

# 今、起きている迷惑メール問題の共有と解決に向けて ～ submission 踏み台問題～

## 1 submission 踏み台問題とは？

加瀬 正樹（ニフティ株式会社）

## 2 ISPの対応事例～BIGLOBE編～

加藤 理人（NECビッグロース株式会社）

## 3 スпамメール×マルウェアの実態

上村 理（トレンドマイクロ株式会社）

## 4 Submission踏み台問題への対策

西島 正憲（株式会社シマンテック）

## 5 対策の実際と将来的な解決は？

加瀬 正樹（ニフティ株式会社）

## submission 踏み台問題とは…

正規のユーザになりすまし、世界中のBotからISPの送信サーバ(submission)を踏み台にして迷惑メールが発信されてしまう問題。正しいID/PWを使ってSMTP-AUTHするのが特徴。

JEAGでもSMTP-AUTHを使ったBot送信は指摘されていて、**通数制限**がプラクティスとして紹介されていた

Recommend 5 : MSA(587+Auth)における送信数制限の実施

JEAG

◆MSAにおいては、「SMTP AUTH」を利用した送信数制限を実施するべきである。

- 通数は「RCPT TO」でカウントするべきである。

■ 対象 : Global IP Addressから投稿を受け付けるMSAの管理者

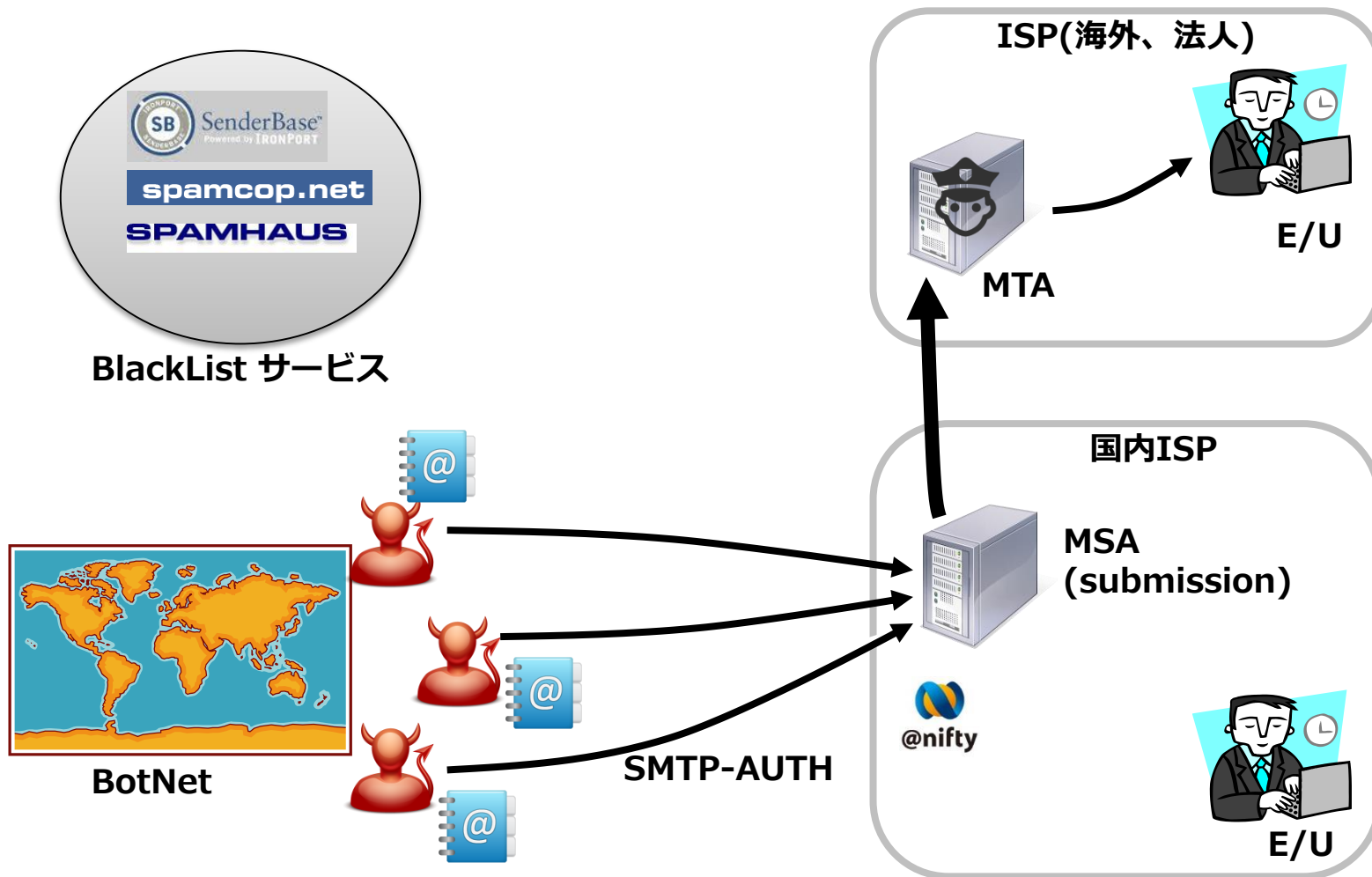
■ OP25Bにより送信手段を失ったSpammerやbotは、バターン上の送信記録を利用し追跡

→ すでにこの傾向は表れている？

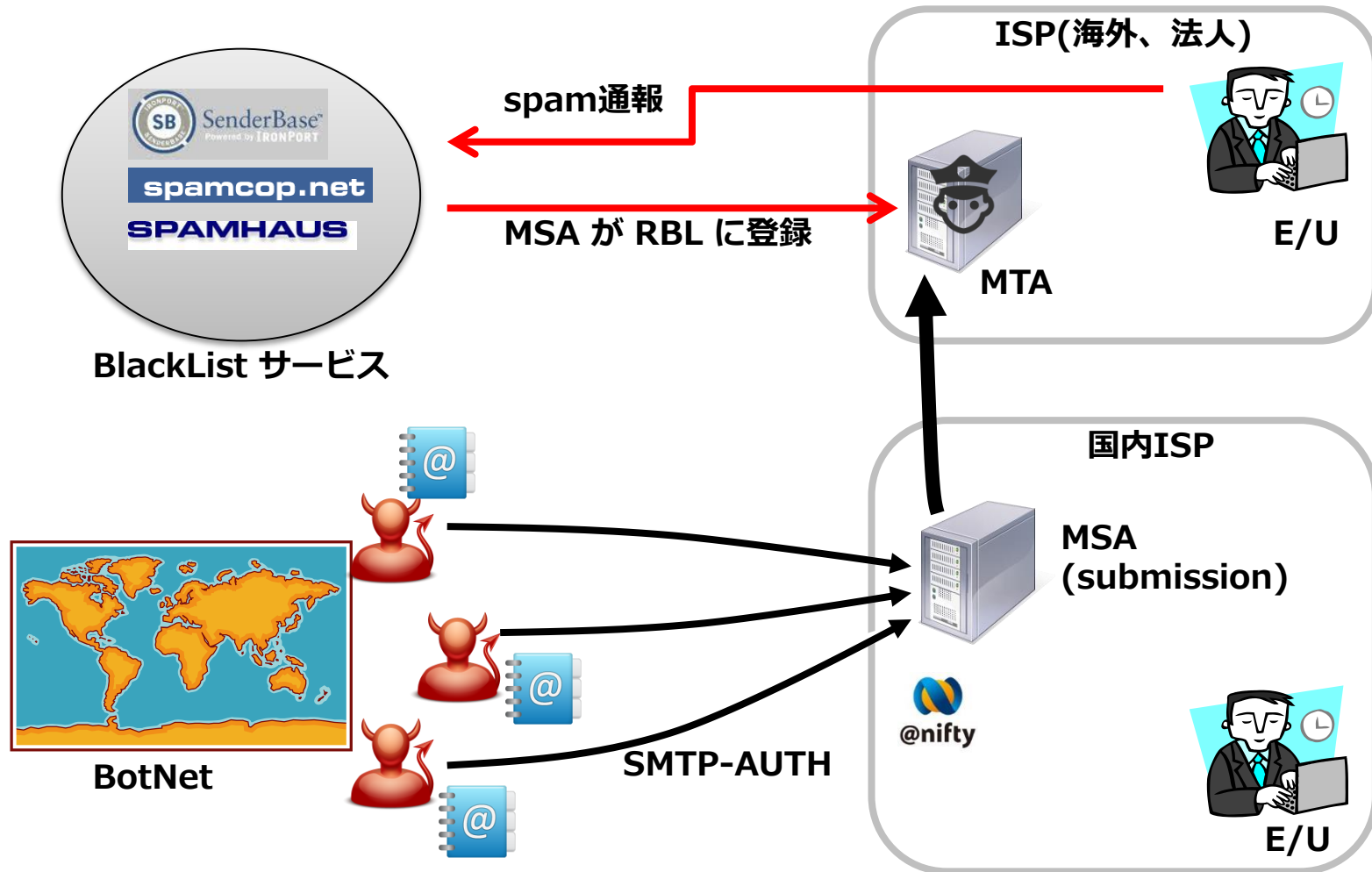
Copyright (c) 2006 JEAG. All rights reserved.

[引用] 第3回迷惑メール対策カンファレンス  
「JEAG1 (導入、携帯、OP25B)」 (2006年)

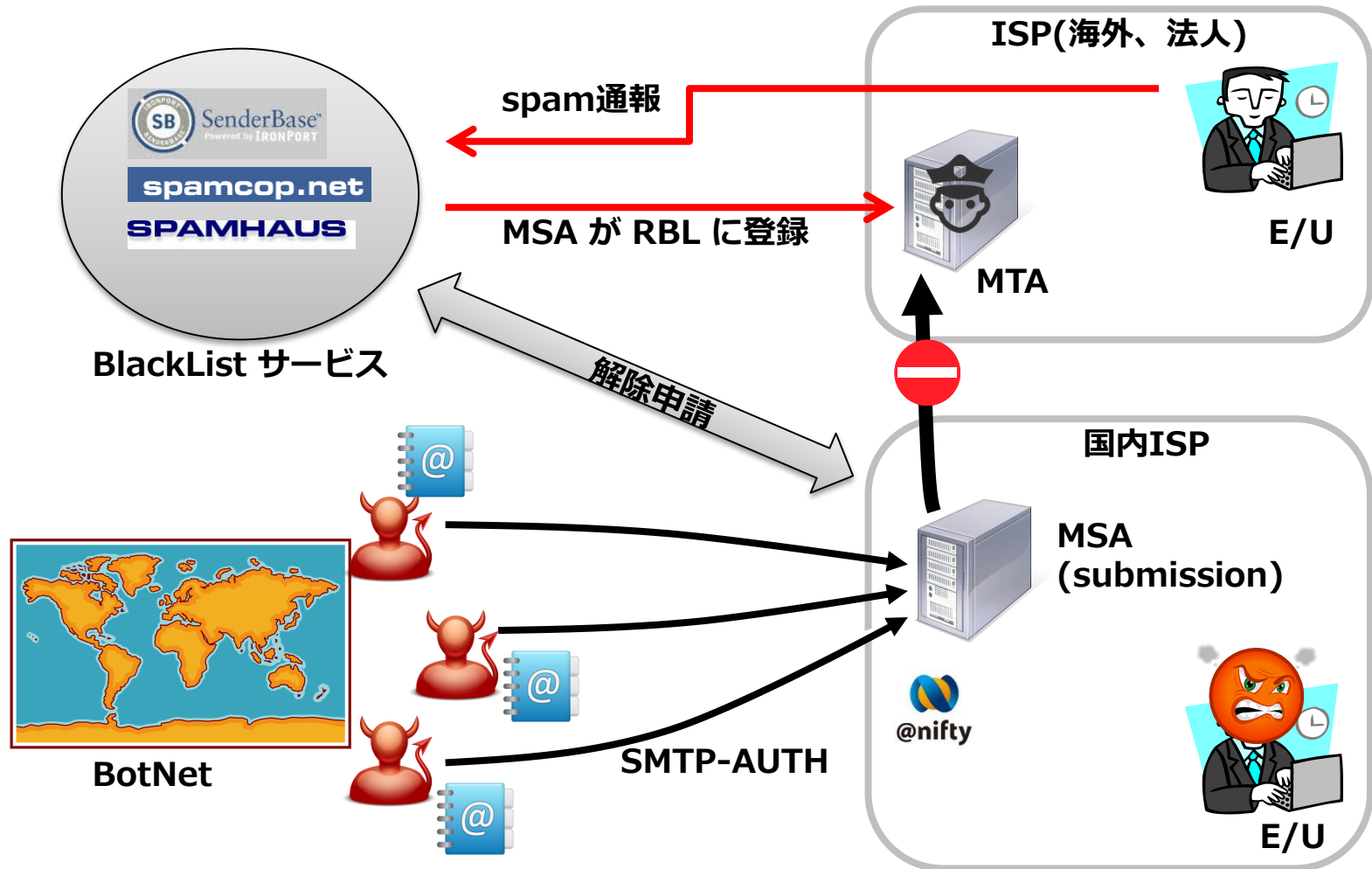
① スパマーは何らかの方法で、正規のID/PWを入手。  
BotからSMTP-AUTHで迷惑メールを大量発信。



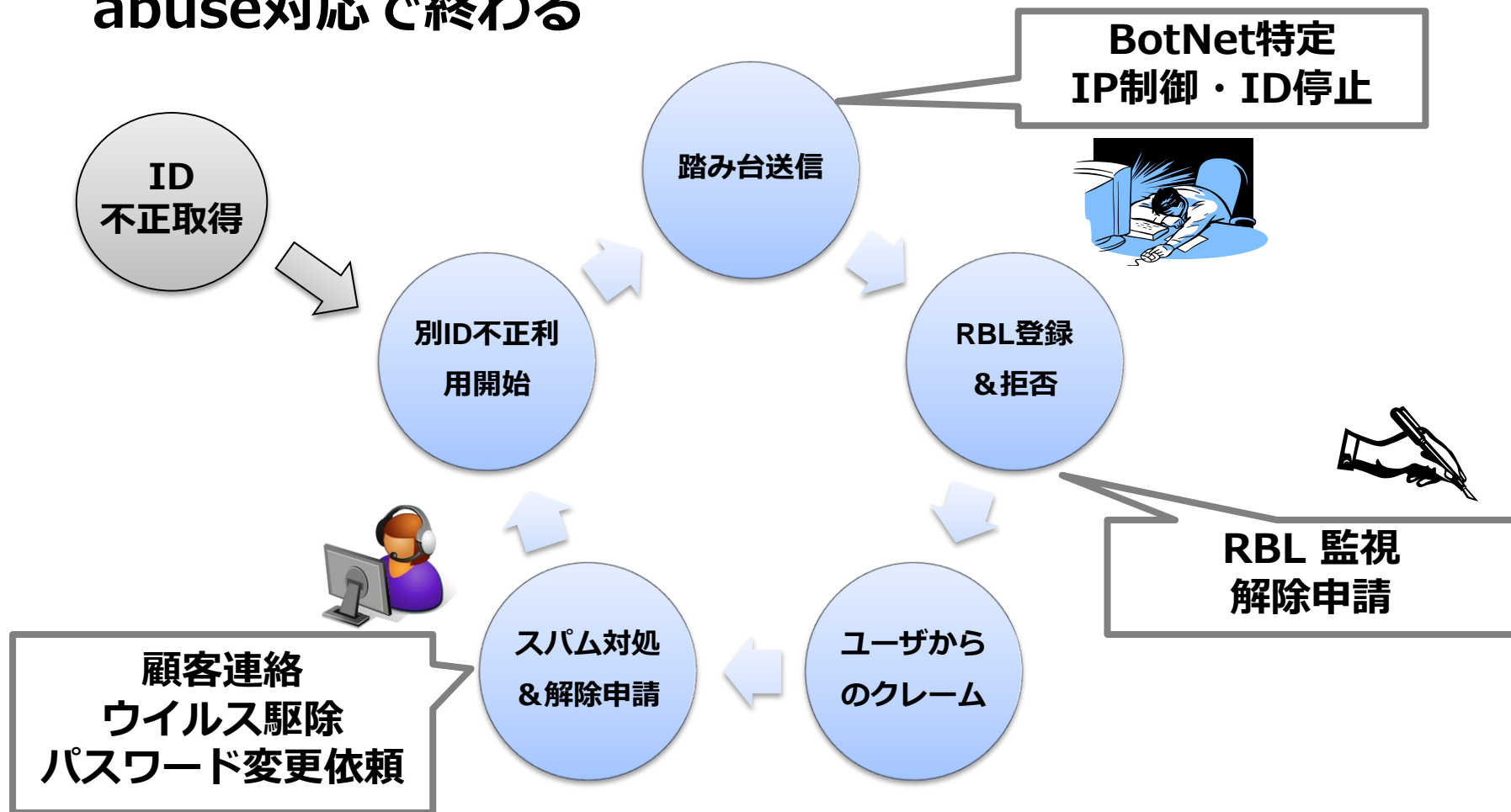
②迷惑メールを受信したエンドユーザは通報。  
BlackList サービスが送信元IPを BlackList へ登録。



③ submission を踏み台にされた ISP のユーザは送信メールが不達になり、BlackList(RBL) 解除申請を行う。



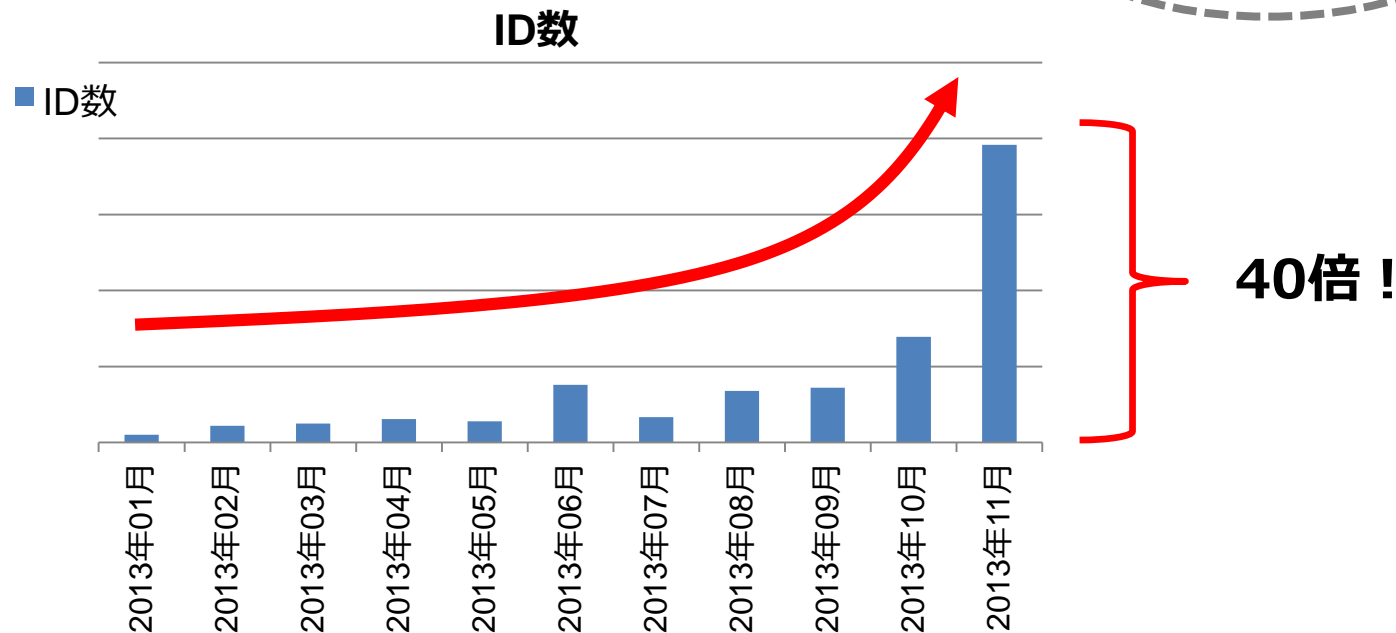
## メール運用者・サポートセンターの日々が abuse対応で終わる



ニフティでは2013年秋ごろから急増（1年で**40倍**）  
「海外IP」「複数IP」「100通～100万通」

POP before SMTP: 54%  
Submission: 44%

あくまで参考  
PbS廃止が解決  
ではない





## いくつかの切り口から詳細解説



③

OutBound Filtering  
の可能性は？



②

いかにしてID  
は乗っ取られる？



踏み台送信

別ID不正利  
用開始

RBL登録  
& 拒否

①



ISPのabuse対応  
や顧客対応は？

スパム対処  
& 解除申請

ユーザから  
のクレーム