【入替方式確認手順書】

入替方式が不明なお客様はこちらの手順にて、入替方式を確認してください。

【前提条件】
以下の手順は、 /var/ossec 配下のディレクトリにスクリプトがインストールされているものとして記載しております。
別のディレクトリにインストールされている場合は、適宜変更をよろしくお願いいたします。

【確認手順】
1. firewall-drop.sh の状態を確認してください

お客様のサーバにある firewall-drop.sh が現行の firewall-drop.sh と差分が無いかを確認するため、以下コマンドを実施してください。

sha256sum /var/ossec/active-response/bin/firewall-drop.sh

出力されたハッシュ値が以下と同一であることをご確認下さい。
3a08ee08dd318ab56ea2e78b2e9e2f09b39e9dab2d5bd03ece35550ff7dce4f0

※ハッシュ値が異なる場合は、弊社サポートまでお問合せ下さい。
攻撃遮断くんサポートチーム：support@cscloud.co.jp

2. modsecurity.sh の状態を確認してください
対象ファイル：/var/ossec/active-response/bin/modsecurity.sh
grep 'SecRule' /var/ossec/active-response/bin/modsecurity.sh

出力例)
SecRule REQUEST_HEADERS:X-Forwarded-For "@Contains ${IP_ADDRESS}" "log,drop,id:${RULEID}, msg:'deny by ossec-agent'"

上記コマンドで、以下のどちらが記載されているかをご確認ください。

2-1.「REQUEST_HEADERS:X-Forwarded-For」の記載がある場合
SecRule REQUEST_HEADERS:X-Forwarded-For "@Contains ${IP_ADDRESS}" "log,drop,id:${RULEID}, msg:'deny by ossec-agent'"

【3】XFF 遮断入替手順 を参照の上、スクリプトの入れ替えを行ってください。

2-2.「REMOTE_ADDR」の記載がある場合
SecRule REMOTE_ADDR "^${IP_ADDRESS}$" "log,drop,id:${RULEID},msg:'deny by ossec-agent'"

【4】REMOTE_ADDR 遮断入替手順 を参照の上、スクリプトの入れ替えを行ってください。

以上で、入替方式の確認手順は終了です。