

Filter by Yourself

Ichiro Mizukoshi

NTT EAST

i.mizukoshi@east.ntt.co.jp

#librahack

2011/5/25

librahack氏逮捕

拘留20日後、起訴猶予処分で釈放

逮捕理由

岡崎市立図書館へのDoS攻撃

DoS攻撃の内容

新着図書をチェックするために自作ソフト作成

いわゆる、マッシュアップ

アクセスは 1秒に1回程度

参考url <http://www26.atwiki.jp/librahack/>

論点

非常にたくさん

警察、図書館、システム構築者、ユーザー...

ISP側での

DoS対応が

~~なっていない!?~~

運用でカバー

DoS対応:Filter設定

- ホームページ上に掲載していますか？
- 対応が標準化されていますか？
- どうやって受付けますか？
- 誰が設定しますか？
- 解除するタイミングは？

オペレータのボランティア？
コスト回収？

前提条件

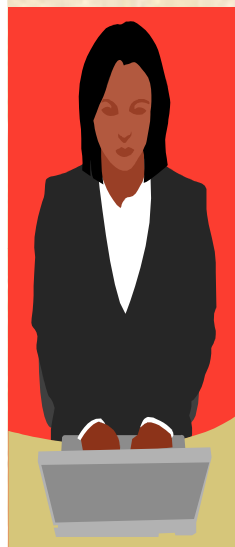
- 人が介在するのはコスト高
 - 伝達ミス
 - 勘違い
- 回線自体が使えない可能性
 - 戻りパッケージが届かない可能性
- ユーザが自立的に設定・解除

CPEの存在

- トラフィックを把握
- FW機能

CPEが自動的に設定・解除

提案 Filter by yourself



HGW

CPE

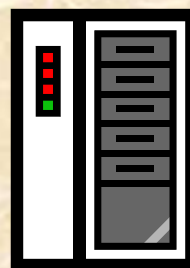
Set Filter

check Filter

Filter LIST

Clear Filter

アクセスライン

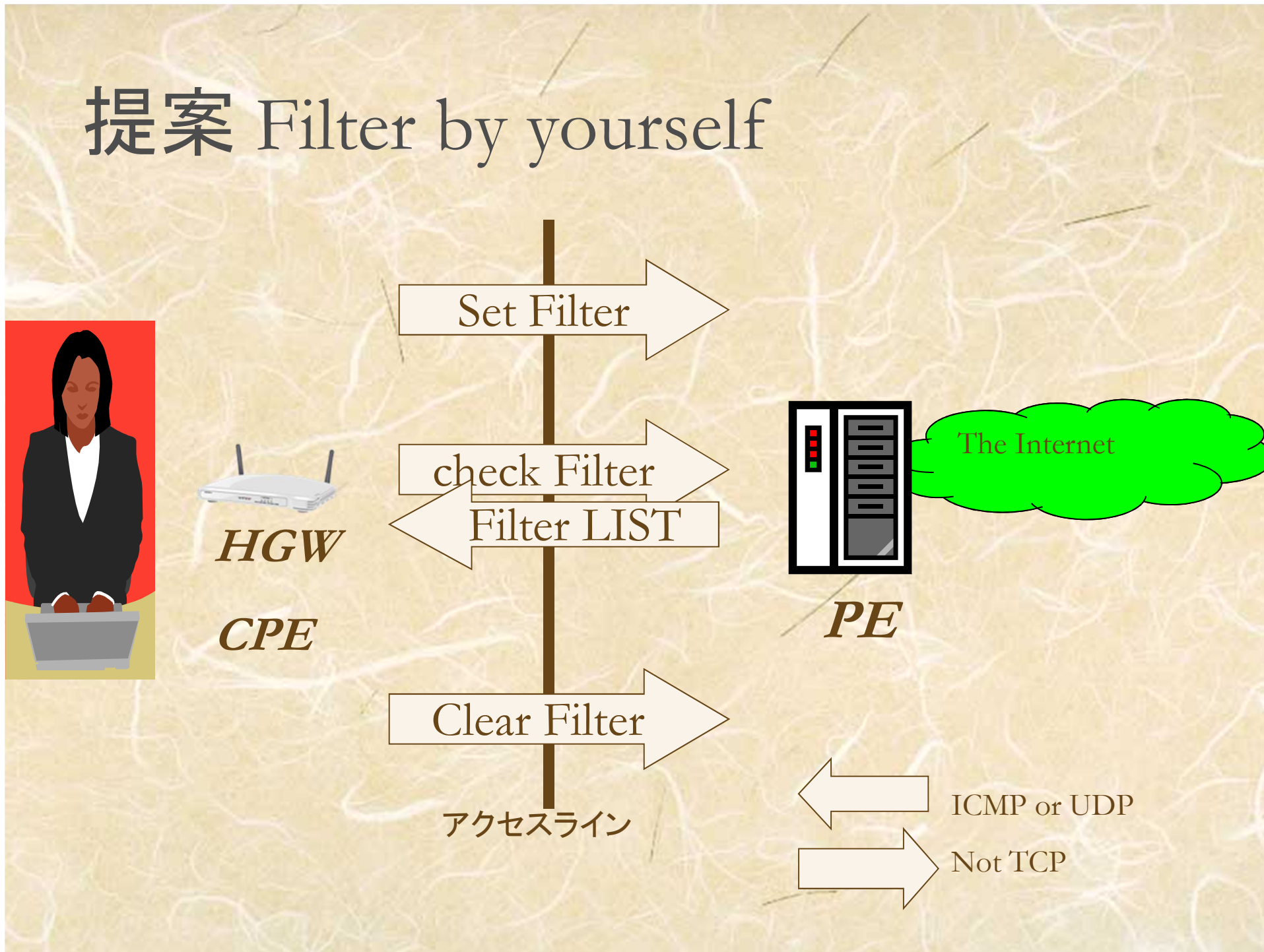


PE

The Internet

← ICMP or UDP

→ Not TCP



おまけ

- PEのFilterを上流に伝播 moving FW 😊
- Filterでとめられた場合
CPEが生成するICMP unreachable を
戻り側スタックでもう少し配慮を...

さらにおまけ 迷惑電話おことわりサービス

http://web116.jp/shop/benri/meiwaku/mei_00.html