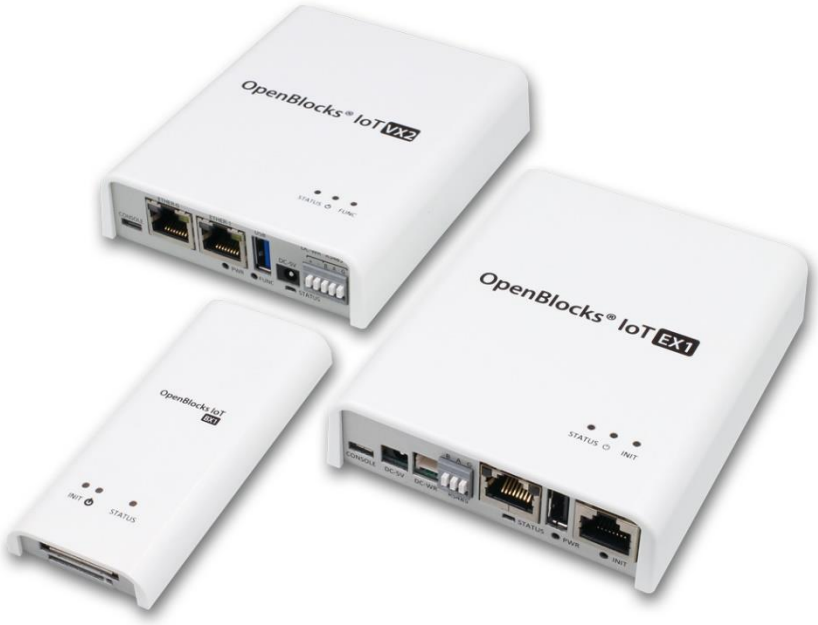
Plat' Home
TECHNOLOGY to serve you.

OpenBlocks IoT Family向け
セキュリティガイド



Ver.3.3.0

ぷらっとホーム株式会社

■ 商標について

- Linux は、Linus Torvalds 氏の米国およびその他の国における商標あるいは登録商標です。
- 文中の社名、商品名等は各社の商標または登録商標である場合があります。
- その他記載されている製品名などの固有名詞は、各社の商標または登録商標です。

■ 使用にあたって

- 本書の内容の一部または全部を、無断で転載することはご遠慮ください。
- 本書の内容は予告なしに変更することがあります。
- 本書の内容については正確を期するように努めていますが、記載の誤りなどにご指摘がございましたら弊社サポート窓口へご連絡ください。
  また、弊社公開の WEB サイトにより本書の最新版をダウンロードすることが可能です。
- 本装置の使用にあたっては、生命に関わる危険性のある分野での利用を前提とされていないことを予めご了承ください。
- その他、本装置の運用結果における損害や逸失利益の請求につきましては、上記にかかわらずいかなる責任も負いかねますので予めご了承ください。

目次

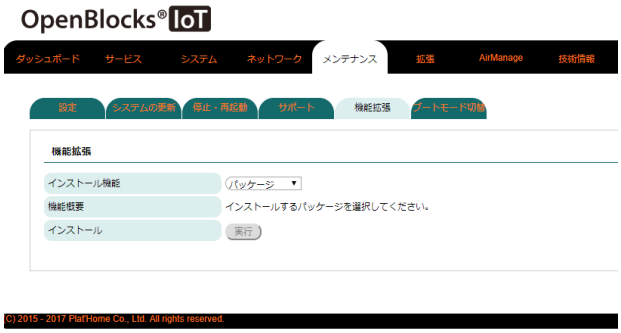
第 1 章 はじめに

本書は、OpenBlocks IoT Family に搭載可能な WEB UI 込みでの一部不正アクセス対応のセキュリティ設定の使用方法を解説しています。

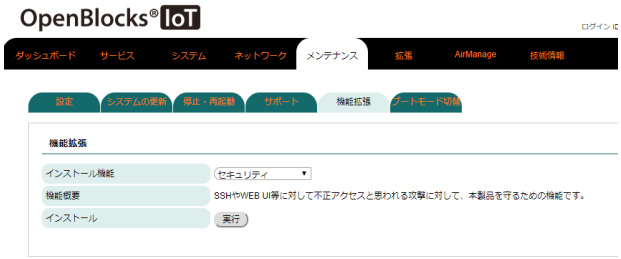
第 2 章 セキュリティ設定

2-1. セキュリティ機能のインストール

本製品出荷時では、セキュリティ設定 WEB UI はインストールされておりません。そのため、WEB UI の「メンテナンス」→「機能拡張」タブからセキュリティ設定用 WEB UI のインストールを行います。



WEB UI の「メンテナンス」タブを選び、さらに「機能拡張」タブをクリックすると機能拡張用のパッケージを選択することができます。

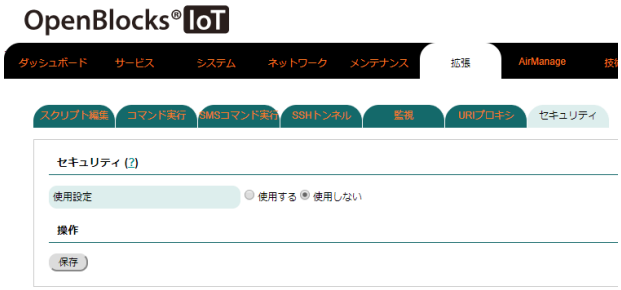


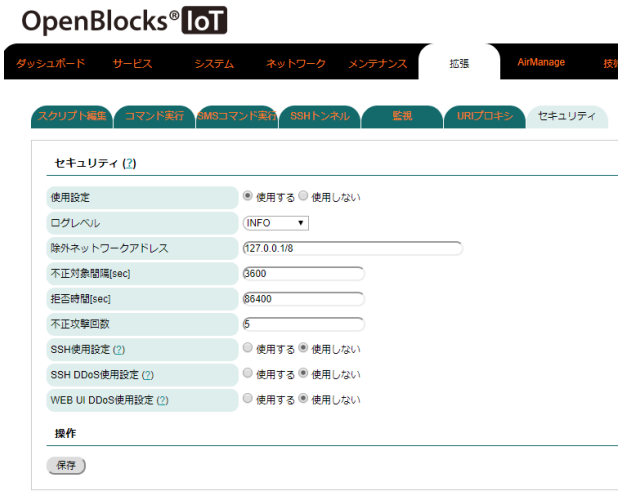
インストール機能のリストから「セキュリティ」を選択します。
その後、インストールの「実行」ボタンを押し、インストールを行ってください。

尚、インストール完了後には反映を行うため、本体再起動が必要となります。そのため、「メンテナンス」→「停止・再起動」から本製品の再起動を行ってください。

2-2. セキュリティ使用設定について

セキュリティ機能のインストールが完了している場合、サービス WEB UI の「拡張」→「セキュリティ」タブにセキュリティの設定項目が表示されます。
使用設定を「使用する」に設定し、適用するセキュリティ使用を「使用する」にし保存することで対象のセキュリティ機能が適用されます。
尚、本機能は起点の初回不正攻撃から、一定時間の間に指定不正攻撃回数(初回含む)分の不正攻撃があった場合、対象 IP アドレスの対象サービスへのアクセスを拒否します。





セキュリティ

使用設定：

セキュリティ機能の使用設定を行います。セキュリティ機能を使用する場合には、「使用する」を選択してください。

ログレベル：

出力するログレベルを以下から選択します。

・INFO
・CRITICAL
・ERROR
・WARNING
・NOTICE
・DEBUG

尚、基本的には「INFO」から変更す必要はありません。

除外ネットワークアドレス：

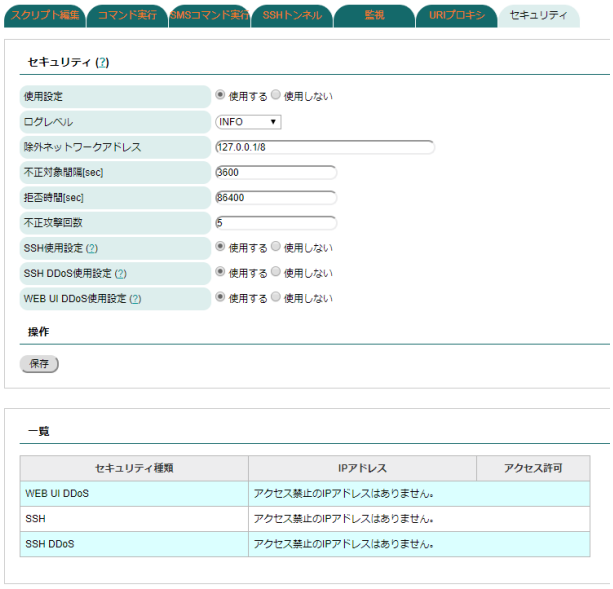
セキュリティ機能から除外するネットワークアドレスを指定します。尚、複数指定する場合には、空白にて追加してください。

Ex.）192.168.254.0 のネットワークを追加する場合

“127.0.0.1/8 192.168.254.0/24”

不正対象間隔[sec]：

対象 IP アドレスから対象サービスへの不正攻撃が開始された際に、同様の不正攻撃としてグループ化する時間を指定します。



拒否時間[sec]：

対象 IP アドレスから対象サービスへのアクセスを拒否する時間を指定します。

不正攻撃回数：

不正対象間隔内に不正攻撃が一定回数来た場合、アクセス拒否と判定する際の回数を指定します。

SSH 使用設定：

SSH のログイン失敗によるセキュリティ機能の使用設定を行います。

使用する場合には、「使用する」を選択して下さい。

SSH DDoS 使用設定：

SSH への DDoS 攻撃によるセキュリティ機能の使用設定を行います。

使用する場合には、「使用する」を選択して下さい。

WEB UI DDoS 使用設定：

WEB UI 使用ポートでの HTTP/HTTPS アクセスにおける、403/404 アクセス攻撃によるセキュリティ機能の使用設定を行います。

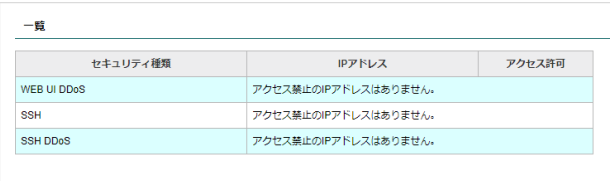
使用する場合には、「使用する」を選択して下さい。

各使用設定を「使用する」に保存した場合、セキュリティ機能が有効となります。

2-3. 不正攻撃のアクセス拒否解除

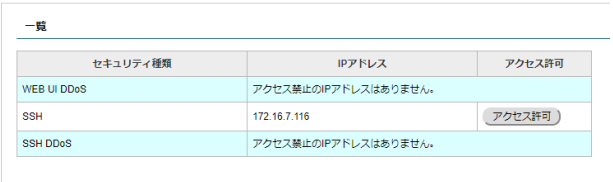
セキュリティ機能を有効とした場合、「拡張」→「セキュリティ」タブのページ下部に有効となっているセキュリティ一覧が表示されます。
また、アクセス拒否となっている IP アドレス/対象サービスの組み合わせが表示されます。

※アクセス拒否が存在しない場合



不正攻撃等が無く、正常に稼働している場合には左図のようにアクセス拒否となっている IP アドレスは表示されません。

※SSH にアクセス拒否が存在する場合



不正攻撃が行われ、アクセス拒否となっている IP アドレスが存在する場合、左図のように IP アドレス及び「アクセス許可」ボタンが表示されます。

尚、「アクセス許可」ボタンは対象 IP アドレスから対象サービスへの再アクセスを許容するようにします。問題のないユーザーがログイン失敗等による再アクセスを行わせたい場合にご使用ください。

第 3 章 その他

3-1. 機能拡張等について

本機能は fail2ban デーモンを使用しています。お客様ご自身でセキュリティ機能を拡張したい場合には以下のページをご確認ください。尚、拡張によるファイル編集及び追加・削除についてはお客様責任となりますのでご注意ください。

https://www.fail2ban.org/wiki/index.php

WEB UI の拡張タブ内の保存ボタンイベントにて、以下のファイルは再生成されます。
・/etc/fail2ban/fail2ban.conf
・/etc/fail2ban/jail.local

拡張の際にこれらのファイルについて上書きされたくない場合には、以下のファイルを用意してください。
●上書禁止ロック用ファイル
/var/webui/config/fail2ban.userlock

また、既存の/etc/fail2ban/配下のファイルを編集した場合、元に戻すことはできません。もとに戻したい場合には、ファクトリーリセット及び再インストールを実施してください。

ぷらっとホーム株式会社
〒102-0073　東京都千代田区九段北 4-1-3　日本ビルディング九段別館 3F