資料1

活動報告

2015.10.07

技術ワーキンググループ

迷惑メール対策推進協議会

活動記録

- 活動方針
  - 1回/月程度の会合を開催 (長期休暇時期等を除く)
  - 資料は事前に Web で公開し共有
  - 当日はプロジェクタを利用し資料の紙配布をしない
  - 開催場所は各メンバ企業から提供
  - テーマに関係するゲストの参加も可能
  - 迷惑メール対策およびメールシステムに関わる情報共有を積極的に行う
- WG会合実績
  - 第1回 2015.05.25[月] @ 総務省
  - 非公式会合 2015.06.03
  - 第2回 2015.07.07[火] @ 日本データ通信協会
  - 第3回 2015.08.04[火] @ ビッグローブ株式会社
  - 第4回 2015.09.03[木] @ ソフトバンク株式会社

主な検討課題

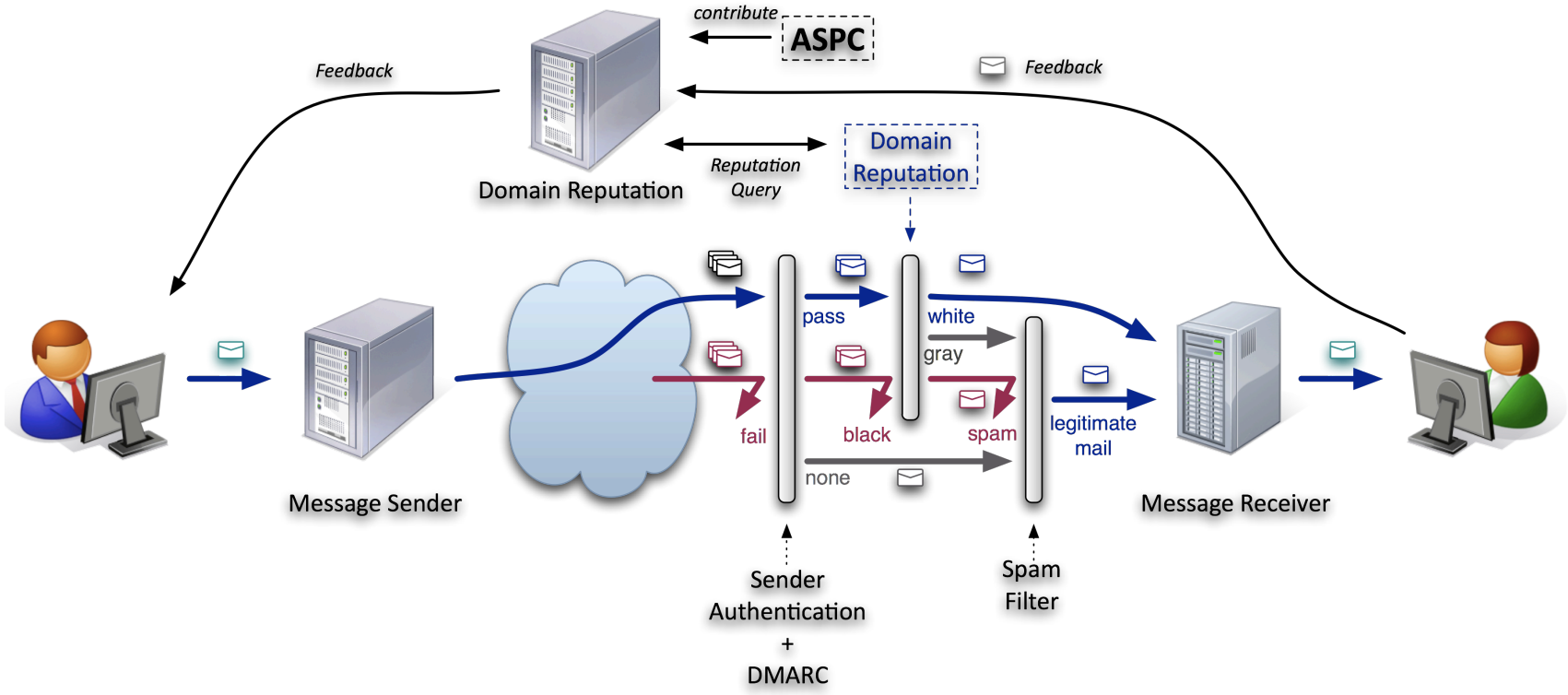
- DMARC + レピュテーション + フィードバック
- 踏み台問題対策
- その他
  - SMS の迷惑メール対策
  - セキュリティ的に好ましくない古いシステムの刷新に関する取り組みの共有 (ex. POP before SMTP の廃止)
  - メールに関連する技術の紹介 (ex. DANE)

背景

- 迷惑メール量は増大していないがセキュリティ的脅威は深刻
  - 各種情報漏洩が継続して発生している
  - インターネットバンキングの悪用による金銭的被害
  - メールによるマルウェア(添付ファイル)の混入
  - メールによる危険なWebサイトへの誘導でマルウェアのダウンロードや各種脆弱性をついた攻撃による感染
- メール送受信環境改善の必要性
  - 受信側対策の強化により必要なメールが届きにくい状況に
  - メールはコミュニケーション基盤，ビジネスや防災連絡などにも利用
- 迷惑メール送信対策強化の必要性
  - 日本がspam送信国として上位
    - Sophos 社 Dirty Dozen (11位, 2015Q1:1月-3月)
    - Spamhaus による The World's Worst Spam Enabling Countries (5位, 2015.09.16)
- 送信ドメイン認証技術の普及
  - 送信側(SPF)の導入率が高い一方で受信側で認証しているISPが少ない
  - 送信ドメイン認証を導入していてもその認証結果がうまく利用されていない

DMARC+レピュテーション+フィードバック

全体構成



DMARC+レピュテーション+フィードバック
各構成要素

- メール送信者
  - メールの送信元，メールサービス事業者等のメールサーバを経由してメール受信者へ配送される
  - 委託によりメール配信をおこなう送信事業者も含まれる
- メール受信者 (事業者)
  - 特定のドメイン宛のメールを受信
  - メール利用者との契約に基づき不要なメールを排除するなどのフィルタリング機能を提供
- メール受信者 (個人)
  - 最終的なメールの受け取り手
  - 受信したメールが必要であるかどうかを判断できる存在
- ドメインレピュテーション
  - メール受信者 (個人) からの不要なメールや購読解除の通知を受けて協力関係にある(通知に対応可能な)送信事業者への連絡を行う
  - 適切な対応を実施可能なメール送信者をホワイトリストとしてメール受信者に情報提供を行う (ブラックリストの提供はオプション)

課題

- 受け取るべきメールの判断
  - 普及した送信ドメイン認証技術(SPF/DKIM)を利用した統一的な認証技術を利用して受け取るべき送信者を判断できるように → DMARC
  - 受け取るべきメールが事前に明らかになればspam filterの判断基準を上げることも可能 → レピュテーション(ホワイトリスト)
- 迷惑メール送信対策
  - 認証(SMTP-AUTH)してメールサーバを利用してもPCがマルウエアに感染して乗っ取られている場合もある → 踏み台問題対策，フィードバック
  - 悪意を持った利用者(認証IDの不正入手，悪用者)のメールサーバ利用対策(緊急避難的なものを含む) → 踏み台問題対策，フィードバック
  - 迷惑メール送信が明らかになれば緊急的にメールサーバ利用の停止や送信依頼元の判断が可能に(送信代行事業) → フィードバック，踏み台問題対策
- メール利用環境の改善
  - 受信したメールが不要であることを安全に通知しopt-outできるように → フィードバック
  - opt-out できない送信元に関する不要通知は受け取らないように → レピュテーション，フィードバック

技術WGの検討内容

- DMARC+レピュテーション+フィードバックの検討
  - 各構成要素(送信者，受信者，レピュテーション)の果たすべき役割の整理
  - 各種仕様(DMARC, フィードバックのための ARF，レピュテーションプロトコル, etc) の調査と利用部分の整理
  - レピュテーションの有効性の検証
    - 明らかなホワイトリストドメインおよびブラックリストドメインの収集
    - ログ等を利用して誤判定(False Positive/Negative)がどれだけ救えるかを調査
  - 普及のためのそれぞれへの働きかけ
- 踏み台問題対策
  - 各社で実施しているあるいは検討している施策の共有と有効性の検討
  - 有効な対策の集積 → ベストプラクティス
- 法的留意点
  - 各技術や対策を実施するにあたり法的に留意すべきポイントの洗い出し
  - 抽出したポイントの解釈や整理については別途検討 (WG 外で)

DMARC+レピュテーション+フィードバック
各構成要素の役割

- メール送信側
  - SPF/DKIM の導入
  - DMARC レコードの宣言
  - フィードバックの受信と対応 (opt-out, 一時利用停止, 各種対策)
- メール受信側 (事業者)
  - SPF/DKIM の導入 (受信側認証)
  - DMARC の認証
  - ドメインレピュテーション利用による配送判断 (各社それぞれが利用を判断)
  - フィードバック機能の提供 (Webメールのspamボタン，購読解除ボタン等)
- メール受信者 (個人)
  - 不要なメールの報告 (フィードバック)
- ドメインレピュテーション (フィードバック受け元)
  - 受信側の要求に応じてドメインに対するレピュテーションを提示
  - メール受信者からのフィードバックを受信
  - 必要に応じて送信側にフィードバックを行う

DMARC+レピュテーション+フィードバック
要件整理(例)

- メール送信側
  - SPF 及び DMARC レコードを宣言
  - SPF が fail するような場合には DKIM を導入 (できれば必須としたいが)
  - DMARC が fail しないようなヘッダを設定
    - RFC5321.From と RFC5322.From の一致
    - もしくは　Identifier Alignment となるドメインであること
  - 送信メールの発信者及び宛先を管理できること
    - SMTP-AUTH や 送信依頼元による発信者管理
    - ログ等による宛先と日時情報の一定期間保持
  - フィードバックを受けた場合に適切に管理できること
    - opt-in メールの送信で不要と申告された場合には opt-out 手続きを行う
    - 迷惑メール (spam) と申告された場合には送信者を特定し，一時的に認証 (SMTP-AUTH) を不許可とし，迷惑メールが送信されないような対応を行うこと (PC の cleanup 等)
    - 悪質な送信者である場合 (故意に大量送信を行っている場合等) には契約者情報を共有し他事業者で利用できないような対応について検討 (別途)
- メール受信側
- ドメインレピュテーション

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。さらに、迷惑メールは各社の正規の送信メールサーバから発信されるため、ブラックリストへ登録されやすくなり、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、日本全体で踏み台送信問題に取り組む。

主な対策技術と効果

対策名	技術の概要	踏み台送信への効果
SMTP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。	大量の不正利用には効果が薄小さい。
送信時コンテンツフィルタリング	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にはペナルティを与える方法。	効果は高いとみられる。
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。
送信IPアドレスの分離	なんらかの方法でペナルティが与えられたメールと、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限定できる効果がある。
マルチ要素認証	SMTP認証以外の方法で本人認証を実施し、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。
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。
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。

各社の導入事例紹介（A社： 送信元情報による制限）

対策概要

海外からのメール送受信を禁止する選択機能を利用者に提供、海外からの不正利用を低減する

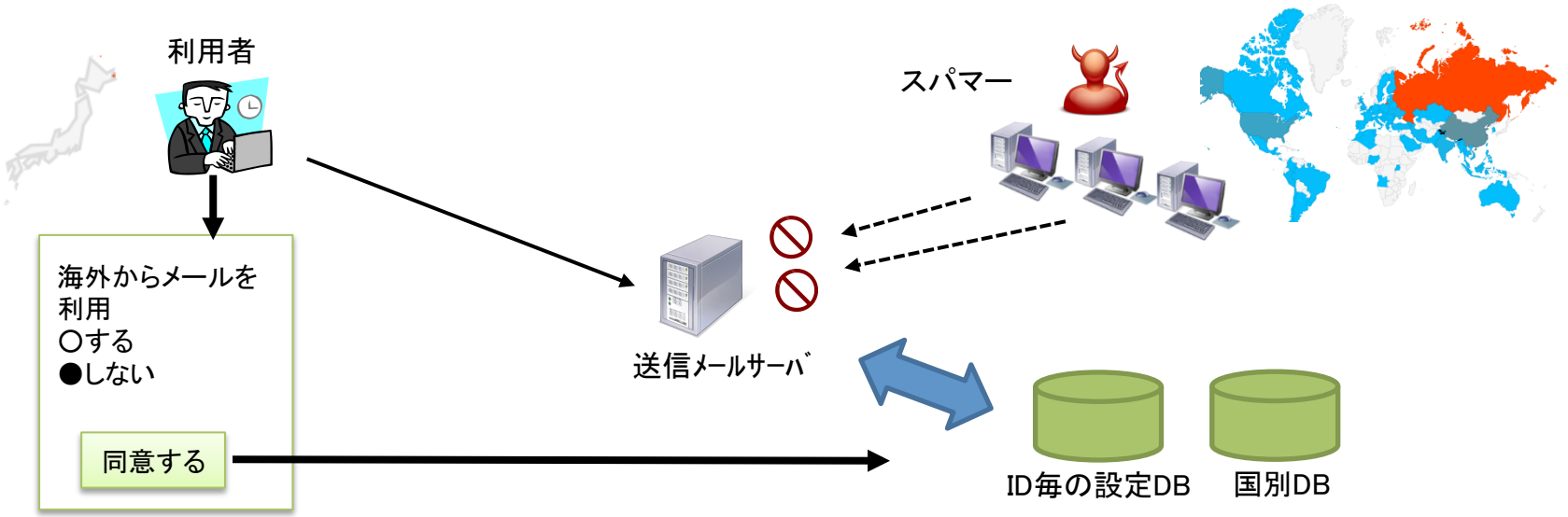
導入時期

2014年10月 （準備期間： 4か月）

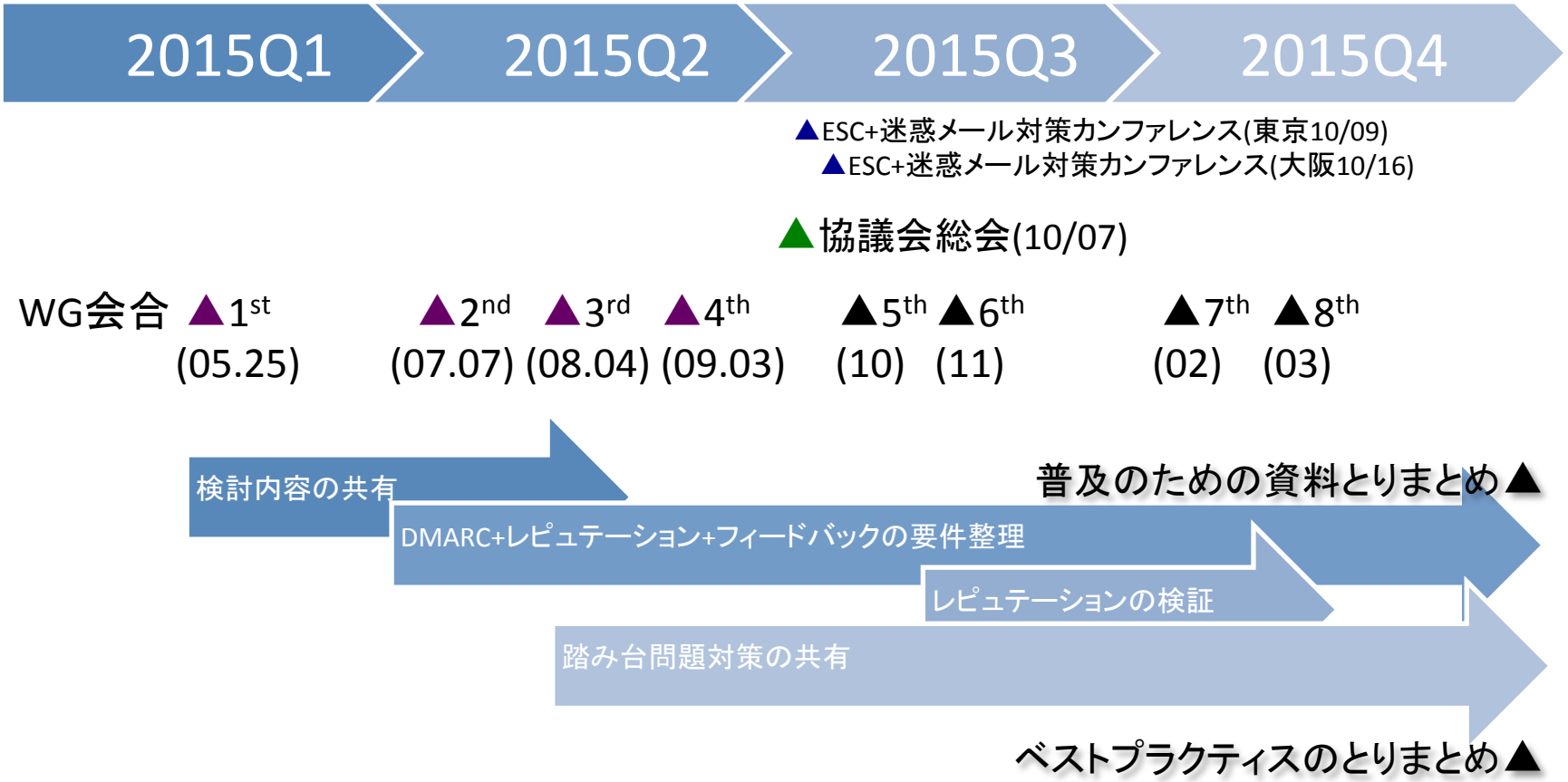
導入準備

1. 国別情報のデータベース化（最低限、日本国内と海外の区別ができる仕組み）
2. 送信メールサーバプログラムの修正（例 判定プログラムのMilter化）
3. ID毎の設定変更ウェブページの作成（例 海外からの接続許可： ON／OFF）
4. カスタマーサポートへの周知
5. サービス提供

図解



スケジュール


2015Q1
2015Q2
2015Q3
2015Q4
▲ESC+迷惑メール対策カンファレンス(東京10/09)
▲ESC+迷惑メール対策カンファレンス(大阪10/16)
▲協議会総会(10/07)
WG会合
▲1st (05.25)
▲2nd (07.07)
▲3rd (08.04)
▲4th (09.03)
▲5th (10)
▲6th (11)
▲7th (02)
▲8th (03)
検討内容の共有
普及のための資料とりまとめ▲
DMARC+レピュテーション+フィードバックの要件整理
レピュテーションの検証
踏み台問題対策の共有
ベストプラクティスのとりまとめ▲