SITEGUARD

Server Edition Apache 版
管理者用ガイド

― ウェブアプリケーションへの攻撃を水際で防ぐ
ウェブアプリケーション・ファイアウォール・ソリューション ―

Sample

EG Secure Solutions

はじめに

この度は、「SiteGuard Server Edition」をご購入いただきありがとうございます。
本マニュアルでは、製品のインストールおよびアンインストール、基本的な設定例、詳細な設定例などについて説明しています。
尚、本マニュアルでは、「SiteGuard Server Edition」を SiteGuard または本製品と表記します。

本マニュアルで使用するマーク

マーク	説　明
	注意していただきたいことを記載しています。
	ヒント・補足情報を記載しています。
	参照先を記載しています。

本マニュアルで使用する記号と書体

記号・書体	説　明	例
［ ］	メニュー名、項目名	**［モジュール設定］**を選択します。
〔 〕ボタン	ボタン名	〔適用〕ボタンをクリックします。
あいう ABCabc123	ウェブ管理画面の設定値	**［シグネチャ検査］**：**有効**
ABCabc123	コマンド名、ファイル名、ディレクトリ名、ディスプレイ上の出力、コード例など	**# rpm -Uvh siteguard-server-edition-*XXX*-*X*.apache.x86_64.rpm**
ABCabc123	コマンドラインでユーザが入力する文字列	
ABCabc123	コマンドラインの可変部分	

書式等が崩れる可能性があるため、各種設定で入力を行う際に、本マニュアル(PDF)の内容をそのままコピー&ペーストすることは避けてください。

1. SiteGuard について

本製品は、オンラインショッピング、イントラネット、電子商取引、電子申請、情報検索、企業・官公庁での情報提供、個人間の情報交換等で利用されているウェブサーバー、ウェブアプリケーションへの攻撃を防ぐための「ウェブアプリケーション・ファイアウォール・ソリューション」です。

ウェブサーバー、ウェブアプリケーションへの攻撃は、情報漏えい・ウェブページやデータの改ざん等に繋がる重大な脅威です。特に、最近の電子商取引の普及、官公庁の電子化、各種 ASP サービス等によるウェブアプリケーションの普及と、世界的なインターネットの利用者増大により、攻撃が広がっています。企業の場合、個人情報漏洩・データ改ざん等の被害に加え、評判や信頼の低下による間接的な影響もあります。

システム管理者は本製品を使用することで、ウェブアプリケーションの脆弱性を悪用した攻撃からウェブサーバー、ウェブアプリケーションを保護することができます。

本製品には、高品質・高性能なトラステッド・シグネチャによる「シグネチャ検査機能」が搭載されています。
また、完全な国産製品となっているため、管理画面の言語やドキュメント類の提供などはすべて日本語対応となっています。

5.4 基本的な設定

ここでは、基本的な設定内容についてのみ説明します。

詳細設定については、「7. 詳細設定」を参照してください。

メインメニューの**[モジュール設定]** →サブメニュー**[基本設定]**を選択します。

[基本設定]の画面が表示されるので、以下の設定・確認を行います。

[ウェブ攻撃検査]	検査を開始する場合は「有効」を選択します。(デフォルト無効)
[管理者への通知設定] **[検出通知]** **[障害通知]** **[メールアドレス]** **[SMTP サーバ]**	通知機能を利用する場合は「有効」を選択します。 (デフォルト無効) 通知機能を「有効」にした場合、通知先のメールアドレスとメールの送信に使用する SMTP サーバ、ポート番号を指定します。

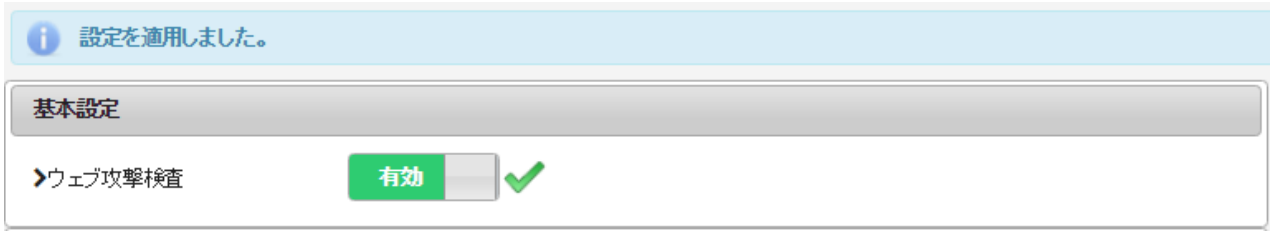
設定が完了したら、画面下の〔適用〕ボタンを押します。

Note

〔適用〕ボタンをクリックすると、apachectl graceful コマンドが実行されます。

確認ダイアログが表示されるので、設定内容が正しいことを確認してから、〔OK〕ボタンを押します。

設定適用のメッセージと検査が有効であることを示すアイコン(緑のチェック)を確認します。



Note

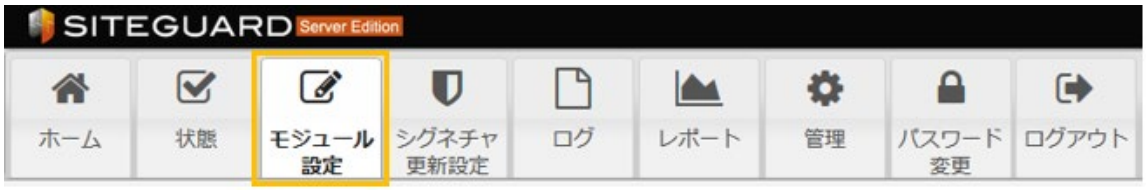
[ウェブ攻撃検査]で”有効”が選択されていて、且つ有効なシリアルキー(TRIAL VERSION を含む)が登録されている場合、アイコンが緑のチェックで表示されます。

アイコン	説　明
	本製品による検査が”有効”であることを示しています。 (緑のチェックで表示されます。)
	本製品による検査が”無効”であることを示しています。

7. 詳細設定

7.1 モジュール設定

本製品のインストールと動作確認が完了したら、必要に応じて詳細設定を行います。
検査や通知に関する設定は、メインメニューの**[モジュール設定]**で行います。



[モジュール設定]には、**[基本設定]**と**[詳細設定]**があります。
必要な設定を行い、〔適用〕ボタンで設定の保存と適用を行います。

■ボタンに関する説明

ボタン	説　明
適用	設定後、〔適用〕ボタンをクリックすると、設定の保存と適用を行います。
保存	設定後、〔保存〕ボタンをクリックすると、設定の保存を行います。
キャンセル	〔キャンセル〕ボタンをクリックすると、保存されていない設定内容を破棄します。

Note

〔適用〕ボタンをクリックすると、`apachectl graceful` コマンドが実行されます。

Note

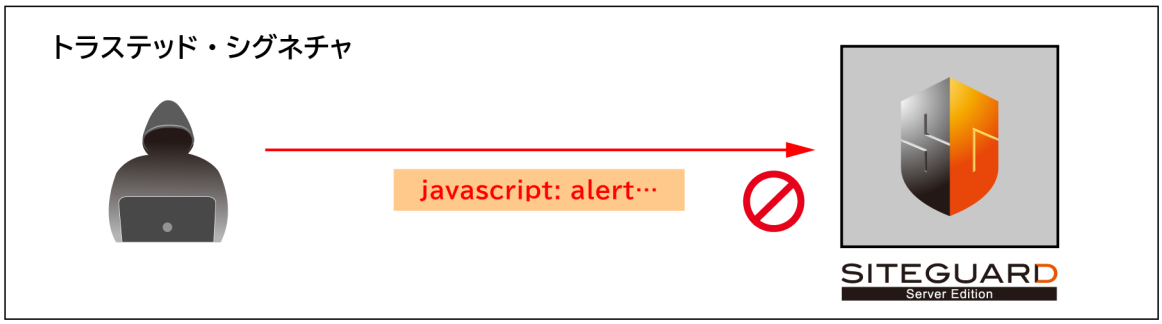
各項目の（ ）は、設定ファイル (conf/siteguardlite.ini) での項目名です。
ウェブ管理画面を使用せずに、設定ファイルを編集することも可能ですが、通常はウェブ管理画面を使用してください。

7.1.1 基本設定

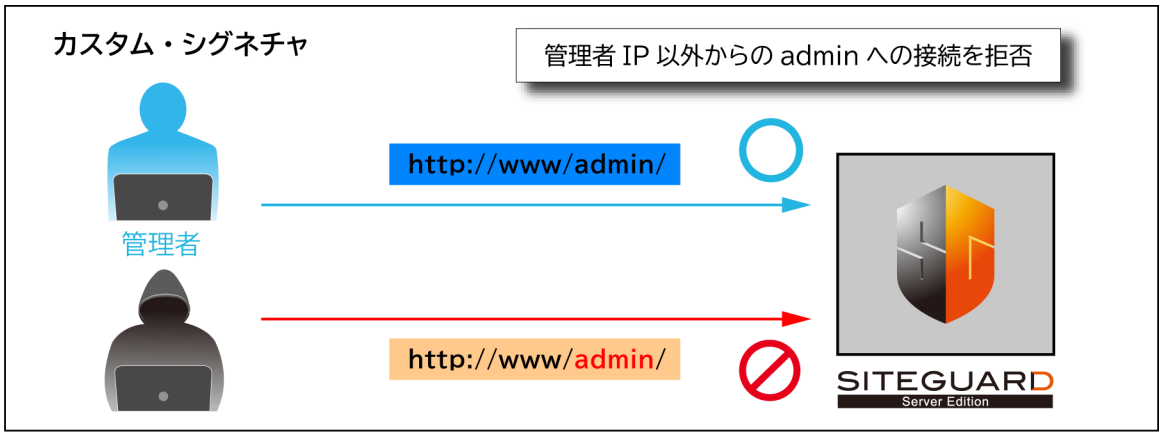
［基本設定］
Standard Settings

［ウェブ攻撃検査］
Web attack check (enabled)

本製品による検査の有効/無効の指定です。(デフォルト無効)
攻撃パターンのシグネチャを用いたシグネチャ検査を主としています。
シグネチャには、トラステッド・シグネチャとカスタム・シグネチャの 2 種類があります。
カスタム・シグネチャでは、条件を指定した検出の除外設定を行うこともできます。



詳細については、「7.1.5.1　トラステッド・シグネチャ」を参照してください。



詳細については、「7.1.5.3　カスタム・シグネチャ」を参照してください。

[管理者への通知設定]

Report settings to admin

[検出通知]

Detection notification (notify_admin)

有効にすると、攻撃を検出した場合に管理者へメールで通知します。(デフォルト無効)
通知の間隔は、分単位の**[通知間隔]**と日単位の**[毎日]**のいずれかを指定できます。

Note

・指定間隔の間に検出がなかった場合、メールは送信されません。
・メールサーバーへの接続失敗など、通知に失敗したメールは削除されます。

[通知間隔]

Notification interval (notify_admin_interval)

管理者に検出通知をメール送信する間隔(分)の指定です。(デフォルト 10)
指定した間隔(分)ごとに、サマリされた検出情報を管理者にメールで通知します。

[毎日]

Daily (notify_admin_minute / notify_admin_hour / notify_admin_daily)

管理者に検出通知を日単位でメール送信するための指定です。
毎日、指定した時間に、サマリされた検出情報を管理者にメールで通知します。
(デフォルト 0 時 0 分)

[最大詳細件数]

Max Detail (notify_admin_max_detail)

通知に含める検出情報の詳細件数(件)の指定です。(デフォルト 100)
指定した件数までは、検出情報の詳細が通知内容に含まれます。

[応答ヘッダフィールド追加]

Addition of response header field (insert_resphead)

有効にすると、応答ヘッダに指定したフィールドと値を追加します。(デフォルト有効)

Note

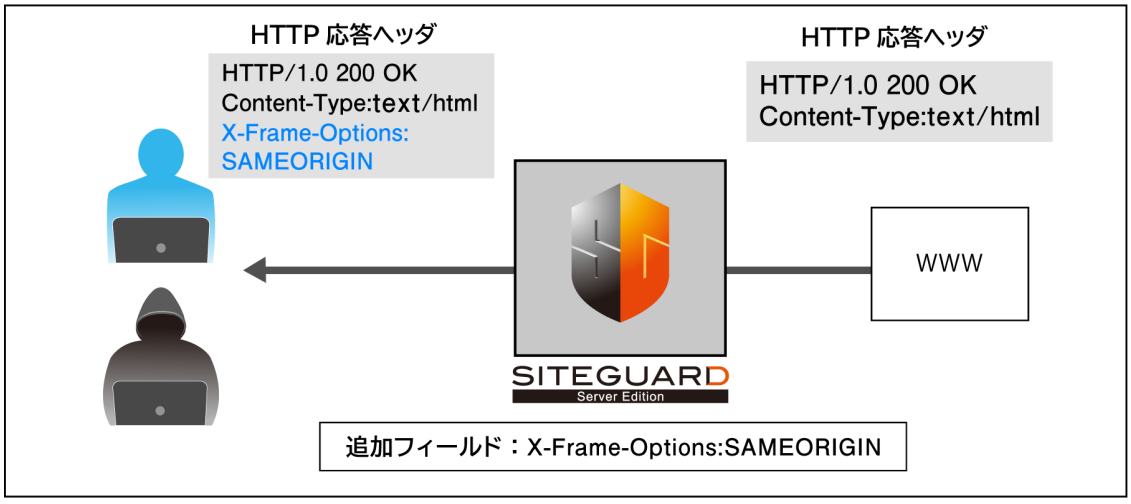
応答ヘッダフィールドの追加は、ウェブサーバーの動作が優先され、追加できない場合があります。

[追加フィールド]

Field name for the addition (insert_resphead_list)

ウェブ管理画面の場合、改行入力で複数指定できます。
設定ファイルの編集の場合は、カンマ(",")区切りで複数指定できます。(最大 1999 バイト)
(デフォルト X-Frame-Options:SAMEORIGINX-XSS-Protection:1;mode=block,X-Content-Type-Options:nosniff,Strict-Transport-Security:max-age=31536000)

設定例: クリックジャッキングの対策として活用する場合、
"X-Frame-Options: SAMEORIGIN"または、"X-Frame-Options: DENY"を指定します。



Note

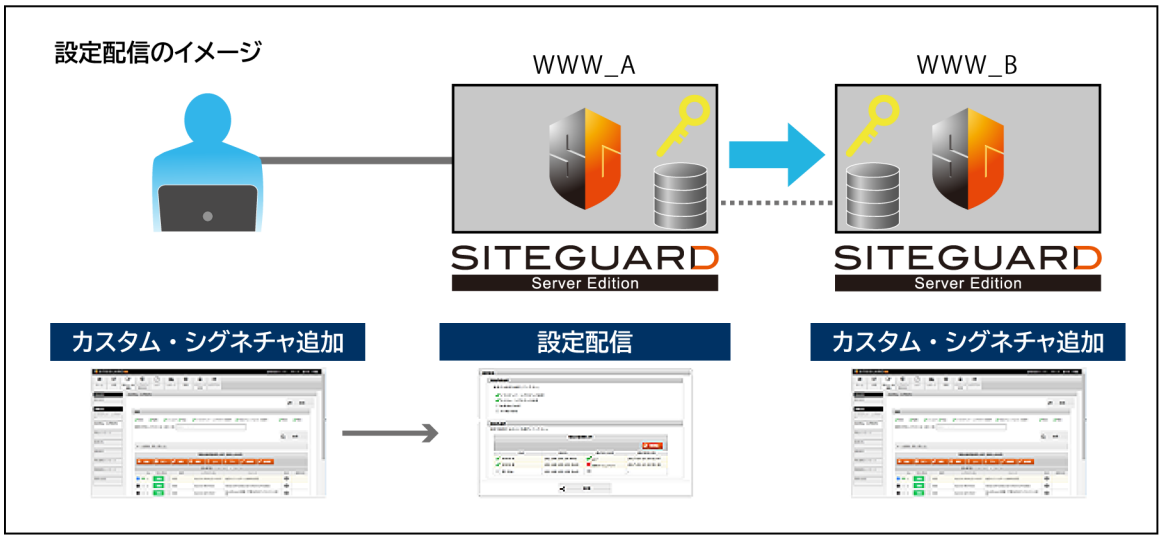
利用環境やセキュリティ要件（クリックジャッキング対策として、X-Frame-Options: SAMEORIGIN など）にあわせて、ご利用ください。

Note

指定したヘッダフィールドが既に存在する場合には、追加しません。
ヘッダフィールドの内容を変更する場合は、**[応答ヘッダフィールド削除]**を有効にして、当該ヘッダフィールド名を指定してください。

9. 設定配信

本製品には、**[設定配信]**の機能があります。
本製品を複数台のウェブサーバーにインストールしている場合、**[設定配信]**の機能を使用することで、配信元から配信先へ各種設定を配信することができます。



Note

設定配信時、ウェブ管理画面で使用しているポート(デフォルト 9443)宛に https で接続します。
予めウェブ管理画面のアクセス制御や iptables 等の設定を確認してください。

Note

・配信先の最大登録数は 20 です。
・一度に配信することのできる配信先の最大数は、10 です。

Caution

製品バージョンが異なる環境、ウェブ管理画面を使わない環境で、設定配信の機能を使用することはできません。
また、異なるプラットフォーム間で、設定配信の機能を使用することはできません。
(IIS 版や Nginx 版へ配信することはできません。)

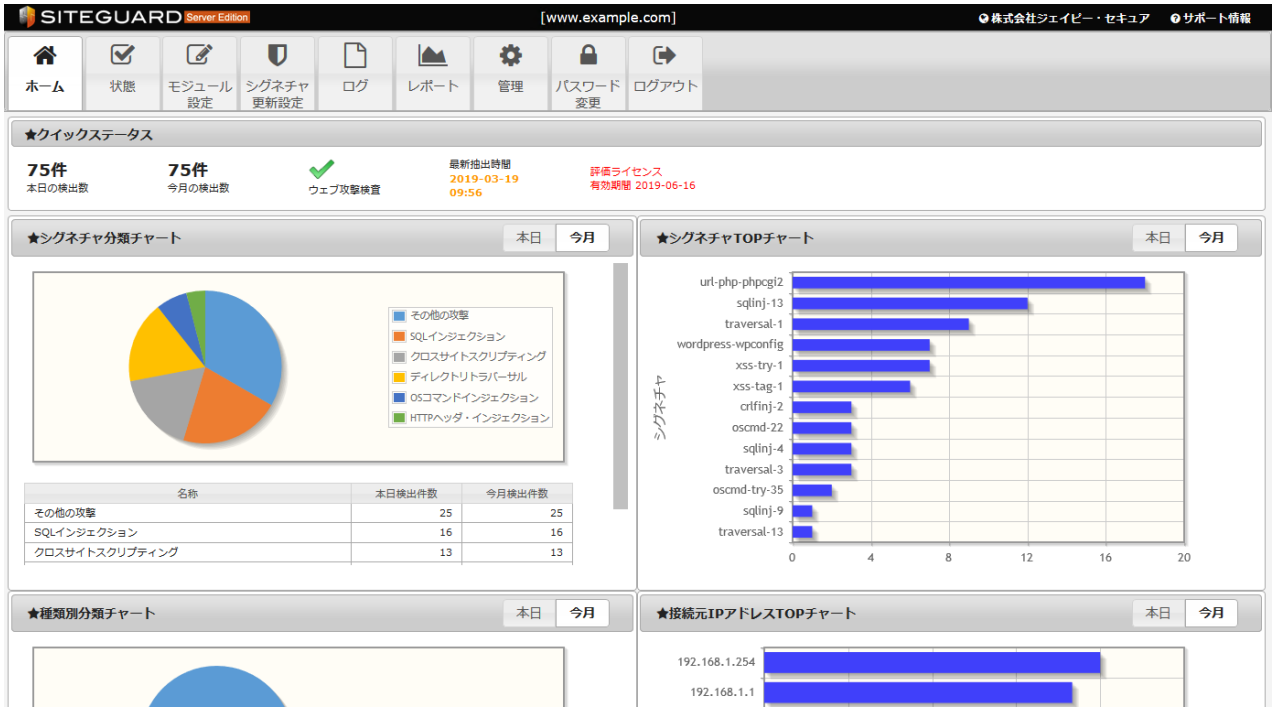
11. 統計・レポート

11.1 ホーム画面

メインメニューの**[ホーム]**では、検出情報の統計と検査の有効/無効、ライセンス状態などを確認することができます。

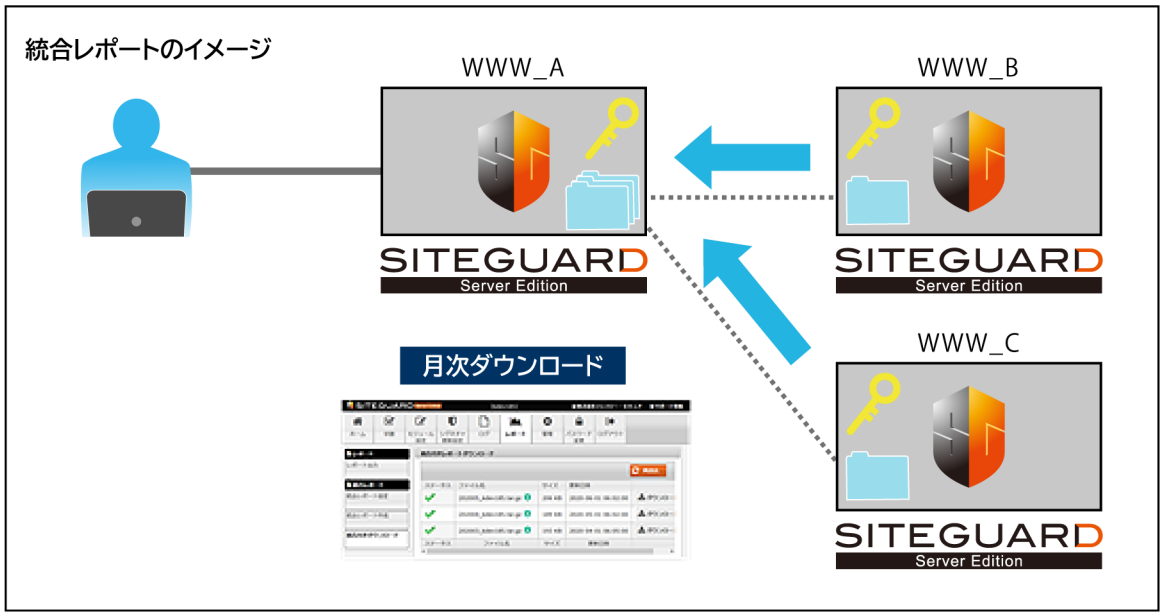
11.1.1 統計

検出全体の種類別統計のほか、検出したシグネチャの TOP チャートなどをグラフで確認することができます。



11.3 統合レポート

設定配信の機能を利用することにより、複数のウェブサーバーの統計情報を収集し、集計した統合レポートファイルを作成することができます。



Note

統合レポートは**[設定配信]**の機能を利用するため、予め**[設定配信]**の登録が必要です。
「9. 設定配信」を参照してください。

Note

統合レポートは、**[設定配信]**の配信元サーバーと配信先に登録されているウェブサーバーの統計情報を集計したレポートファイルを作成します。

Caution

統合レポートは**[設定配信]**の機能を利用するため、製品バージョンやプラットフォームが異なる環境、ウェブ管理画面を使わない環境の統合レポートを作成することはできません。

14. コマンドラインでの操作

本章では、シグネチャの更新やサービスの起動・停止などをコマンドラインで実行する場合の操作方法を説明しています。

通常、コマンドラインでの操作は必要ありません。

14.1 製品バージョン確認コマンド

■動作概要

インストールされている製品のバージョン情報を表示します。

■コマンド名

```
cd /opt/jp-secure/siteguardlite; make show_webui_version
```

■コマンド例

製品のバージョン情報を表示します。

```
# cd /opt/jp-secure/siteguardlite; make show_webui_version
```

14.2 設定情報適用コマンド

■動作概要

編集・保存した設定内容を適用します。
ウェブ管理画面で〔適用〕ボタンを押したときと同様の動作になります。

■コマンド名

```
cd /opt/jp-secure/siteguardlite; make reconfig
```

■コマンド例

編集・保存した設定内容を適用します。

```
# cd /opt/jp-secure/siteguardlite; make reconfig
```

make reconfig により、apachectl graceful コマンドが実行されます。

14.3 シグネチャ更新コマンド

■動作概要

[シグネチャ更新設定]-[手動更新]、[自動更新]で実行されるコマンドです。

https://www.jp-secure.com/download/siteguardlite/updates_lite/latest-lite.zip に接続し、トラステッド・シグネチャを最新版に更新します。(サポート ID とパスワードによる認証があります。)

トラステッド・シグネチャの更新には、以下の 3 つの処理があります。

- ダウンロード：最新シグネチャファイルのダウンロード
- 更新：シグネチャファイルの更新(最新シグネチャと既存シグネチャのマージ、更新)
- 適用：最新シグネチャファイルの適用

■コマンド名

/opt/jp-secure/siteguardlite/dbupdate_waf

dbupdate_waf では、wget コマンドを実行してシグネチャファイルをダウンロードします。

ライセンスに関する設定は、以下のファイルで設定します。

設定項目	ファイル	設定値
シリアルキー	conf/license.txt	シリアルキー
サポート ID	conf/dbupdate_waf.conf	sig_download_user=サポート ID
パスワード	conf/dbupdate_waf.conf	sig_download_pass=パスワード

ダウンロード・更新・適用に関する設定は、以下のファイルで設定します。

設定項目	ファイル	設定値
ダウンロードのみ	conf/dbupdate_waf.conf	downloadonly=yes
ダウンロードと更新	conf/dbupdate_waf.conf	downloadonly=no service_restart=no
ダウンロードと更新・適用	conf/dbupdate_waf.conf	downloadonly=no service_restart=yes

Note

適用までが行われると、最新シグネチャによる検査が有効になります。
適用時は、make reconfig コマンド(apachectl graceful)が実行されます。

追加シグネチャに関する設定は、以下のファイルで設定します。

設定項目	ファイル	設定値
推奨	conf/dbupdate_waf.conf	use_dbsettings=yes add_monitor=no
監視	conf/dbupdate_waf.conf	use_dbsettings=yes add_monitor=yes
無効	conf/dbupdate_waf.conf	use_dbsettings=no

プロキシサーバに関する設定は、以下のファイルで設定します。

設定項目	ファイル	設定値
プロキシサーバ	conf/dbupdate.conf	use_proxy=yes http_proxy_host=プロキシサーバ名 http_proxy_port=プロキシサーバのポート番号
プロキシ認証	conf/dbupdate.conf	use_proxyauth=yes http_proxyauth_user=認証ユーザ名 http_proxyauth_pass=認証パスワード

■オプション

-v　更新結果をログファイル以外（標準出力および標準エラー出力）に表示します。

■コマンド例

シグネチャファイルを更新します。

```
# cd /opt/jp-secure/siteguardlite; ./dbupdate_waf
```

シグネチャファイルを更新し、更新状況を syslog に出力します。

```
# cd /opt/jp-secure/siteguardlite; ./dbupdate_waf -v 2>&1| logger -t dbupdate_waf -p local0.err
```

本製品を導入したサーバーからインターネットへの接続が行えない場合、インターネット接続が可能な管理用 PC などを利用してシグネチャを更新することができます。

管理用 PC などからサポートページにログインして、最新のシグネチャファイル (latest-lite.zip) を取得します。
その後、製品を導入したサーバーの任意のディレクトリにシグネチャファイルを配置して、以下のように dbupdate_waf コマンドを実行します。

例）/var/tmp に latest-lite.zip を配置した場合
 # cd /opt/jp-secure/siteguardlite;./dbupdate_waf /var/tmp/latest-lite.zip

■終了コード

更新成功時は 0 を、失敗時は 0 以外を返します。

■ログファイル

更新結果は、以下のログファイルに記録されます。

/opt/jp-secure/siteguardlite/logs/dbupdate_waf.log　シグネチャ更新結果の履歴
/opt/jp-secure/siteguardlite/logs/dbupdate_waf_err.log　シグネチャ更新エラー情報
/opt/jp-secure/siteguardlite/logs/dbupdate_waf_last_result.txt　wget の実行結果