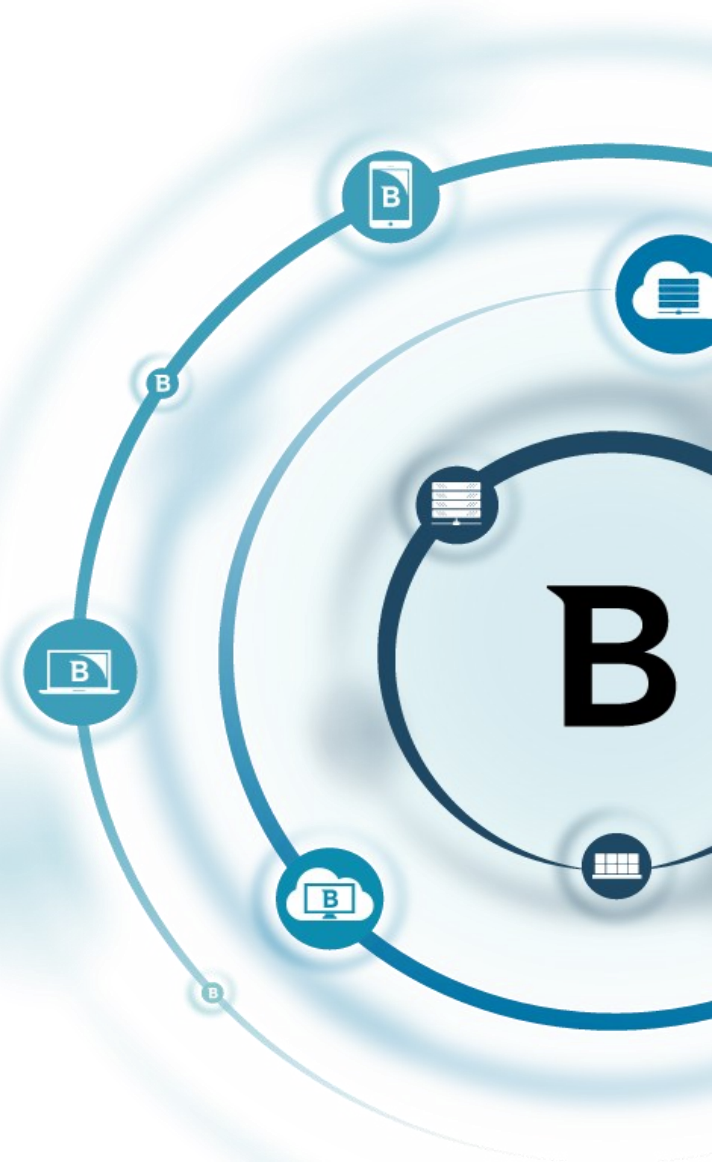
1 グローバル防御ネットワーク アーキテクチャ コンソール エージェント

Bitdefender GravityZone

一つのコンソールでWindows、Linux、Mac、スマホら全てを管理保護する

簡易インストールガイド

無料試用アカウントをご利用の方へ



Bitdefender

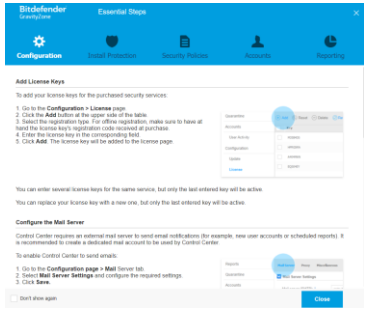
株式会社サンブリッジセキュアウェイク secureawake

① 管理コンソールにログイン後、インストールパッケージの作成へ

マシンにインストールするエージェントを用意します。

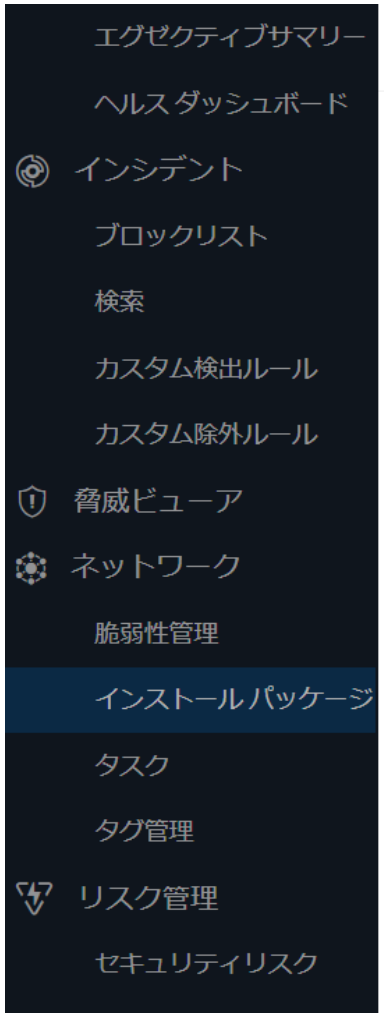
弊社でアカウントを作成が完了すると、Bitdefenderシステムより自動で、登録されたアドレスにログイン方法を記した**メールが送信**されます。

ブラウザからメールに書かれているログイン情報で、**管理コンソールにアクセス**してください。



ログイン後に左のようなダイアログが表示されます。ここのショートカットを利用してすぐに始められますが、今回はあえて×をクリックして閉じて、今後の運用時にも応用が利く通常の手順を紹介します。

ログイン後、以下のリンクをクリック、 作成 して作成画面に入ります。
左メニュー ＞ ネットワーク ＞ インストールパッケージ

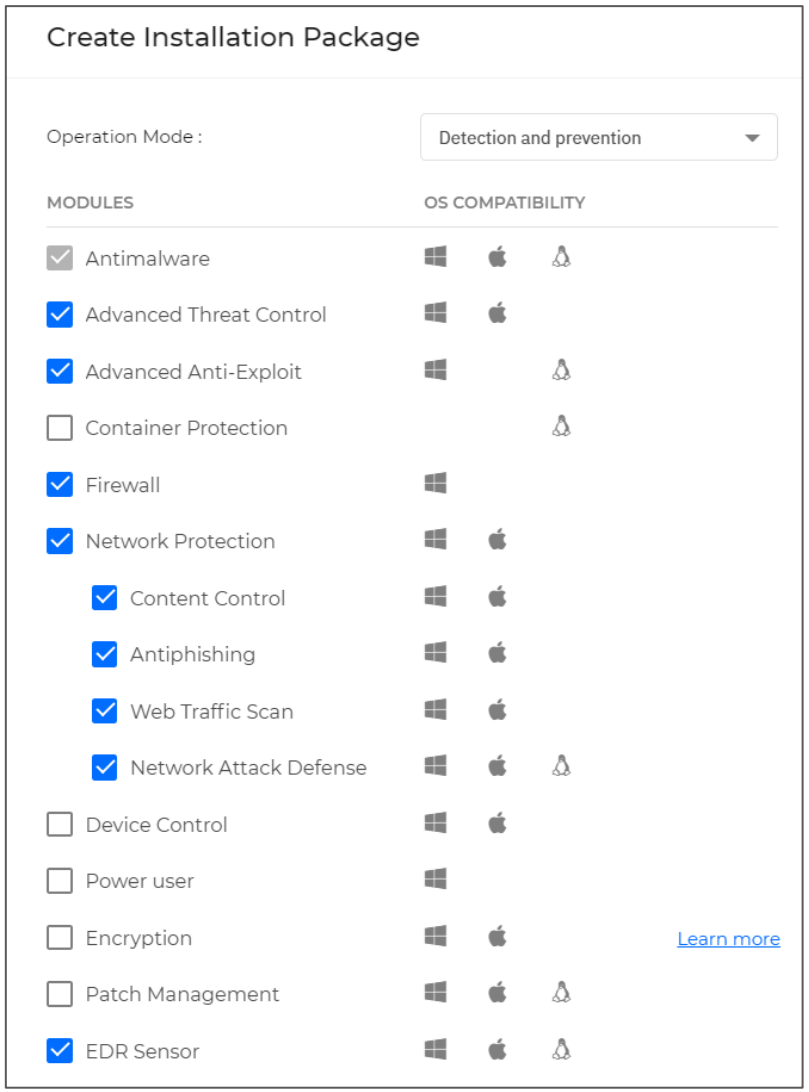


画面は日本語選択時

最初の導入としては右のようなモジュール選択がよいでしょう。これにより基本的な防御機能がインストールされます。

② モジュールの選択について

インストール時点でマシンに実装したい防御能力は選択してパッケージに含めます。



画面は英語選択時

なおモジュールは導入後に任意のタイミングで追加や削除ができます。またOS制限で利用できないモジュールは、そのOSのマシンではインストールされません。

プロキシーがあるネットワークへ導入される場合

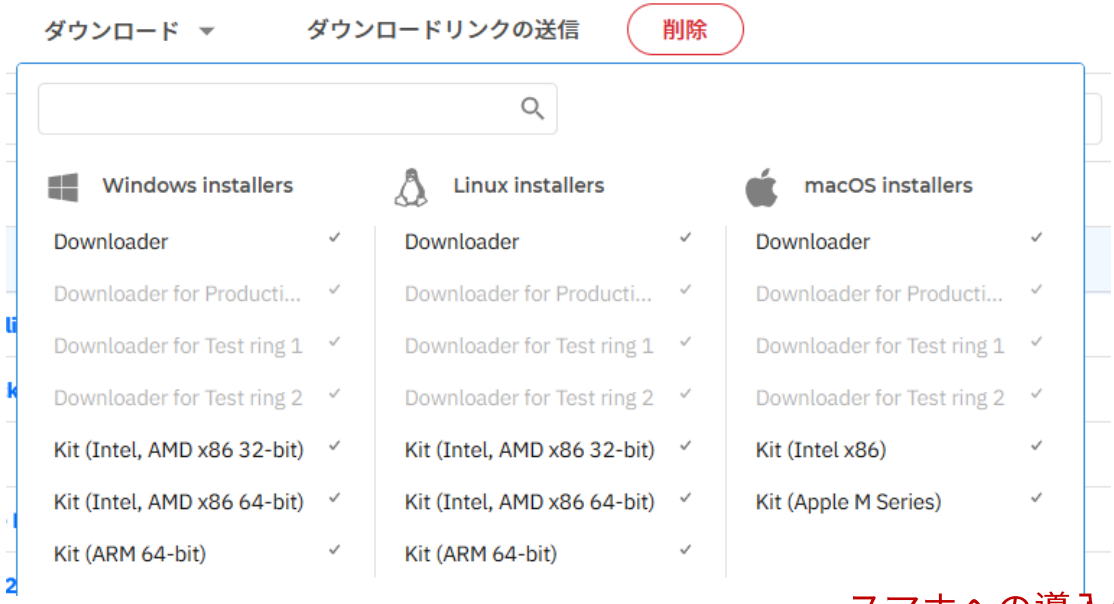
社内ネットワークでプロキシーが設定されている場合には、このパッケージ作成時に合わせて、管理者から案内されている認証情報を入力して SAVE してください。
これがないとインストール後、アップデート等を受け取ることができません。

③ パッケージの配布方法は２つ

管理者がダウンロードしてから配布　or　URLから直接ダウンロードする

管理者がいったんインストーラーを手元にダウンロードして、それを社内共有サービスを利用して配布する方法では、ダウンロードを選択してOSごとに「Kit」を取得します。

Kitは予め本体をダウンロードするためファイルサイズは大きくなりますが、各マシンでのインストール時間は最小となります。



直接ダウンロードさせる方法では、**ダウンロードリンクの送信**を選択してください。Linuxでwgetコマンドでこのurlを渡すことで、直接ダウンロードできます。

Downloaderは、ユーザPCで本体をダウンロードしながらインストールする形式です。各マシンで毎回ダウンロードする時間がかかります。

スマホへの導入は別の専用の方法となります

④最初の導入・動作検証

インストールが成功して最初の同期が完了すると、管理コンソール上にそのマシンがアイコンで表示されます。

作成したパッケージは、まず導入予定のPCを代表する構成を持つPC、同じ業務処理を行う代表的なPCにインストールしてください。
複数のOS、環境への導入予定がある場合には、それぞれで１台でまず実施してください。そして動作確認後、他PCへ展開してください。

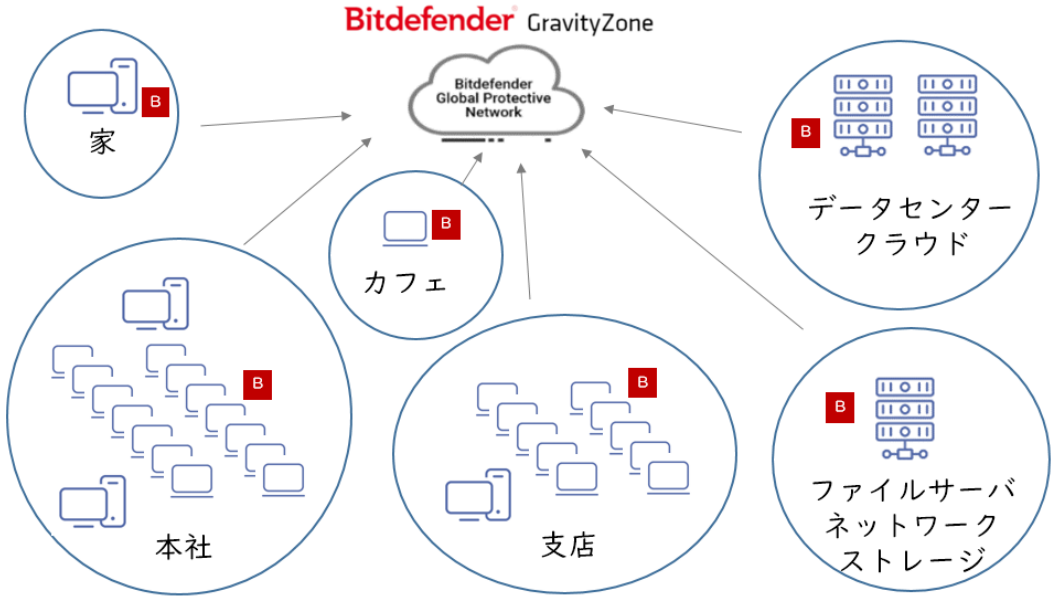
インストール方法　https://secureawake.com/BitDefender-GravityZone.html#eval

WindowsおよびMac:

パッケージはインストーラー形式になっていますのでそのまま実行、
またはアーカイブ形式になっている場合には解凍して実行し、
あとは画面に従ってください。

Linux:

マシンで直接パッケージをダウンロードする場合は以下全てroot権限で、
#wget [前ページのInstallation LinkのURL]
tarファイルを解凍後、実行権限を与えて実行してください。
chmod +x installer
./installer



⑤ デフォルトポリシー作成のおすすめ

社内のセキュリティレベルの標準化を実現

ポリシーとは、各マシンにインストールされたBitdefenderの動きを規定するためのルールです。パッケージで選択されてインストールされたモジュール毎に設定します。

例えばアンチマルウェアの設定で、検出強度をアグレッシブにしたり、定期的にマシンをスキャンさせるなどの設定を行います。

このポリシー、ぜひおすすめしたいのが御社専用のポリシーを作成することです。これにより各マシンでバラバラだった社内マシンのセキュリティレベルを一定のものに保つことができます。

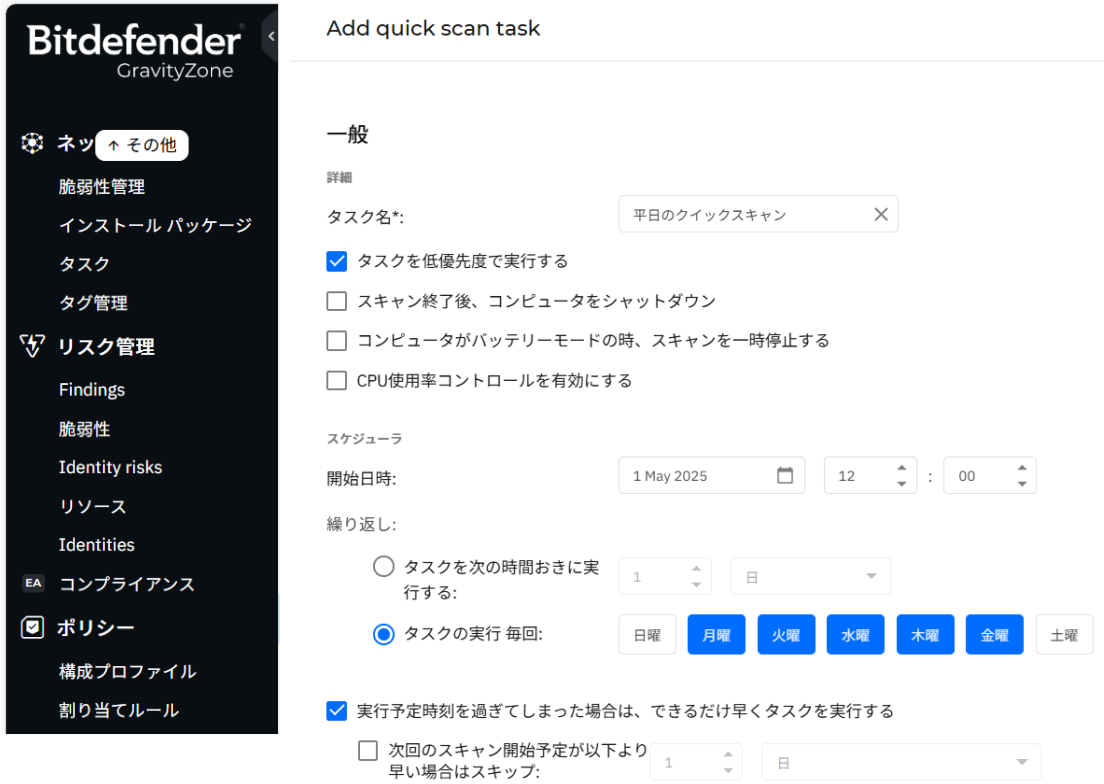
左メニューポリシーを選択して、追加（Add）をクリックして新規ポリシーを作成します。すでに推奨設定がされていますので、そのままSAVEで保存してください。

次に、作成したポリシーにチェックを入れた状態で、デフォルトに設定（Set as default）します。これ以後導入されるマシンに対してはこのポリシーが自動で適用されます。

また、例えば開発部隊用には一部セキュリティ設定を変えたい場合は、このデフォルトポリシーを複製（Clone）してから、その部分だけを変更して別名で保存。マシンに対して適用してください。

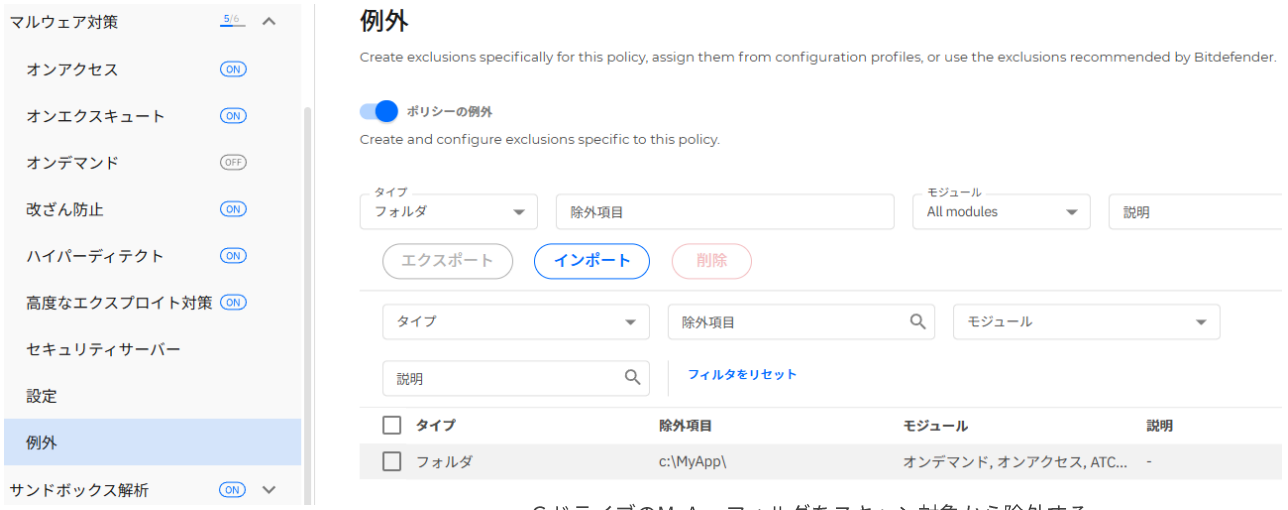
⑤’ ポリシー例

平日は毎日スキャンを実施したい



クイックスキャンと呼ばれるシステムやメモリのみを対象とした
高速スキャンを行われている業務に影響を与えないようにします。

開発中のアプリ・システムはスキャンから除外したい



CドライブのMyAppフォルダをスキャン対象から除外する

それでもインポートしている外部ライブラリから、脅威が入りこむ
可能性があるため、定期的なスキャンは推奨されます。

⑥ 評価ライセンスから正規ライセンスへの移行

ご注文後こちらで購入された正規ライセンスへ切り替えます。

社内PCへの展開、動作確認が済みましたら、お見積りを sales@secureawake.comまでご依頼ください。折返しお見積り金額をお伝えいたします。

返信にてご注文指示をいたたげましたら、弊社で手続きを開始します。発行されたライセンスをお客様アカウントに登録、同期がされたことを確認したのちに、請求書PDFを送る流れとなります。
https://blog.secureawake.com/2021/04/transaction.html

ライセンス内容は管理コンソール内のMy Company ページにて確認できます。本番運用開始後に、マシン数の追加や上位エディションへのアップグーレードが可能です。