第14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～

取り組み事例②
ニフティ

2016年10月4日 大阪

ニフティ株式会社 伊藤隼人

ニフティ株式会社

アカウント認証の必須化

- OP25B/IP25Bの実施
- 自網内25番投稿、POP before SMTPの廃止

アカウント単位での流量制御

- 単位時間たりの1アカウントでの送信数を制限

IPアドレス単位での流量制御

- 単位時間たりの1IPアドレスでの送信数を制限

これだけでは踏み台問題は解決できない！

不正利用されているアカウントへの対策

- 接続元IPアドレスの国情報を用いた制御
- ユーザーへの通知フローの整備

不正利用を未然に防ぐための対策

- パスワードエラー時の利用制限
- 海外送受信拒否設定

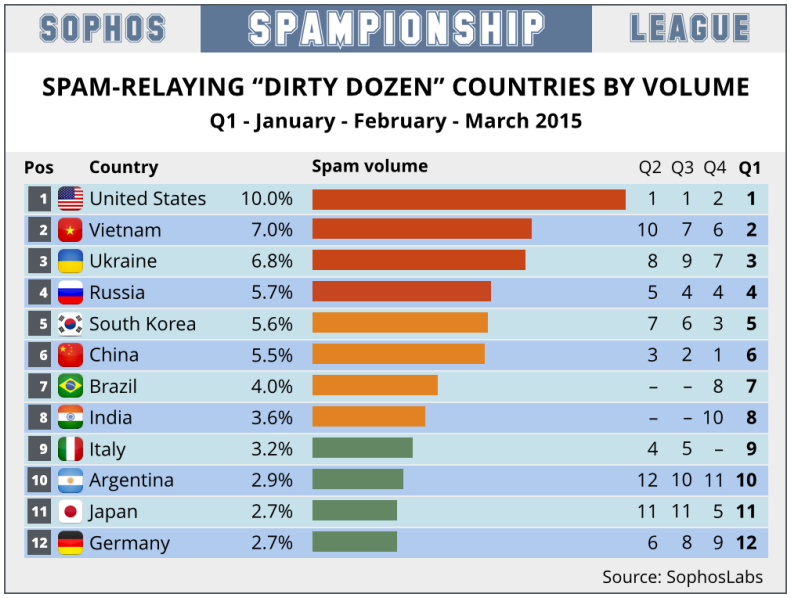
- 迷惑メール大量送信のほとんどは海外から
- 正規ユーザーの送信のほとんどは国内から

国情報に基づいて制限をかけることで多くの迷惑メール大量送信を遮断可能

制限の内容

- 同時送信通数を制限
- Fromアドレスと認証アカウントの一致性を確認

※制限内容は国別に設定可能



SOPHOS SPAMPIONSHIP LEAGUE

SPAM-RELAYING "DIRTY DOZEN" COUNTRIES BY VOLUME

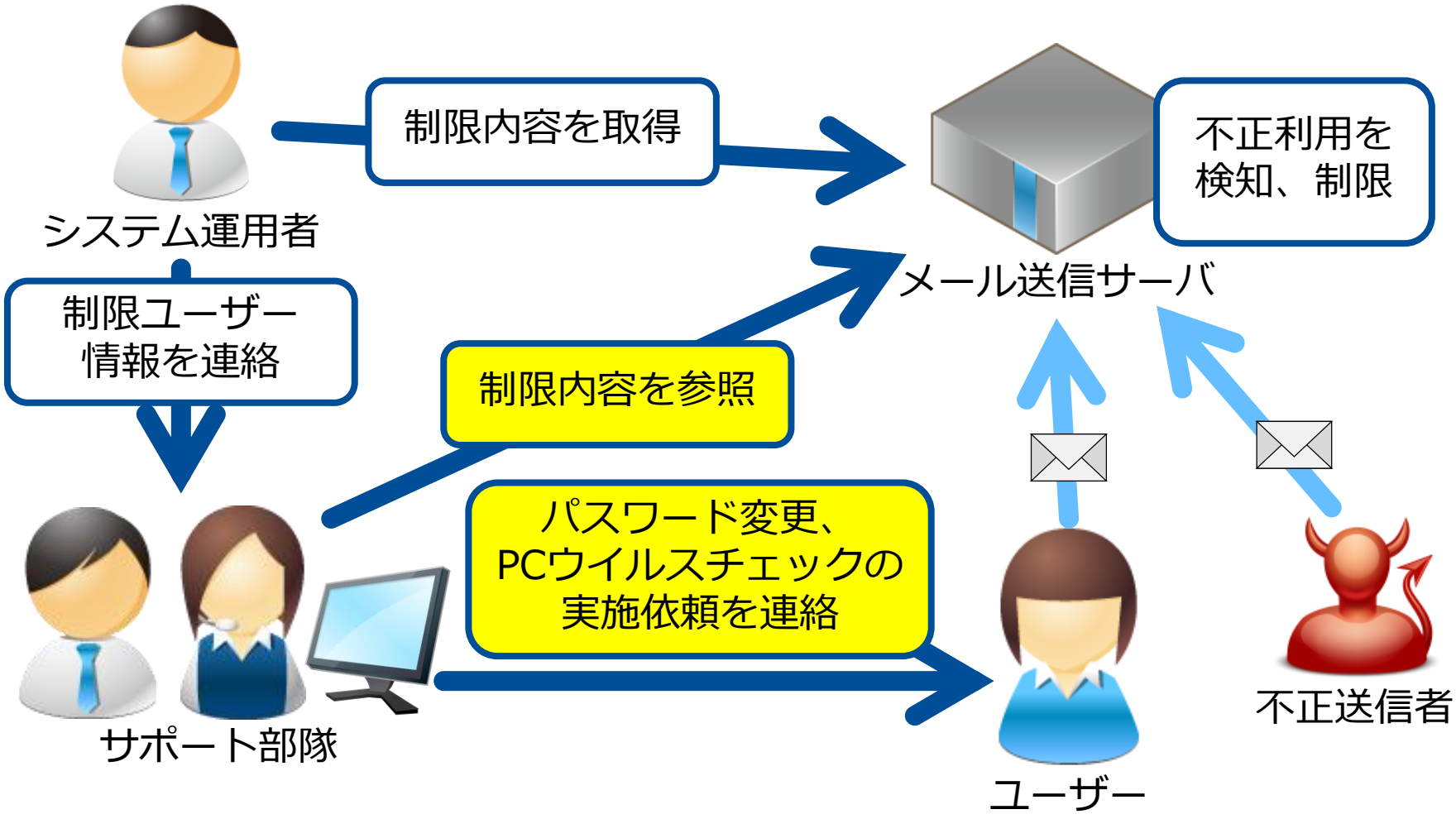
Q1 - January - February - March 2015

Pos	Country	Spam volume	Q2	Q3	Q4	Q1
1	United States	10.0%	1	1	2	1
2	Vietnam	7.0%	10	7	6	2
3	Ukraine	6.8%	8	9	7	3
4	Russia	5.7%	5	4	4	4
5	South Korea	5.6%	7	6	3	5
6	China	5.5%	3	2	1	6
7	Brazil	4.0%	–	–	8	7
8	India	3.6%	–	–	10	8
9	Italy	3.2%	4	5	–	9
10	Argentina	2.9%	12	10	11	10
11	Japan	2.7%	11	11	5	11
12	Germany	2.7%	6	8	9	12

Source: SophosLabs

（naked security by SOPHOS より）

ユーザーへの通知フローの整備



サポート部隊が制限内容を取得しユーザーへ
連絡することで、アカウント不正利用の停止を迅速化

パスワードエラーをカウントし、閾値に達したものは一定時間利用を自動制限

アカウントベースでのカウント
- 辞書攻撃、ブルートフォースアタック対策

IPアドレスベースでのカウント
- リバースブルートフォースアタック対策

海外IPアドレスからの
SMTP/POPを
拒否する設定が
アカウント単位で可能

ユーザーへ
機能として提供

現在はデフォルトOFF

将来的には・・・

デフォルトON

既存アカウントの一括ON

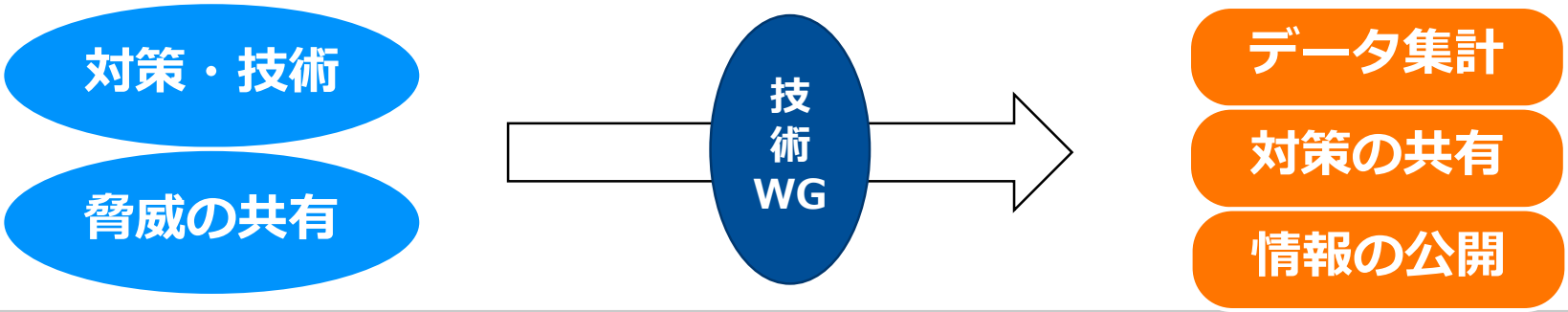
検知した不正利用ID数の推移

９月より、Webメールを用いた大量送信を検知

SMTPサーバーでの制限強化の成果？

2008年11月に発足。送信ドメイン認証普及や迷惑メール対策の普及を目的として迷惑メール対策ハンドブック策定や導入マニュアルを作成。2014年、技術に特化したワーキンググループを発足、月1回程度で活動中。

[引用]　http://www.dekyo.or.jp/soudan/anti_spam/



技術WGで取り扱っているのはこの2テーマを扱っている

DMARC の普及・活用

踏み台問題への対策

各ISPが取り組んでいる踏み台問題への対策を整理
ベストプラクティスとして紹介しよう

代表的な対策を6つ紹介

みんなにも取り組んでもらう

踏み台送信対策の状況（通称：踏み台問題ベストプラクティス）

1

電気通信事業者による迷惑メールの踏み台送信対策の状況（概要）

背景

近年、利用者の送信者IDおよびパスワードが何らかの方法で大量に不正取得され、それらを用いた迷惑メール送信が急激に増加している。言い換えれば、迷惑メールは事業者各社の正規の送信サーバから大量に発信されている。そのため、事業者の送信サーバがブラックリストへ登録されやすく、利用者のメールが届きにくい状況（特に海外宛）が発生している。

このような迷惑メール送信方法は「迷惑メールの踏み台送信」と呼ばれ、SMTP認証や送信トラフィック制御といった従来の迷惑メール対策技術だけでは防止することが困難になっている。ここでは、各社の踏み台送信問題への対策（ベストプラクティス）を共有し、国内のサービス事業者全体で踏み台送信問題に取り組んでいくきっかけとする。

主な対策技術と効果

対策名	対策概要	踏み台送信問題への効果等
①SMTP認証と送信通数制限	送信者IDあたりの送信通数に制限を設ける方法。	すでに導入事例は多く、基礎となる対策といえる。
②送信IPアドレスの分離	送信メールの内容を元にしたレピュテーションを用いて、迷惑メールと判定したメールとそうでないメールを別々のIPアドレスから送信する方法。	ブラックリスト登録の影響範囲を局所化する効果がある。
③接続元情報による制限	接続元のIPアドレスや地域情報を元にしたレピュテーションを用いて、迷惑メール発信元と判定した場合にはペナルティを与える方法。	現在は、海外接続や複数地域からの同時接続が多いため、効果は高い。
④マルチ要素認証	SMTP認証やパスワード認証以外の方法で本人認証を実施し、送信者IDの不正利用を防止する方法。	不正利用の防止効果は高いが、利便性低下が懸念される。
⑤送信者詐称の制限	SMTP認証結果と、送信者情報の一致性を用いて、なりすましを見分ける方法。	効果は高いが、第三者送信による偽陽性も考えられる。
⑥利用者への啓発	不正利用のリスクを伝え、対策を知ってもらう方法。	フィッシングを未然防止する意味で、効果はある。

1 SMTP認証と送信通数制限

2 送信IPアドレスの分離

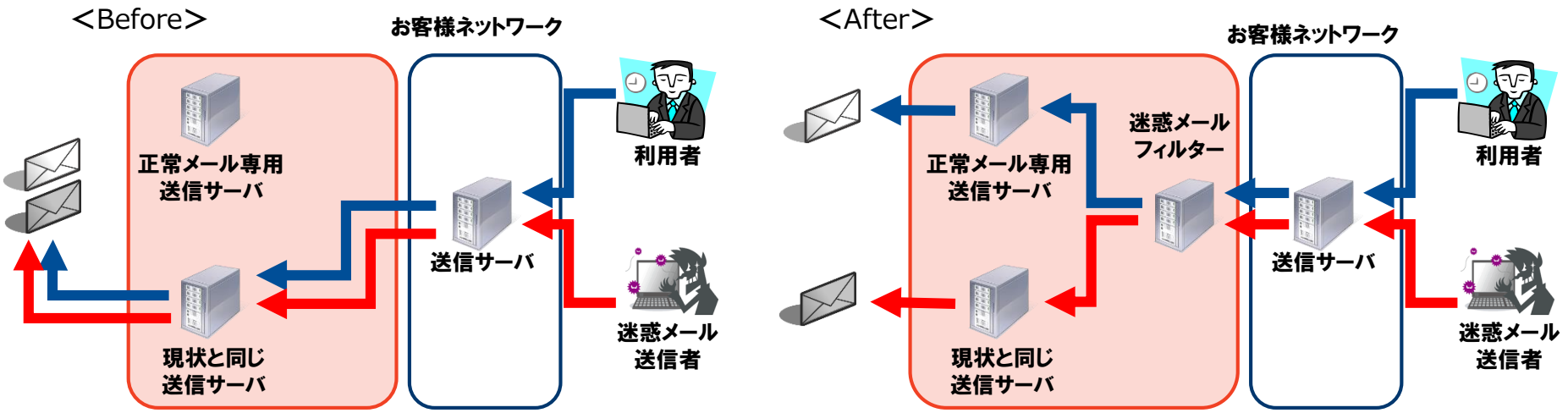
3 接続元IP情報による制限

4 マルチ要素認証

5 送信者詐称の制限

6 利用者への啓発

送信メールのヘッダー情報や本文をもとにして迷惑メールとそうでないメールに**分類**し、それぞれを**異なる送信IP アドレス**を持つ送信サーバから配送し、**ブラックリストによる影響**を局所化する



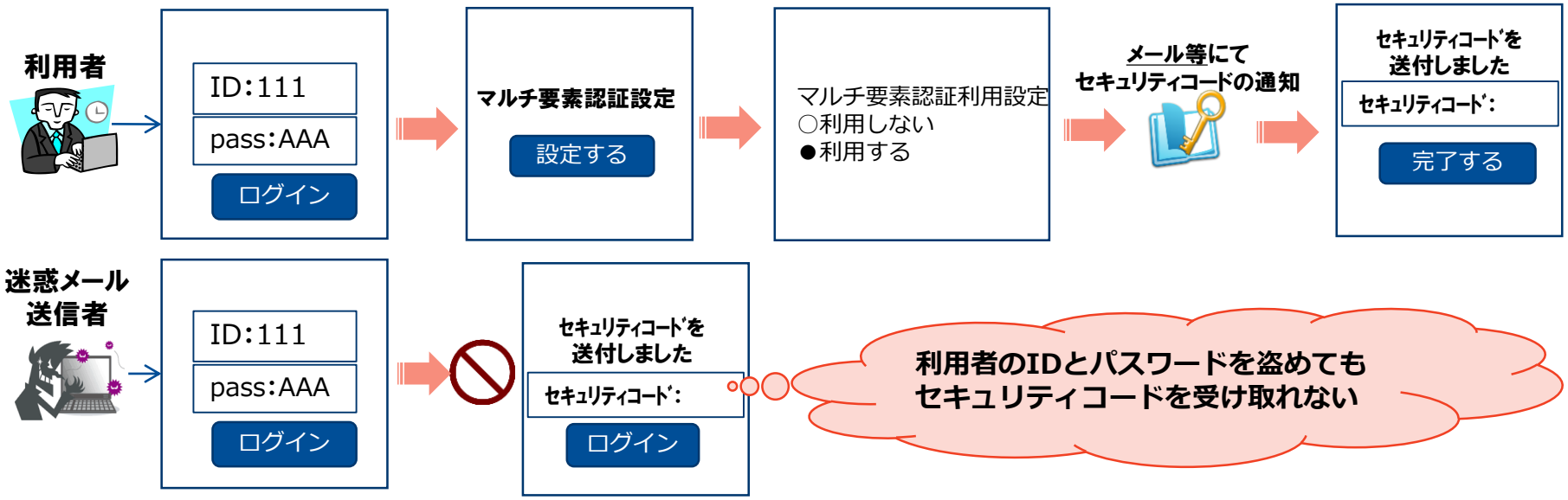
利用者周知
契約見直し

フィルタ実装
MTA準備

導入
(新規契約)

導入
(既存契約)

（Webメールにおいて）従来のパスワード認証の他の認証機構を設けて、**不正利用の難易度を高め**、踏み台送信を防止する



利用者周知 契約見直し → 認証実装 設定ﾍﾟｰｼﾞ実装 → 紹介サイトや告知 → 利用者への導入

踏み台問題への対応状況（10社）

@nifty

1

電気通信事業者による迷惑メールの踏み台送信対策の状況（概要）

背景

近年、利用者の送信者IDおよびパスワードが何らかの方法で大量に不正取得され、それらを用いた迷惑メール送信が急激に増加している。言い換えれば、迷惑メールは事業者各社の正規の送信サーバから大量に発信されている。そのため、事業者の送信サーバがブラックリストへ登録されやすく、利用者のメールが届きにくい状況（特に海外宛）が発生している。

このような迷惑メール送信方法は「迷惑メールの踏み台送信」と呼ばれ、SMTP認証や送信トラフィック制御といった従来の迷惑メール対策技術だけでは防止することが困難になっている。ここでは、各社の踏み台送信問題への対策（ベストプラクティス）を共有し、国内のサービス事業者全体で踏み台送信問題に取り組んでいくきっかけとする。

主な対策技術と効果

対策名	対策概要	踏み台送信問題への効果等
①SMTP認証と送信通数制限	送信者IDあたりの送信通数に制限を設ける方法。	すでに導入事例は多く、基礎となる対策といえる。
②送信IPアドレスの分離	送信メールの内容を元にしたレピュテーションを用いて、迷惑メールと判定したメールとそうでないメールを別々のIPアドレスから送信する方法。	ブラックリスト登録の影響範囲を局所化する効果がある。
③接続元情報による制限	接続元のIPアドレスや地域情報を元にしたレピュテーションを用いて、迷惑メール発信元と判定した場合にはペナルティを与える方法。	現在は、海外接続や複数地域からの同時接続が多いため、効果は高い。
④マルチ要素認証	SMTP認証やパスワード認証以外の方法で本人認証を実施し、送信者IDの不正利用を防止する方法。	不正利用の防止効果は高いが、利便性低下が懸念される。
⑤送信者詐称の制限	SMTP認証結果と、送信者情報の一致性を用いて、なりすましを見分ける方法。	効果は高いが、第三者送信による偽陽性も考えられる。
⑥利用者への啓発	不正利用のリスクを伝え、対策を知ってもらう方法。	フィッシングを未然防止する意味で、効果はある。

1 10/10 SMTP認証と送信通数制限

2 4/10 送信IPアドレスの分離

3 6/10 接続元IP情報による制限

4 6/10 マルチ要素認証

5 6/10 送信者詐称の制限

6 8/10 利用者への啓発

今後の送信対策や送信手口の議論