMS は通常のテキストメッセージとして送信されるため、各キャリアの所定の料金が発生する可能性があります。 Bitdefender ▪ では追加の料金は一切かかりません。 ▪

▪ Bitdefender Mobile Security. へのサインイン時に表示される「Google Token」エラーを修復する方法。 ▪.

このエラーは、デバイスが Google アカウントに紐付けられていない場合や、紐付けられたアカウントが一時的にGoogleに接続できない場合などに発生します。 以下のいずれかの解決方法をお試しください:

- Android 設定 > ▪アプリケーション > アプリケーションの管理 > Bitdefender Mobile Security を選択し、データをクリア をタップします。 次に、もう一度サインインし直してください。 ▪
- お使いのデバイスが Google アカウントに紐付けられていることを確認してください。

  これを確認するには「設定」▪>「アカウントと同期」を開き、アカウントの管理 に Google アカウントが表示されているかを確認します。 アカウントが表示されていない場合は、アカウントを追加してからデバイスを再起動し、それから Bitdefender Mobile Security にサインインしてください。 ▪
- デバイスを再起動し、サインインし直してください。

▪ Bitdefender Mobile Security はどの言語で利用できますか？ ▪.

Bitdefender Mobile Security ▪ は現在以下の言語で利用可能です: ▪

- ブラジル語
- チェコ語

- オランダ語
- 英語
- フランス語
- ドイツ語
- ギリシャ語
- ハンガリー語
- イタリア語
- 日本語
- 韓国語
- ポーランド語
- ポルトガル語
- ルーマニア語
- ロシア語
- スペイン語
- タイ語
- トルコ語
- ベトナム語

その他の言語も今後のリリースで追加される予定です。 ▪ Bitdefender Mobile Security インターフェイスの言語を変更するには、デバイスの 言語とキーボード 設定を開き、任意の表示言語を選択します。 ▪

お問い合わせ

34. サポートを依頼

Bitdefender は、速くて正確な比類のないサポートをご提供できるよう努めております。 Bitdefender 製品についての問題やご質問は、オンラインサポートセンターをご利用ください。お客様が解決方法や答えをすばやく見つけられるよう、サポートセンターにはいくつかのリソースが用意されています。 同時に、Bitdefender カスタマーケアに問い合わせることもできます。 サポート担当者がお客様のご都合のよい時間にご連絡し、ご質問にお答えします。また、必要なサポートの提供も行います。

「一般的な問題を解決する」 (p. 182)には本製品を利用中に遭遇した問題の詳細や対処法などの情報が掲載されています。

お客様の問題に対する解決策が見つからない場合は、直接お問い合わせいただくことも可能です：

- 「Bitdefender Total Security から製品サポートへ直接問い合わせる」 (p. 317)
- 「オンライン上のサポートセンターからお問い合わせください。」 (p. 318)

Bitdefender Total Security から製品サポートへ直接問い合わせる

パソコンがインターネットへ接続している場合、製品の管理画面から直接 Bitdefender のサポートへ問い合わせることができます。

次の手順に従ってください：

1. Bitdefender インターフェイスのナビゲーションメニューにある サポート をクリックします。
2. 次の選択肢があります：
   - 製品マニュアル

     データベースを確認し、必要な情報を探してください。
   - カスタマーサポート

     弊社のオンライン記事やビデオチュートリアルにアクセスできます。
   - サポート用のログを作成する

サポートに問い合わせる ボタンをクリックすると、 Bitdefender のサポートツールを起動し、カスタマーケア部門に連絡することができます。

a. フォームへ必要なデータを入力してください。

   i. 問題のタイプを選択してください

   ii. 発生した問題についての説明を入力してください。

   iii. 製品で問題が発生している場合は、問題を報告する前に、問題の再現を試みる をクリックします。 問題を再現し、「問題を再現する」フレーム内の終了をクリックします。

   iv. チケットを確定をクリックします。

b. 送信フォームに必要なデータをすべて入力してください。

   i. お名前を入力してください。

   ii. メールアドレスを入力してください。

   iii. 同意のチェックボックスを選択します。

   iv. バグパッケージを作成 をクリックします。

   Bitdefenderが製品情報を収集しています。しばらくお待ちください。 収集した製品情報は、サポート・エンジニアが問題をトラブルシューティングする際に有効な情報となります。

c. 閉じるをクリックして、ウィザードを終了します。 弊社の担当者ができるだけ早くご返事いたします。

オンライン上のサポートセンターからお問い合わせください。

Bitdefender を使って必要な情報にアクセスできない場合は、オンラインサポートセンターを参照してください:

1. http://www.bitdefender.co.jp/home-users/ を開きます。

   Bitdefender サポートセンターでは、 Bitdefender のトラブルや問題などに対する様々な解決策を提供しています。

2. 画面上部のサーチバーを使って問題に関連する記事を探すことができます。 記事を検索するには、サーチバーに検索したいキーワードを入力して検索をクリックしてください。

3. 関連する記事やドキュメントを読み、解決策を試してみる。

4. この方法で問題が解決しない場合は、

   https://www.bitdefender.com/support/contact-us.htmlにアクセスし、サポート担当者までお問い合わせください。

35. オンライン リソース

Bitdefender に関連する問題や質問を解決するのに役立つ、いくつかのオンライン上のリソースが使用可能です。

- Bitdefender サポートセンター：

  http://www.bitdefender.co.jp/home-users/

- Bitdefender サポート フォーラム：

  http://forum.bitdefender.com

- HOTforSecurity セキュリティ情報サイト：

  http://www.hotforsecurity.com

コンピュータ セキュリティ、Bitdefender 製品、会社に関する追加の情報を得るために、お気に入りの検索エンジンを使うことができます。

35.1. Bitdefender サポートセンター

Bitdefender サポートセンターには、 Bitdefender 製品に関する様々な情報が掲載されています。 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の修正履歴に加えて、脅威保護や 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サポートセンターは、誰でもアクセスし、検索することができます。 Bitdefenderのお客様に必要な技術的知識と見識をご提供しています。 Bitdefenderクライアントから送られてきたバグレポートや製品情報リクエストは、最終的にはバグ修正報告、既存の問題への回避策、ヘルプファイルへの補足情報などという形で、Bitdefenderサポートセンターに掲載されます。

Bitdefenderサポートセンターは、いつでも参照いただけます。

http://www.bitdefender.co.jp/home-users/.

35.2. Bitdefender サポート フォーラム

Bitdefender サポート フォーラムでは、 Bitdefender ユーザにサポートをご提供しています。

Bitdefender 製品がうまく動かない場合や、コンピュータから特定の脅威を駆除できない場合、動作方法に関してご質問がある場合は、問題や質問をフォーラムに投稿してください。

Bitdefenderのテクニカルサポート担当者がフォーラムを管理し、新しい書き込みがあった場合はご対応いたします。 また、他のBitdefenderユーザーからアドバイスやコメントをいただける場合もあります。

問題や質問を投稿する前に、フォーラム内の類似・関連するトピックをご確認ください。

Bitdefender サポート フォーラムは、http://forum.bitdefender.com で使用可能で、英語・ドイツ語・フランス語・スペイン語・ルーマニア語に対応しています。 ホーム & ホーム オフィス保護 リンクをクリックし、コンシューマ向け製品のセクションにアクセスしてください。

35.3. HOTforSecurity

「HOTforSecurity」には、コンピュータセキュリティに関する最新情報を掲載しています。 ここでは、パソコンがインターネットに接続している間に遭遇する可能性がある脅威（ウイルス、フィッシング、迷惑メール、サイバー犯罪など）について学習することができます。

新しい記事は、発見された最新の脅威、現在のセキュリティ傾向、コンピュータ セキュリティ産業に関する情報で、常に最新の状態になっています。

HOTforSecurityのWebページはhttp://www.hotforsecurity.comです。

36. 連絡先

効率的なコミュニケーションは成功の秘訣です。 BITDEFENDER は 2001 年より、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。 ご不明な点がありましたら、いつでもご連絡ください。

36.1. 連絡先

販売部門：sales@bitdefender.jp
カスタマーサポート：http://www.bitdefender.co.jp/home-users/
文書制作：documentation@bitdefender.com
各地の代理店：http://www.bitdefender.co.jp/become-partner/
パートナープログラム: partners@bitdefender.jp
広報: pr@bitdefender.com
人材募集: jobs@bitdefender.com
脅威報告：virus_submission@bitdefender.com
迷惑メールを報告: spam_submission@bitdefender.com
不正利用を報告: abuse@bitdefender.com
ウェブサイト：http://www.bitdefender.co.jp

36.2. 各地の代理店

Bitdefender 代理店は、その地域での営業または一般的な事柄について対応いたします。

地域の Bitdefender 代理店を見つける：

1. https://www.bitdefender.com/partners/partner-locator.html を開きます。
2. 該当するオプションを選択して国および都市を選択します。
3. あなたの国に、 Bitdefender の販売業者が見つからない場合は、お気軽に、sales@bitdefender.com までメールを送信してください。 迅速にサポートできるようにするため、当社宛のメールは英語にてお送りください。

36.3. Bitdefender 事業所

Bitdefender オフィスは、その地域での営業または一般的な事柄について対応いたします。 住所と連絡先は下記のとおりです。

U.S.A

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
電話(事務所&営業): 1-954-776-6262
営業部門： sales@bitdefender.com
技術サポート： https://www.bitdefender.com/support/consumer.html
ウェブサイト： https://www.bitdefender.com

イギリスとアイルランド

BITDEFENDER LTD
C/O Howsons Winton House, Stoke Road, Stoke on Trent
Staffordshire, United Kindon, ST4 2RW
メールアドレス： info@bitdefender.co.uk
電話番号： (+44) 2036 080 456
営業部門： sales@bitdefender.co.uk
技術サポート： https://www.bitdefender.co.uk/support/
ウェブサイト： https://www.bitdefender.co.uk

ドイツ

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
事務所： +49 2304 9 45 - 162
Fax： +49 2304 9 45 - 169
営業部門： vertrieb@bitdefender.de
技術サポート： https://www.bitdefender.de/support/consumer.html
ウェブサイト： https://www.bitdefender.de

Denmark

Bitdefender APS
Agern Alle 24, 2970 Hørsholm, Denmark
事務所： +45 7020 2282
技術サポート： http://bitdefender-antivirus.dk/
ウェブサイト： http://bitdefender-antivirus.dk/

スペイン

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax： +34 93 217 91 28
電話番号： +34 902 19 07 65
営業部門： comercial@bitdefender.es
技術サポート： https://www.bitdefender.es/support/consumer.html
ウェブサイト： https://www.bitdefender.es

ルーマニア

BITDEFENDER SRL
Orhideea Towers, 15A Orhideelor Street, Sector 6
Bucharest
Fax： +40 21 2641799
販売部門連絡先： +40 21 2063470
販売部門宛メールアドレス： sales@bitdefender.ro
技術サポート： https://www.bitdefender.ro/support/consumer.html
ウェブサイト： https://www.bitdefender.ro

アラブ首長国連邦

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
販売部門連絡先： 00971-4-4588935 / 00971-4-4589186
販売部門宛メールアドレス： mena-sales@bitdefender.com
技術サポート： https://www.bitdefender.com/support/consumer.html
ウェブサイト： https://www.bitdefender.com

用語集

ActiveX
: ActiveXは、プログラムやOSがサーバー上から他のアプリケーションを呼び出すことを可能にする技術です。 ActiveX技術はMicrosoft Internet Explorerで、静的なwebページをユーザーの操作などにあわせて動的に見せるために使用されています。 ActiveXを利用すれば、ユーザーはwebページで質問をしたり、質問に対する返答を受け取ったり、ボタンを押したり、様々な方法でページとインタラクティブにやり取りすることができます。 多くのActiveXコントロールは、Visual Basicでプログラミングされています。

  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。

Botnet
: 「ボットネット」は、「ロボット」と「ネットワーク」をつなげた造語です。 ボットネットとは、インターネットに接続している脅威感染デバイスを意味し、スパムメールの送信、データの窃盗難、脆弱なデバイスのリモート制御、スパイウェア、およびランサムウェアなどの脅威の拡散に使用できます。 マルウェアの目的は、大企業内の PC、サーバー、モバイルデバイス、および IoT デバイスなど、できるだけ多くのデバイスに感染することです。

Cookie（クッキー）
: クッキーはユーザーの趣向やブラウジング動向などの情報を保存した小さなファイルです。 クッキーは特にユーザーの趣向にあわせた公告などを表示させるために利用されます。 良い点としては、ユーザーの趣向にあった広告が表示されるので、全く興味のない公告が延々と表示されることがなくなります。 悪い点としては、ユーザーの個人情報は収集されないとは言え、ユーザーがどこに行って何をクリックしたかなどの情報は収集されるので、動向をトラッキングされることに対して気にされるユーザーもいます。 このようにプライバシー観点から考えても、クッキーの使用を問題視される方もいます。 これは極端と考えることもできますが、場合によっては正しいともいえます。

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
: Webページ上でのみ動作するように作られた、Javaのプログラム。 Webページでアプレットを使用するには、アプレットに名前とサイズ（縦横をピクセル単位で）を指定する必要があります。 Webページがアクセスされると、ブラウザがアプレットをサーバーからダウンロードし、ユーザーのパソコン（クライアント）上で実行します。 アプレットは、通常のアプリケーションと違って、厳しいセキュリティプロトコルによって制御されています。

  例えば、アプレットはクライアント上で実行されるにも関わらず、クライアントパソコンへデータを書き込んだり、読み出すことはできません。 さらにアプレットには提供元と同じドメインからしかデータを読み書きすることができないという制限が加えられています。

Photon
: Photon は、セキュリティソリューションによるパフォーマンスの低下を最小化するために設計された Bitdefender 独自の革新的なテクノロジーです。 PC のアクティビティを バックグラウンドで監視し、起動およびスキャン処理を最適化するために役立つ使用パターンを作成します。

TCP/IP
: Transmission Control Protocol/Internet Protocol - インターネットで広く使用される、ネットワーク接続された異なるハードウェアや異なるOS上の通信を可能にするネットワークプロトコル。 TCP/IPにはパソコン通信の基準や、トラフィックルーティング、ネットワーク接続の慣例などが含まれています。

アップデート
: 古いバージョンのソフトウェアまたはハードウェアを置き換えるように作成された、新しいソフトウェアまたはハードウェア。 また、アップデートのインストールルーチンとしては、古いバージョンの製品がインストールされているかを確認するようになっています。古いバージョンがなければ、アップデートはインストールできません。

Bitdefender は手動でアップデートを確認する以外に、製品を自動でアップデートできる独自のアップデート機能を持っています。

アドウェア
アドウェアは大抵、ホストとなるアプリケーションと一緒に提供され、アプリケーションを無料提供するのと引き換えに、ユーザーにアドウェアのインストールに同意を求めます。 大抵のアドウェアは、ユーザーが（アプリケーションの目的を明記した）使用許諾書に同意した後にインストールされるため、法には触れていません。

ただしポップアップの公告が頻繁に表示されると、ユーザーにとっては目障りなだけではなく、システムのパフォーマンス低下の原因になる場合もあります。 また使用許諾書をしっかり確認せずにインストールしてしまった場合、アプリケーションが収集する情報に対してプライバシー的な懸念を感じるかもしれませんので、注意が必要です。

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。

1つ以上のファイルを圧縮した状態で含んだ圧縮ファイル。

イベント
プログラムによって検出される動作。 イベントはマウスクリックや、キーを押したなどのようなユーザーアクションの場合もあれば、メモリ不足などのようなシステムで発生した出来事の場合もあります。

キーロガー
キーロガーとは、キーボードで入力されたキーを記録するプログラムです。

キーロガー自体は悪質なものではありません。 社員やお子様のパソコン操作を監視したり、正当な目的のために使用される場合もあります。ただし、最近はキーロガーを悪質な行為（パスワードやログインID、個人情報の収集など）のために使用するサイバー犯罪が増えてきています。

コマンドライン
コマンド ライン インタフェースでは、ユーザは画面上に直接コマンドを入力します。

サブスクリプション
ユーザーに、所定の数のデバイス上で特定の製品またはサービスを、所定の期間利用する権利を付与する購入契約。 有効期限が切れたサブスクリプションは、初回購入時にユーザーが入力した決済情報を使って自動的に更新できます。

システムトレイ
Windows 95から採用されたタスクトレイ（画面右下のPC時計の隣）には、プリンタ、モデム、音量など、あらゆるシステム関連のタスクを実行するためのアイコンが表示されています。 アイコンをダブルクリック、または右クリックして、各コントロールの詳細を表示します。

シリアル番号
これはショップなどで購入し、特定の製品またはサービスのライセンスを有効化するために使用する一意のキーです。 アクティベーションコードは、サブスクリプションを所定の期間および所定のデバイス数に対して有効にします。また、同一の製品またはサービスのサブスクリプションを延長する目的にも使用されます。

スクリプト
マクロやバッチファイルの別名です。スクリプトはコマンドを列記したもので、ユーザの操作なしに実行されます。

スタートアップ項目
このフォルダに配置されたファイルはパソコンの起動時に実行されます。 例えばパソコン起動時の起動音や、スタートアップ画面や、リマインダーカレンダー、アプリなどがスタートアップ項目となります。通常はファイルそのものではなく、ファイルのエイリアスがフォルダ内に配置されます。

スパイウェア
ユーザーのインターネット接続からこっそりとユーザー情報を抜き出し、公告目的に利用するソフトウェア。 スパイウェアの多くは、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・アプリケーションの隠れコンポーネントとして同梱されてきます。 インストールされると、スパイウェアはユーザーのインターネット上の動作などを監視し、収集した情報をユーザーへ知られないように裏で送信します。 スパイウェアはメールアドレス、パスワード、クレジットカード番号のような機密情報を収集することもあります。

スパイウェアがトロイの木馬の脅威に似ている点は、ユーザーが別のアプリをインストールしようとした際に無意識にスパイウェアもインストールしてしまうところです。 よくあるスパイウェアにかかる方法は、ピア・ツー・ピアのファイル交換で製品をダウンロードすることです。

道徳に反することや、プライバシーの侵害である点以外にスパイウェアはパソコンのメモリを勝手に消費し、収集した情報を送信するためにネットワーク帯域幅を無断で利用するため、あらゆる面でユーザーへ危害を加えます。 スパイウェアによってメモリやシステムのリソースが圧迫され、他のアプリケーションがクラッシュしたり、システムが不安定になってしまうこともあります。

スパム
ジャンクEメールや、ニュースグループの迷惑メールなど。 未承諾の不要メール（迷惑メール）とも呼べます。

ターゲット型攻撃
ターゲット型攻撃 (APT) は、システムの脆弱性を悪用して重要な情報を盗み出し、攻撃者に送信します。 この脅威は企業、政府機関を含めた大規模な組織をターゲットにしています。

ターゲット型攻撃はシステム内に潜み、ターゲットのコンピュータに損害を与えることなく、長期間にわたって情報を盗み出し続けます。 脅威をネットワークに拡散する方法としては、ユーザーが安心して実行してしまいやすい PDF ファイルや Office ドキュメントを悪用する方法がポピュラーです。

ダウンロード
ソース元からデータ（大抵の場合はファイルを丸ごと）をコピーして、周辺機器デバイスにコピーすること。 大抵の場合、ファイルをオンライン上のサービスからパソコンへコピーする行為を表すために使用される単語です。 ダウンロードとは、ネットワークファイルサーバーからネットワーク上のパソコンにファイルをコピーすることに対しても使用できます。

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。

トロイの木馬
安全なアプリケーションとしてみせかける、破壊的なプログラム。 トロイの木馬は悪意のあるソフトウェアプログラムやワームのように自己増殖しませんが、もたらす被害は同様に深刻です。 最も油断のできないトロイの木馬は、コンピュータの脅威を駆除すると称しておきながら、実際にはコンピュータに脅威を移植する種類のものです。

名前の由来は、古代ギリシャ人が敵のトロイ人に和解の贈り物として、巨大な木馬を贈ったという、ホメロスの有名な作品『イリアス』から来ています。 この巨大な木馬の中にはギリシャ兵が潜んでいて、トロイ人がこれを知らずに町へと運び込むと、夜になってギリシャ人が中から出てきてトロイアの町を滅ぼされてしまうという作品です。

ハニーポット
ハッカーの行動を把握し、彼らがシステムからデータを盗み出す方法を特定することを目的に作られた、おとりのコンピュータシステム。 企業や各機関は、組織全体のセキュリティを向上するために、ハニーポットを導入・活用することにさらに意欲的です。

バックドア
制作者あるいは管理者によって意図的に用意された、システムのセキュリティホール（弱点）。 これらのセキュリティホールは決して全てが悪意あって残されたものではなく、OSによってはデフォルトの状態でフィールド・サービステクニシャンがメンテナンス時に使用できる特有の権利が与えられたアカウントが用意されている場合もあります。

パス
パソコン内のファイルへの正確な位置情報。 この位置情報はトップダウンの階層型ファイリングシステムで表されます。

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。

パックされたプログラム
圧縮された状態のファイル。 多くのOSやアプリケーションにはファイルをパッキング（圧縮）させるコマンドがあります。 例えば、あるテキストファイルに空白スペースが連続で10回使用されていたとします。通常でしたらこれは10バイトのストレージを必要とします。

ただしファイルを圧縮するプログラムは、この空白スペースを特殊な文字と入れ替え、繰り返される回数を数字として記録します。 この方法だと、10個の空白スペースでも2バイトの容量しか使用しません。 これは数多くあるパッキング（圧縮）のテクニックのほんの一つです。

ヒューリスティック
新しい脅威を識別するために使用される方式。 このスキャン方式は、特定の脅威情報データベースに依存しません。 ヒューリスティック・スキャンの利点は、既存脅威の新しい亜種が現れたとしても、検知できることです。 ただし、時には正常のプログラム内のコードを疑わしいとして「誤検知」してしまう場合もあります。

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やMS-DOSなど、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用します。 拡張子の長さは大抵1文字～3文字です（古いOSの場合は3文字以上に対応していないこともあります）。 例としましては、C言語のソースコードに使用される"c"、PostScriptに使用される"ps"、テキストに使用される"txt"などがあります。

フィッシング
ユーザーの個人情報を盗み出すことを目的として、正当な企業を装ってメールを送りつける行為。 このメールからユーザーをwebページへ誘導し、「登録済みの情報を最新の状態に更新してください」というような理由でパスワード、クレジットカード番号、保険証番号などの個人情報の入力を求めます。 ただし、webサイトは正規なサイトではなく、ユーザーの個人情報を盗み出す目的で作られた偽サイトです。

ブラウザ
Web ブラウザの略。Webページを表示するためのソフトウェアアプリケーション。 一般的に有名なブラウザはMicrosoft Internet Explorer、Mozilla Firefox、Google Chromeなどです。 これらはすべてグラフィカル・ブラウザであり、テキスト以外にもグラフィック（画像）も表示することができます。 これに加え、最近のブラウザは音声や動画など様々なマルチメディアに対応していますが、場合によっては再生にはプラグインが必要な場合があります。

ブートウイルス
フロッピーディスクなどのブートセクタに感染する脅威。 ブートセクタ・ウイルスに感染したディスクから起動してしまうと、脅威がメモリ内へ侵入してしまいます。 それ以降、システムを起動する度に、メモリに脅威が潜んだ状態でシステムが起動します。

ポート
デバイスを接続するためのパソコンのインターフェイス。 パソコンには様々な種類のポートがあります。 内部的にはディスクドライブや、キーボードや、ディスプレイ画面を接続するためのポートがあります。外部的にはモデムやプリンタ、マウスなど、その他の周辺機器を接続するためのポートがあります。

TCP/IPやUDPネットワークでは論理的接続のエンドポイントを指します。ポート番号はポートの種類を表します。 例えばポート80はHTTP通信に使用されます。

マクロウイルス
文書ファイル内にマクロとして埋め込まれたコンピュータ脅威。Microsoft WordやExcelなど、多くのアプリケーションには操作を省略するマクロ機能が搭載されています。

これらのアプリケーションでは、文書にマクロを埋め込み、文書ファイルを開くたびにマクロを実行させることができます。

メモリ
パソコンの内部ストレージエリア。 メモリという単語はチップなどの形を取るデータストレージを指し、ストレージという単語はテープやディスク上にあるメモリのことを指します。 どんなパソコンにも物理メモリは存在します。この物理メモリは「メインメモリ」や「RAM」と呼ばれることもあります。

メールアドレス
Eメール ローカルやグローバルのネットワークを介してメッセージを送信するサービス。

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

ランサムウェア
ランサムウェアは、ユーザーのシステムに勝手にロックをかけて人質にとり、ユーザーに身代金として金銭を要求する悪質なプログラムです。CryptoLocker、CryptoWall、TeslaWall などは、システムから個人情報を盗み取ろうとするマルウェアのごく一部です。

感染は、スパムメール、添付ファイルのダウンロード、感染したウェブサイトの訪問、悪意のあるソフトウェアのインストールなどによって引き起こされます。通常、ユーザーはシステムが感染したことに直ちに気付くことはありません。 個人ユーザーおよび企業は、ランサムウェアを悪用するハッカーに常に狙われています。

ルートキット
ルートキットとは、システムへの管理者レベルアクセスを与えるソフトウェアツールです。 ルートキットという単語が最初に使われたのはUNIX系のOSで、こちらは攻撃者に管理者権限を与え、システム管理者から自身を隠蔽させることを可能にする、再コンパイルされたツールのことを指しました。

ルートキットの主な役割りはプロセスやファイル、ログイン情報や履歴などを隠蔽させることです。 また、必要なアプリケーションを導入すれば、端末やネットワーク接続、周辺機器などからデータをインターセプトすることも可能となってしまいます。

ルートキット自体は悪意あるものではありません。 実際にシステムやアプリケーションなどでも重要ファイルをルートキットを使用して隠す場合があります。 ただし、大抵の場合は脅威を隠すためや、攻撃者の侵入を隠すために使用されています。 このため脅威と併用されると、ルートキットはシステムのセキュリティと整合性に対する大きな脅威となります。 通信を監視したり、システムへのバックドアを作ったり、検知を免れるためにファイルや履歴を改ざんすることもできてしまいます。

レポートファイル
実行されたアクションの一覧が記録されたファイル。 Bitdefenderは、検査したパスやフォルダ、検査したアーカイブの数、検出した感染ファイルの数をレポートファイルで管理します。

ワーム
ネットワーク上で増殖し、感染させながら自身を増殖するプログラム。他のプログラムへ寄生することはありません。

仮想プライベートネットワーク（VPN）
: あまり安全でないネットワークを暗号化し、一時的に安全に直接接続できるようにするテクノロジーです。 これによりデータは暗号化後に送受信されるため、第三者に傍受される可能性が低くなります。 セキュリティには、ユーザー名とパスワードによる認証が使われます。

多形性ウイルス
: ファイルを感染するごとに形を変える脅威。 バイナリパターンが変化するため、このような脅威は検知が難しいです。

脅威
: ユーザーの意思に反し、知らない間にパソコンに読み込まれるプログラムやコード。 多くの脅威は自己増殖することができます。 全てのコンピュータ脅威は人の手によって作られたものです。 自身をコピーし続けて増殖する脅威は、知識ある人には簡単に作成できてしまいます。 そんな簡単な脅威であっても、増殖し続けるとパソコンのメモリを圧迫し、システムが利用できない状態に陥らせることができてしまいます。 また更に危険な脅威はネットワークを介して自身を増殖させ、セキュリティをバイパスできる種類の脅威です。

脅威情報アップデート
: セキュリティソリューションがウイルスを検出して除去するために使う、脅威のバイナリパターンです。

誤検知
: 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。

起動セクタ
: ディスクのアーキテクチャ（セクタサイズ、クラスタサイズなど）を定義する第一セクタ。 スタートアップディスクなどの場合、ブートセクタにはオペレーティングシステムを起動するプログラムが含まれます。

非ヒューリスティック
: このスキャン方式は、特定の脅威情報データベースに依存します。 非ヒューリスティックなスキャンの利点は、脅威の挙動などに騙されて正常なファイルを誤検知てしまわないことです。