# AS Engine によるスキャンについて

2010 年 7 月 21 日現在

| | |
|---|---|
| 対象製品 | FortiGate |
| 対象 OS | FortiOS 4.0 and upper |
| 項目 | Spamfilter, Update |

このドキュメントでは、FortiOS 4.0 から新しく導入された AS(Antispam) Engine によるスキャンについて説明します。

AS Engine はメールデータから検出される IP アドレスや URL などをスキャンし、スコアリングを行います。そのスコア値がしきい値を越える場合はそのメールをスパム判定するヒューリスティック方式の検出を行います。その際にスキャンを行うプログラムが AS Engine です。

これは、Blacklist に登録された IP アドレスや URL が FortiGate に保存されるという事ではありません。FortiOS 4.0 以降でも Blacklist された情報については、リアルタイムで FortiGuard Center へ確認を行います。

◆ FDN との接続性確認

下記コマンドによって、リアルタイムな問合せ先の FDN に接続できているかどうかを確認することができます。

```
# diagnose spamfilter fortishield servers
```

◆ Blacklist の照会

特定の IP アドレスや URL が Blacklist に登録されているかどうかを下記サイトから確認することができます。
http://www.fortiguard.com/antispam/antispam.html

◆ AS Engine の設定

下記設定によって、AS Engine が SPAM 判定するスコアのしきい値を設定することができます。Defualt は 80 です。もし AS Engine によるスキャンを無効にしたい場合は、このしきい値を 100 より大きく設定してください。しきい値は 100 を越えることがありませんので、AS Engine によってメールをブロックすることはなくなります。

```
# config system fortiguard
# set antispam-score-threshold <Value>
# end
```

現在この設定は Global 設定ですので、Protection Profile 毎に設定を変更することはできません。

◆　AS Engine によるスキャン結果

詳しいスキャン結果については、下記 2 つの方法で確認することができます。

下記 Debug を有効にして、そのログ内容の範囲で確認することができます。

```
# diagnose debug application spamfilter 255
# diagnose debug enable
```

また、スキャンされたメールが送信先へ配送されるケースでは、そのメールヘッダの X-ASE-REPORT フィールドにスキャン内容が追記されております。

◆　AS Engine のログ

AS Engine によって検出されたメールについては、Spamfilter Log に記録されます。その時には"email is reported as spam by ASE"というメッセージがログに記録されます。

また、各メッセージに付与されている tracker ID によってどのようなスキャンが行われたかを識別することができます。現在はこの ID からその内容を確認する情報はございませんが、今後提供する予定です。

■　**参考資料**

AntiSpam Rule Set Updates in FortiOS Version 4.0
http://kb.fortinet.com/kb/documentLink.do?externalID=FD30017

-以上-