

第14回・第15回
迷惑メール対策カンファレンス
『ISPが取り組む迷惑メール送信対策の紹介
～続・Submission 踏み台問題～』

2016/10/04 大阪
2016/10/05 東京
ビッググローブ株式会社
加藤理人

自己紹介

◆ 氏名

加藤理人

◆ 所属

ビッググローブ株式会社

ITシステム本部 メールサービス開発ユニット

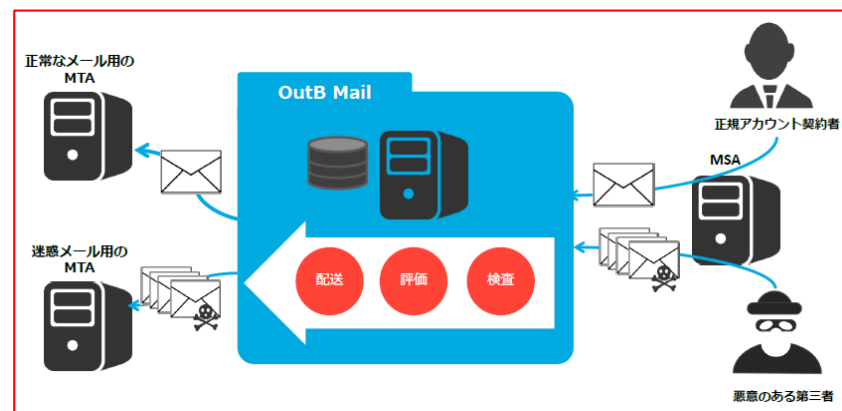
◆ 担当業務

会員向けメールサービス企画・開発・運用

CSIRTメンバ、迷惑メール対策WGメンバ(踏み台問題に注力)

◆ ご参考

- 踏み台問題に対応できるソリューション
- サイバネット株式会社と共同開発
- 送信メールをスパム/ウイルス検査
- BIGLOBEのノウハウを盛り込み
- 判定結果を元に出口MTAを切替
- 送信者のふるまいを分析等の豊富な機能



<http://www.cybernet.co.jp/outbmail/> から引用

自己紹介

◆ 氏名

伊藤 隼人 (いとう はやと)

◆ 所属

ニフティ株式会社

ネットワークサービス事業部 カスタマーサービス部

◆ 担当業務

@nifty 会員向けメールサービスの開発、システム運用

自己紹介

◆ 氏名

加瀬 正樹 (かせ まさき)

◆ 所属

ニフティ株式会社

ネットワークサービス事業部 カスタマーサービス部
部長代理

◆ 担当業務 (プロダクトオーナー)

@nifty 会員向けメールサービス

@nifty 会員向けセキュリティサービス

@nifty 会員向けオプションサービス (一部)

踏み台問題のおさらい

- ◆ 踏み台問題とは
 - 迷惑メール送信手口の一つ
 - 正規のアカウント/パスワードを使用してメール送信
 - アカウント所有者は送信していない場合が多い
- ◆ アカウント所有者以外が正規の送信サーバを悪用するところから『踏み台問題』と呼ばれている
- ◆ 過去2回 取り上げ

- ◆ 2014年2月14日
第10回 迷惑メール対策カンファレンス
『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～』
http://www.iajapan.org/anti_spam/event/2014/conf0214/program.html

- ◆ 2014年10月8日
第11回 迷惑メール対策カンファレンス
『日本がスパム発信元でなくなるためには
～続・Submission 踏み台問題～』
https://www.iajapan.org/anti_spam/event/2014/conf_11th/program.html

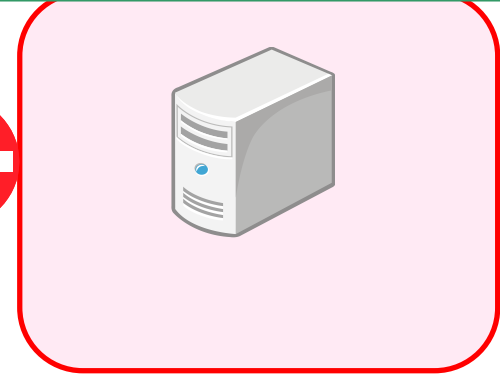
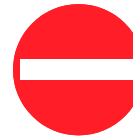
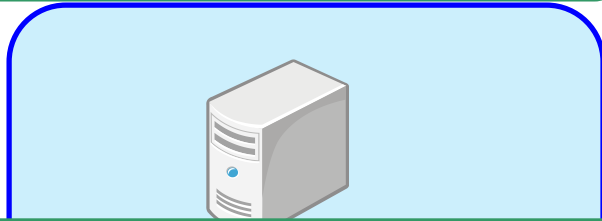
踏み台問題の構図 (第10回 迷惑メール対策カンファレンス資料より)



④ BlackListに登録される



⑤ 送信メールの到着遅延/不達



③ サーバ高負荷、メール滞留発生

② アクセス集中で送信しづらい状況

正常利用者にも影響発生！



踏み台問題が及ぼす影響(サポート/利用者)

(第10回 迷惑メール対策カンファレンス資料より)

サポート部門の負荷が増加
踏み台問題の対応に時間取られる

アカウントが悪用されている

システム管理 サポート部門



問い合わせ調査/回答

BlackList解除申請

エラーメールがたくさん届いたのはなぜですか？

○月○日に
大量にメール送信
していますよ

SPAMメールを送信した
心当たりがありません

送信したメールの到着が遅延した

迷惑メールが届いた
対処してください

会員



受信者

事例紹介 <ビッググローブ>

- ◆ 踏み台問題に取り組むWG活動実施中
- ◆ WGメンバ：Abuse担当、メールシステム部門、セキュリティ部門



踏み台送信の発生

Abuseチーム

共有

WG活動

検知・対処

手口分析・対策検討・実施

踏み台送信の実例

会場のみ公開とさせていただきます

踏み台送信の実例

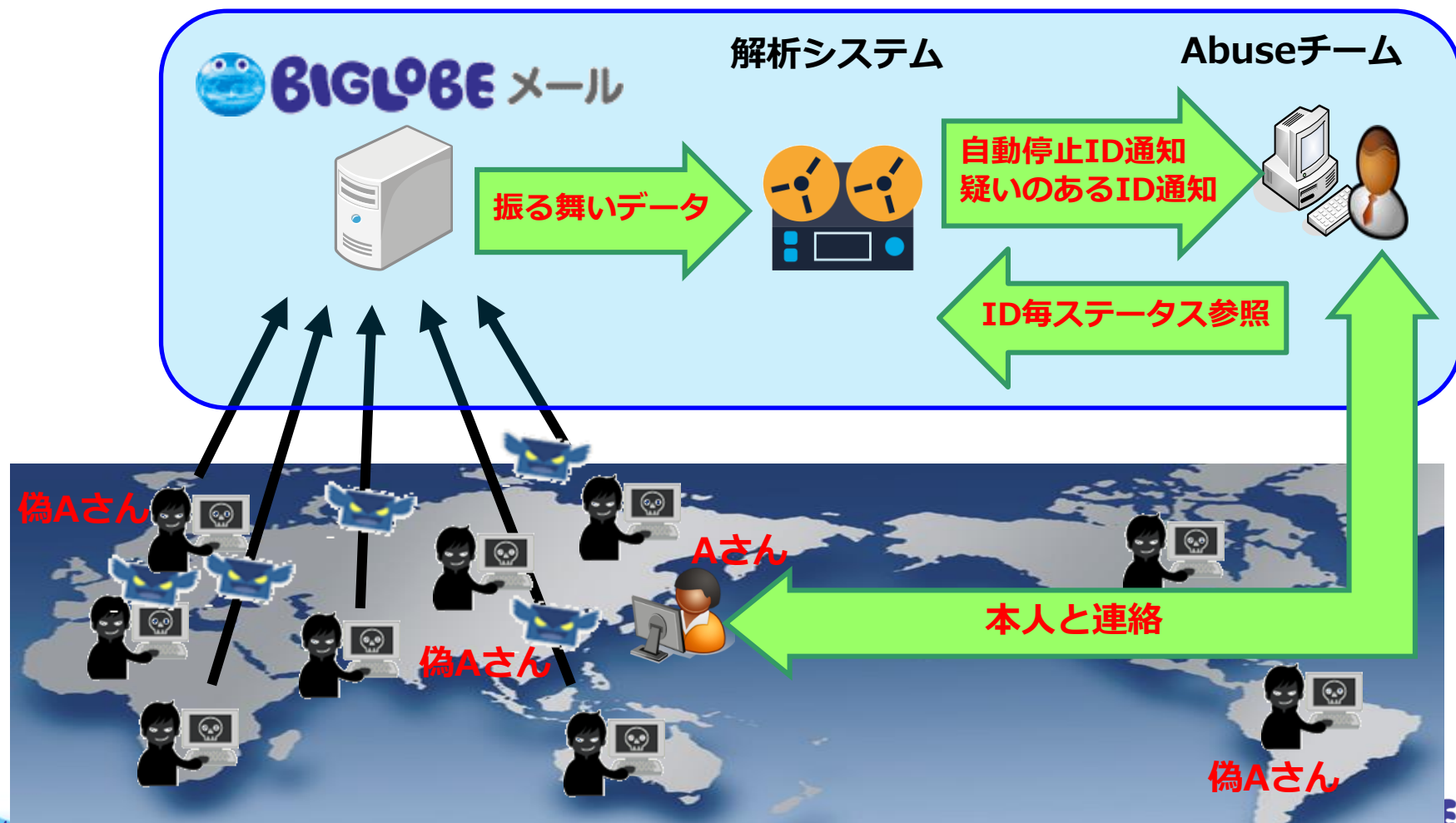
◆ 傾向：送信元の国に偏り

A world map where countries are shaded in various shades of green, representing the distribution of transmission sources. The shading is most intense in North America and Europe, indicating a high concentration of transmission sources in these regions. Other areas like Asia and South America show lighter shades, indicating fewer sources. A white rectangular box with red text is overlaid on the map.

会場のみ公開とさせていただきます

踏み台送信対策その1

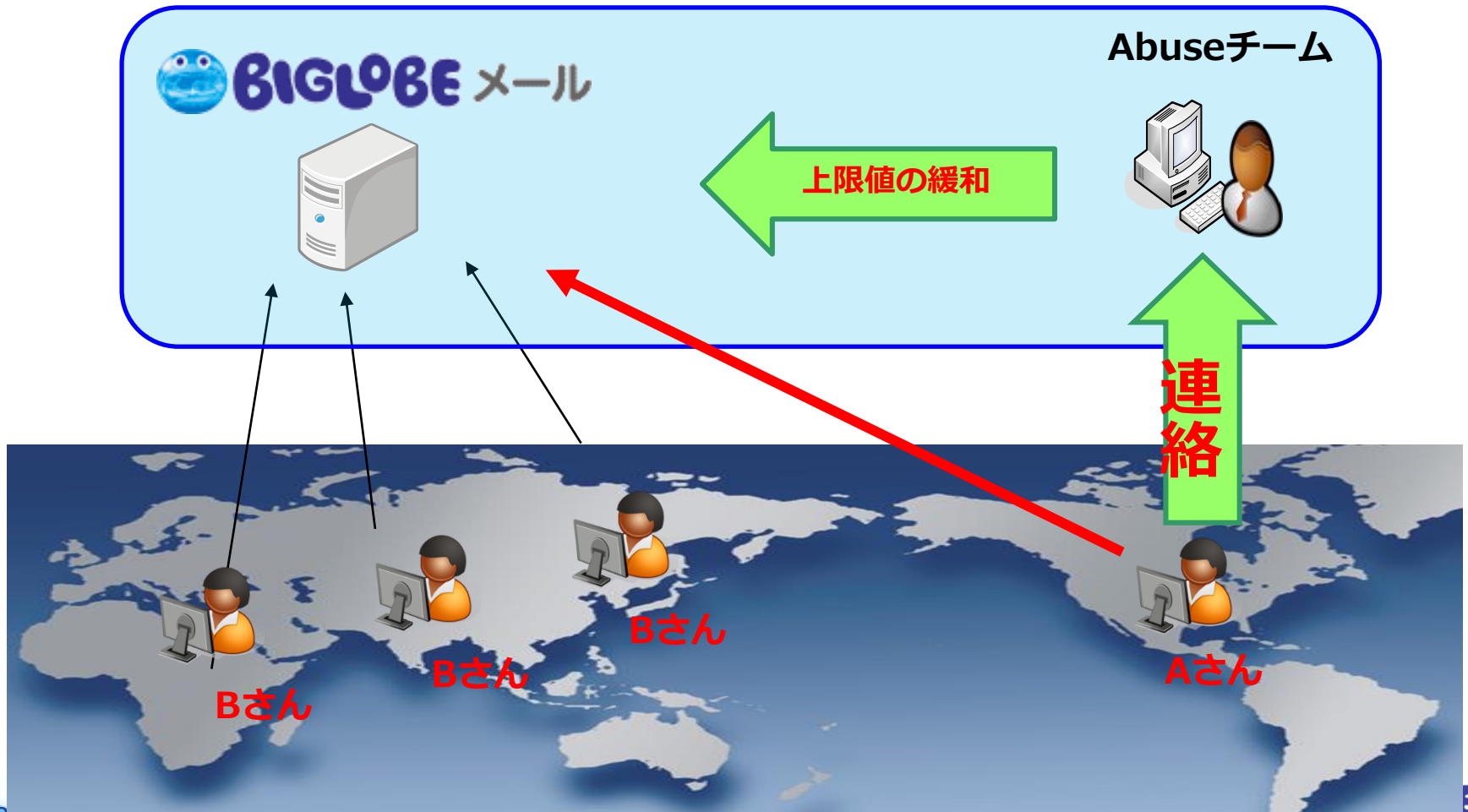
- ◆ アカウント単位に**送信通数制限**、制限越えると**自動停止(送信のみ)**
- ◆ Abuseチームの操作で**強制停止(送信のみ)**、本人へ**連絡**



踏み台送信対策その2

◆ 対策

- 特定の国IPからの送信可能メール数を絞る機能(アカウント単位)
- 正常な送信の影響は回避できるようにアカウント毎に送信上限を変更できる機能を準備



踏み台送信対策の効果 1

踏み台メール送信通数



踏み台送信対策の効果 2

~~④ BlackListに登録される~~

~~⑤ 送信メールの到着が遅延/不達~~



~~③ サーバ高負荷、メール滞留発生~~

~~② アクセス集中で送信しづらい状況~~



正常利用者への影響なし！

