攻撃遮断くんマニュアル

目次

インストール手順(Linux 編)

お客さまでインストールが行えない場合、弊社にて無償で代行いたします。
ご希望の場合攻撃遮断くん 技術に関するお問い合わせフォームよりご連絡ください。

■ 事前準備

① FW 等の穴あけ

UDP/ (ポート番号は管理画面の対象 IP アドレス詳細ページからご確認ください)	
IN	54.92.14.101
OUT	54.92.14.101

② コンパイラ "**gcc**" または "**cc**"、及び コマンド "**make**" のインストール

上記がないとインストールを行うことができません。

■ インストール

① hosts ファイルに下記の記述を追加します。

```
49.128.58.72 msm
```

② 攻撃遮断くんパッケージの入手

※ 保存場所は任意の場所で問題ありません（/opt など）。

※ 下記 URL より攻撃遮断くんパッケージを入手し、コンソールソフトを用いてインストール作業をします。

```
# wget http://kougekishadankun.cscloud.co.jp/Download/servertect/servertect-2.7.tar.gz
```

③　解凍

```
# tar zxvf servertect-2.7.tar.gz
```

④　インストール

```
# cd servertect-2.7
# ./install.sh
```

⑤　以下、対話形式でインストール開始

※［Enter］は、エンターキーを押下することを表します。
※特に入力項目が記載されていない場合は、ブランクのままで問題なし

以下を上から順に作業してください。

```
- (en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/sr/tr) [en]: jp
-- 続けるには ENTER を押してください．また，Ctrl-C で中止します．  -- [Enter]
- どの種類のインストールを選択しますか (server，agent，local または help)? : agent
- OSSEC HIDS のインストール先を選択してください [/var/ossec]: [Enter]
- OSSEC HIDS サーバーの IP/hostname アドレスは何ですか?: msm
- 整合性検査を行うデーモンを実行させますか? (y/n) [y]: [Enter]
- rootkit 検知エンジンを実行させますか? (y/n) [y]: [Enter]
- アクティブレスポンスを有効にしますか? (y/n) [y]: [Enter]
--- 続けるには ENTER を押してください --- [Enter]
```

※上記作業を終えるとインストールが開始されるのでしばらく待ちます。

以下のメッセージが表示されればインストール完了。

```
- 初期スクリプトはブート中に OSSEC HIDS を起動するよう修正しました
- 設定が完全に終了しました.
- OSSEC HIDS を開始させます:
/var/ossec/bin/ossec-control start
- OSSEC HIDS を停止させます:
   /var/ossec/bin/ossec-control stop
 - 以下のファイルで設定についての確認と変更ができます /var/ossec/etc/ossec.conf
OSSEC HIDS の使用に感謝します.
   あなたが何らかの質問，提案したいときや，バグを発見したときは,
   contact@ossec.net まで連絡するか ossec-list@ossec.net にある
   我々の公開メーリングリストを使ってください.
(http://www.ossec.net/main/support/).
   詳細な情報は http://www.ossec.net にあります.
   ---  ENTER を押すと終了します (以下，詳細な情報が続きます). --- [Enter]
```

［Enter］を押下しインストール完了

■　セットアップ

以下で使用するエージェントキーは別途発行し、ご連絡します。発行にあたり IP アドレス情報が必要なため、事前に IP アドレス情報をお送りください。

■　エージェントへキーをインポート

```
# /var/ossec/bin/manage_agents
```

```
****************************************

* OSSEC HIDS v2.7 Agent manager.       *

* The following options are available: *

****************************************

   (I)mport key from the server (I).

   (Q)uit.

Choose your action: I or Q: i
```

i を入力し［Enter］

```
Provide the Key generated by the server.

* The best approach is to cut and paste it.

*** OBS: Do not include spaces or new lines.

Paste it here (or '¥q' to quit): ********************************
```

お申し込み後に送付されたエージェントキー文字列を入力（ペースト）し、［Enter］

```
Agent information:

    ID:xxx

    Name:VMxxxxxx_amitie

    IP Address:xxx.xxx.xxx.xxx

Confirm adding it?(y/n): y
```

IP Address が今回インストールを行ったサーバーの IP アドレスであることを確認し、y を入力し［Enter］

```
Added.

** Press ENTER to return to the main menu. [Enter]
```

［Enter］を押下しインポートメニューから離脱

```
****************************************

* OSSEC HIDS v2.7 Agent manager.       *

* The following options are available: *

****************************************

    (I)mport key from the server (I).

    (Q)uit.

Choose your action: I or Q: q
```

q を入力後、［Enter］を押下。

```
** You must restart OSSEC for your changes to take effect.

manage_agents: Exiting ..
```

上記メッセージが表示され、エージェントキーのインポートは完了

■ エージェントのセットアップ

ディレクトリの場所がデフォルトの場合、下記はご確認のみで問題ありません。

```
# vi /var/ossec/etc/ossec.conf
```

54 行目以降に記載のある<localfile>というタグで囲まれた部分を確認する。

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/messages</location>
</localfile>
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/secure</location>
</localfile>
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/maillog</location>
</localfile>
<localfile>
  <log_format>apache</log_format>
  <location>/var/log/httpd/error_log</location>
</localfile>
<localfile>
  <log_format>apache</log_format>
  <location>/var/log/httpd/access_log</location>
</localfile>
```

上記の中に、監視対象のサーバー内の

- ログインログ（secure、auth.log)
- メールログ（mail_log、mail.log)
- メッセージログ（messages、syslog)
- WEB アクセスログ（httpd/access_log、apache2/access.log)
- WEB エラーログ（httpd/error.log、apache2/error.log)

各種ログのパスが正しく記載されているか確認する。

正しく記載されていない場合は タグ内を修正する。
※もし追加で監視させたいログがある場合は、以下のルールに則り、タグを追加できます。

- **管理ツール Plesk なしの場合**

```
<localfile>
<log_format>ログの種類(web の場合は apache、syslog の場合は syslog)</log_format>
<location>ログのパス(絶対パスで記載)</location>
</localfile>
```

- **管理ツール Plesk 12 以降をご利用の場合**

```
<localfile>
  <log_format>apache</log_format>
  <location>/var/www/vhosts/[ドメイン名]/logs/access_log</location>
</localfile>

<localfile>
  <log_format>apache</log_format>
  <location>/var/www/vhosts/[ドメイン名]/logs/access_ssl_log</location>
</localfile>

<localfile>
  <log_format>apache</log_format>
  <location>/var/www/vhosts/[ドメイン名]/logs/error_log</location>
</localfile>
```

➢ **管理ツール Plesk 10,11 をご利用の場合**

```
<localfile>
  <log_format>apache</log_format>
  <location>/var/www/vhosts/[ドメイン名]/statistics/logs/access_log</location>
</localfile>

<localfile>
  <log_format>apache</log_format>
  <location>/var/www/vhosts/[ドメイン名]/statistics/logs/access_ssl_log</location>
</localfile>

<localfile>
  <log_format>apache</log_format>
  <location>/var/www/vhosts/[ドメイン名]/statistics/logs/error_log</location>
</localfile>
```

- **管理ツール Plesk なしの場合**

① iptables に localhost を ACCEPT するルールを一番上に追加

```
iptables -I INPUT -s 127.0. iptables -I INPUT -s 127.0.0.1 -j ACCEPT

iptables -I FORWARD -s 127.0.0.1 -j ACCEPT0.1 -j ACCEPT
```

② localhost の ACCEPT ルールが一番上にセットされたことを確認

```
iptables -L
```

③ Linux.zip　ZIP ファイルをダウンロードし、解凍する。

④ 解凍したファイルを、以下のディレクトリに上書き

ファイル名	firewall-drop.sh
ディレクトリ	/var/ossec/active-response/bin

⑤ ファイル権限の変更

```
chown root:ossec firewall-drop.sh

chmod 755 firewall-drop.sh
```

以下のようなパーミッション設定になっていれば問題ありません。

```
-rwxr-xr-x 1 root ossec 6841 May 31 22:34 firewall-drop.sh
```

⑥ エージェントの起動

```
/var/ossec/bin/ossec-control start
```

➢ **管理ツール Plesk をご利用の場合**

① サーバー管理 ＞ ツールと設定＞ファイアーウォールで、カスタムルールとして下記 2 つを追加。入力後［OK］をクリックし、［変更内容を適用］をクリック。

プロパティ	**ルールの名前**	任意
	一致方向	着信
	アクション	許可
ポート		指定なし
ソース		127.0.0.1

プロパティ	**ルールの名前**	任意
	一致方向	転送中
	アクション	許可
ポート		指定なし
ソース		127.0.0.1

② Plesk_Linux.zip のファイルをダウンロードし、解凍する。

③ 解凍したファイルを、以下のディレクトリに上書き

ファイル名	firewall-drop.sh
ディレクトリ	/var/ossec/active-response/bin

④　ファイル権限の変更

```
chown root:ossec firewall-drop.sh

chmod 755 firewall-drop.sh
```

以下のようなパーミッション設定になっていれば問題ありません。

```
-rwxr-xr-x 1 root ossec 6841 May 31 22:34 firewall-drop.sh
```

⑤　エージェントの起動

```
/var/ossec/bin/ossec-control start
```

導入後の注意点(Linux 編)

■ FW 穴あけ

以下の穴はふさがないでください。

UDP/ (ポート番号は管理画面の対象 IP アドレス詳細ページからご確認ください)	
IN	TCP/10050 from 122.248.248.133, 49.128.58.78, 49.128.58.72
	UDP/1514 from 122.248.248.133, 49.128.58.78, 49.128.58.72
OUT	UDP/1514 to 122.248.248.133, 49.128.58.78, 49.128.58.72

■ サーバー内設定

IP アドレス (監視対象サーバーの IP アドレス)の変更を予定される際は事前にご連絡ください。

■ ファイル

以下にて指定箇所の操作はお控えください

- /etc/hosts (ファイル内の "49.128.58.72 msm" のエントリ)
- /var/ossec （ファイル及びディレクトリ）
- /etc/init.d/ossec （ファイル及びディレクトリ）
- /etc/ossec-init.conf （ファイル）

■ サービス

以下の停止はお控えください（サービスの動作に影響を及ぼします）。

- /var/ossec/bin/ossec-control
- /etc/init.d/rsyslog　または　/etc/init.d/syslog
- /etc/init.d/iptables

■ サーバーの再起動について

お客さまのサーバーを再起動後、エージェントが自動起動しない場合がございます。
再起動後は以下のコマンドから、エージェントの起動を行ってください。

```
/var/ossec/bin/ossec-control start
```

■ ログ関連

導入後のログディレクトリ位置変更はお控えください。

Red Hat **(Federa,CnetOS など)**	● Messages ● secure ● maillog
Debian **(Ubuntu など)**	● Messages ● auth.log ● mail.log
Apache	● httpd/error_log ● httpd/access_log
apache2(debian)	● httpd/error.log ● httpd/access.log

IDS/ IPS モードへの切り替え手順(Linux 編)

■ IDS モードに切り替える

① コンフィグファイルを開く

```
vi /var/ossec/etc/ossec.conf
```

② 以下の設定を、</ossec_config>のすぐ上に記述

```
<active-response>

        <disabled>yes</disabled>

</active-response>
```

■記入例

```
        <localfile>
                <log_format>full_command</log_format>
                <command>last -n 5</command>
        </localfile>

        <active-response>
                <disabled>yes</disabled>
        </active-response>

</ossec_config>
```

③ エージェントの再起動

```
/var/ossec/bin/ossec-control restart
```

④ 再起動完了後、念のため遮断処理が走っていないか確認

```
tail -f /var/ossec/logs/active-responses.log
```

※5 分程度確認し、新しくログが記述されないようであれば問題ありません。

■ IPS モードへの切り替え

① コンフィグファイルを開く

```
vi /var/ossec/etc/ossec.conf
```

② 以下の設定を削除するか、<disabled>の設定値を no に変更

```
<active-response>

        <disabled>yes</disabled>

</active-response>
```

上記 3 行を削除。または、

```
<active-response>

        <disabled>no</disabled>

</active-response>
```

③ エージェントの再起動

```
/var/ossec/bin/ossec-control restart
```

④ 再起動完了後、念のため遮断処理が行われているか確認

```
tail -f /var/ossec/logs/active-responses.log
```

※5 分程度確認し、ログが記述されていることを確認 または、

```
iptables -L
```

で iptables への DROP 文追加が追加されることを確認してください。

【重要】 攻撃遮断くん緊急対応手段(Linux 編)

■ エージェント停止方法

SSH クライアントソフトでサーバーに接続

① root にスイッチ

```
# sudo su
```

② 攻撃遮断くんの各サービスの停止

```
# /var/ossec/bin/ossec-control stop
```

■ エージェント開始方法

SSH クライアントソフトでサーバーに接続

① root にスイッチ

```
# sudo su
```

② 攻撃遮断くんの各サービスの開始

```
# /var/ossec/bin/ossec-control start
```

■ iptables のルール削除

※ **必ずエージェントの停止後に作業をしてください。**

※ **エージェントの停止を手動で行った場合は、必ず弊社までご連絡ください。**

エージェントが停止されていれば、ルールが新たに書き込まれることはございませんが、既に書き込まれたものを削除したい場合、以下を参考にしてください。

- **方法 1**

```
# iptables -L --line-numbers
```

※フォルスポジティブに該当するルールの番号を確認

```
# iptables -D INPUT <番号>
# iptables -D FORWARD <番号>
```

※<番号>は確認したルールの番号。num = 1 なら 1 を入力

- **方法 2**

```
# iptables -L
```

※フォルスポジティブに該当するルールを確認

```
# iptables -D INPUT <確認したルール内容>
# iptables -D FORWARD <確認したルール内容>
```

アンイストールの手順

① エージェントをストップする

```
# /var/ossec/bin/ossec-control stop
```

② ユーザ削除、関連ファイルのリムーブ

```
# userdel ossec

# rm -rf /var/ossec

# rm -f /etc/ossec-init.conf
```

防御証明メール解説

攻撃を検知遮断した際に、お申込時にご連絡いただきました「防御証明メール送付先アドレス」宛にこちらのフォーマットに従いメールが送信されます。

防御証明メール表示上の注意事項

messages ログから攻撃を検出した場合に、正しい攻撃元にて検出を行っているものの、防御証明メール内での Attacker アドレスが、監視対象の IP アドレスになってしまうメール表示上の不具合が発生することがあります。

実際の攻撃元は、「userdata1:」内に記載されている rhost=xxx.xxx.xxx.xxx が攻撃元 IP アドレスとなりこの IP アドレス(ホスト名)からの通信を遮断しており、監視対象の IP アドレスについては一切遮断を行っておりません。

この不具合に関しては現在改修中です。

件名	
[mFusion #0999999]	管理用の ID です
directive_event: xxxxxxxxxxxxxxxxx	検出した攻撃の種類です
本文	
Opening date : DD-MM-YYYY HH:MM	検出日時です。 ここでの日時は SGT です。（日本時間は UTC+9 ですので、この時刻から 1 時間を加えたものとなります）
Name :YYYY-MM-DD HH:NN:SS directive_event: xxxxxxxxxxxxxxxxx	タイトルの記述部です。詳細は上記と同じ

Requesters: N/A	このチケットの発行者です。”z-msmadmin“はシステム用 ID です
Assigned to - Technicians : VMxxxxx Amitie	アラートメール送信先の管理用 ID です
No defined category	検出攻撃のカテゴリの有無です。カテゴリの設定はないので、左記記述となります
Description : Attacker: xxx.xxx.xxx.xxx, prot, 0	検出の説明です。攻撃者の IP アドレス、”prot”にはプロトコルが記載されます(TCP/UDP)。 ”0”にはポート番号が記載されますが、0 が記載されます。
Victim: xxx.xxx.xxx.xxx, VMxxxxx-Amitie, prot, 0	犠牲者＝攻撃を受けたホストの情報です。IP アドレスと、VMxxxxx-Amitie として弊社管理用ホスト名が記載されます。 prot、0 については上記と同様です。
Alert detail:	アラート詳細
* userdata2: xxxxxxxxx	検出の原因となった直接的な理由が記載されます。攻撃内容により、ログの記載部分が記述される場合があります。
* userdata1: Multiple failed logins in a small period of time.	攻撃と判断した理由。ブルートフォースアタックでは、複数のログから相対的に攻撃と判断するため記載されます。
* userdata1: (VMxxxxx-Amitie) xxx.xxx.xxx.xxx->/var/log/secure	検出元となったログファイル名が記載されます。
* protocol: tcp	プロトコル。TCP か UDP が入ります。

* rep_rel_dst: 0	攻撃を受けたホストの評価。悪評に関する評価のため、0 となります。
* userdata5: pam,syslog,authentication_failures,	検出グループを表示しますが、内部管理用の情報です。
* context_id: a9f4379a-5ce7-11e2-9043-001a4beeeca8	内部管理用の ID です
* userdata9: Vmxxxxx-Amitie	弊社内管理用ホスト名です
* actions: 1	検出時のアクションのパラメータの記載です。
* reliability: 8	検出の信頼性を表します。 例えば SQL インジェクションの場合、ユーザページ遷移時の URL に、シグネチャに合致するパラメータが含まれる場合があるため、若干低い信頼性の数値が表示されます。
* plugin_sid: 500002	弊社内部管理用の ID です
* rep_prio_src: 0	攻撃元 IP アドレスの評価。悪評のある IP アドレスの場合、ここに数値が入ります。
* priority: 3	優先性。検出された攻撃からその優先性を示します。
* src_port: 0	攻撃者が攻撃してきた際の攻撃者側ホストの使用ポート。検出内容により 0 が入ります。
* userdata4: Multiple failed logins in a small period of time.	検出理由を記載しています。

* event_id: 4beeeca8-a788-11e2-a483-001ae3a36860	弊社管理用 ID です
* src_ip: xxx.xxx.xxx.xxx	攻撃者の IP アドレス。
* backlog_id: 4beeeca8-a788-11e2-a483-001ae3a365fe	弊社管理用 ID です
* plugin_id: 1505	弊社管理用 ID です
* sensor: 49.128.58.72	この攻撃を検出した仮想アプライアンスの IP アドレスです。
* username: auth	認証失敗時に使用してきたユーザ ID です ブルートフォースアタックの場合に記載されます（左記のケースの場合、auth という ID を使用してきたということになります） auth のほかにも、root、user、admin などで試行されるケースが多いです。
* risk: 1	リスクを表し明日。
* rep_prio_dst: 0	攻撃を受けたホストの評価。悪評に関する評価のため、0 となります。
* date: YYYY-MM-DD HH:NN:SS	検出日時です。 ここでの日時は UTC です。（日本時間は UTC+9 ですので、この時刻から 9 時間を加えたものとなります）
* type: event	アラートメールのタイプです。全て event となります。
* rep_rel_src: 0	攻撃元 IP アドレスの評価。悪評のある IP アドレスの場合、ここに数値が入ります。

* dst_port: 0	攻撃を受けた際の被害者側ホストの使用ポート。検出内容により 0 が入ります。
* dst_ip: xxx.xxx.xxx.xxx	攻撃を受けたホストの IP アドレス
* policy_id: ecf6410f-f344-d8c1-b5f9-869c62181b57	弊社管理用 ID です。