第44回 M^{3}AAWG から

～日本の皆様へ最新情報をお伝えします～

Vade Secure K.K.

伊藤 美佳

アジェンダ

- 2018 JD Falk Award “BEC List”
- 本セッションでお伝えしたいこと
- パネリストの紹介

パネルディスカッション

テーマ①

M³AAWG の印象と議論されているトピックの紹介

テーマ②

最近話題のトピック AI、BEC

テーマ③

JPAAWG への期待

今後目指す形

- M^{3}AAWG と連動して、JPAAWG として活動する内容を検討
- M^{3}AAWG に参画し、日本からの情報を発信していく
- アジア地域におけるリーダーシップを実現する

詳細は、以降のセッションで具体的にディスカッションを予定

初めてM³AAWGに参加してみて

JPCERT コーディネーションセンター
インシデントレスポンスグループ
中井 尚子

カンファレンスに参加するきっかけ

- APRICOT2018 で M³AAWG の方にお会いし、JPAAWG の活動が始まると説明があった
- M³AAWGの方との話の中で、JPCERT/CC として M³AAWG に参加することで、活動の場が広げられるというメリットを感じた
- M³AAWGというコミュニティを調べました
  - 公開情報(M³AAWGウェブサイト)
  - M³AAWG の参加組織にヒアリング (IIJ社)
  - 海外カンファレンスでM³AAWGの会員という方からの情報収集
- 結果：実際に、カンファレンスに参加してみないとM³AAWGの活動は理解できない

  →参加してみました

初参加で感じたこと

- M^{3}AAWGは、問題解決のために活発に議論し、会話を大切にするコミュニティ
- 印象的なのは、意見を言うのは自由だが、他の方の意見をJudgeするのはダメという点
- 新しいことへのチャレンジ力もある
- 縦割りの関係はなく、フラットでCEO だろうが、リバースエンジニアをする方だろうが、気軽に会話ができる

意外に身近なM^{3}AAWGの活動

- GDPRの施行に伴い、従来の whois 情報公開の目的を果たせなくなるなどの懸念点を FIRST, APWG とともにICANNにコメントを出している
- 日本にいて、 M^{3}AAWGというワードを耳にする機会が少ないが、活動の趣旨は身近で、成果も日本のコミュニティに反映されている
- 特定のプロトコルの標準化に向けた活動

JPAAWGに期待すること

- JPAAWG メンバーの意見をM^{3}AAWG に反映またはその逆も
- M^{3}AAWG 初参加組織に対するサポート
  - 例えば発表枠の調整など

M³AAWGについて

東京農工大学
北川　直哉

学術系(学会)とM3AAWGとの違い(私感)

- 「研究成果発表の場」の学会と「議論する場」のM3AAWG
  →少なくともメッセージング分野では，議論の場は M3AAWG > IETF

- 欧米と日本における産業界とアカデミアの距離感の違いも大きい
  →産学連携がなければ実現しないものも多い
  (研究へのデータ活用など)

- 理論系ではなく実際の運用を意識した研究活動の紹介や議論が多い

- メッセージングとセキュリティに特化しているので興味深いセッション多数
  (学会は「ネットワーク」「セキュリティ」のように取り扱い分野が広い)

IDN(Internationalized Domain Names)のHomograph対策

- 44th M3aawg @NY でも “Real time detection of IDN-based homograph abuse” でも有名サイトのホモグラフ問題が話題に
- 従来の「oと0」や「mとrm」等よりもパータンが爆発的に増加
  →「aとa(U+0410)」「ｂとｂ(U+0423)」「cとｃ(U+0421)」…
- Passive DNSによる調査では約1.6億のIDNが存在(キリル文字の利用が40%)
- Homograph IDNを6.1万ドメイン観測
  - 20%が銀行や金融機関を偽称，52%が.com利用，68%がUS向けに使用
- 1日に1.5万の新IDNが登録
- エンドユーザ，管理者，レジストリ/レジストラはどう対応していくべきか？

M^{3}AAWG とはどんな感じのワーキンググループか

TwoFive Inc.
Masaki Kase

[How] どうやって貢献・参加するか

- メンバー/サポーター/ゲスト
- General Meeting/メール/ML/テレコン
- ビジネスミーティング/朝食/ランチ（BoF）
- パネル/レビュー/Open Round Table
- UCENet（旧LAP）

[What] 何の議論がされているか

- M3AAWG #44 @ブルックリン
  - 米国や欧州でのアクション進捗状況を共有
  - Technical WG セッション
  - Connected Device に関するセキュリティ課題
  - 攻撃方法別のセキュリティ対策検討セッション
  - etc

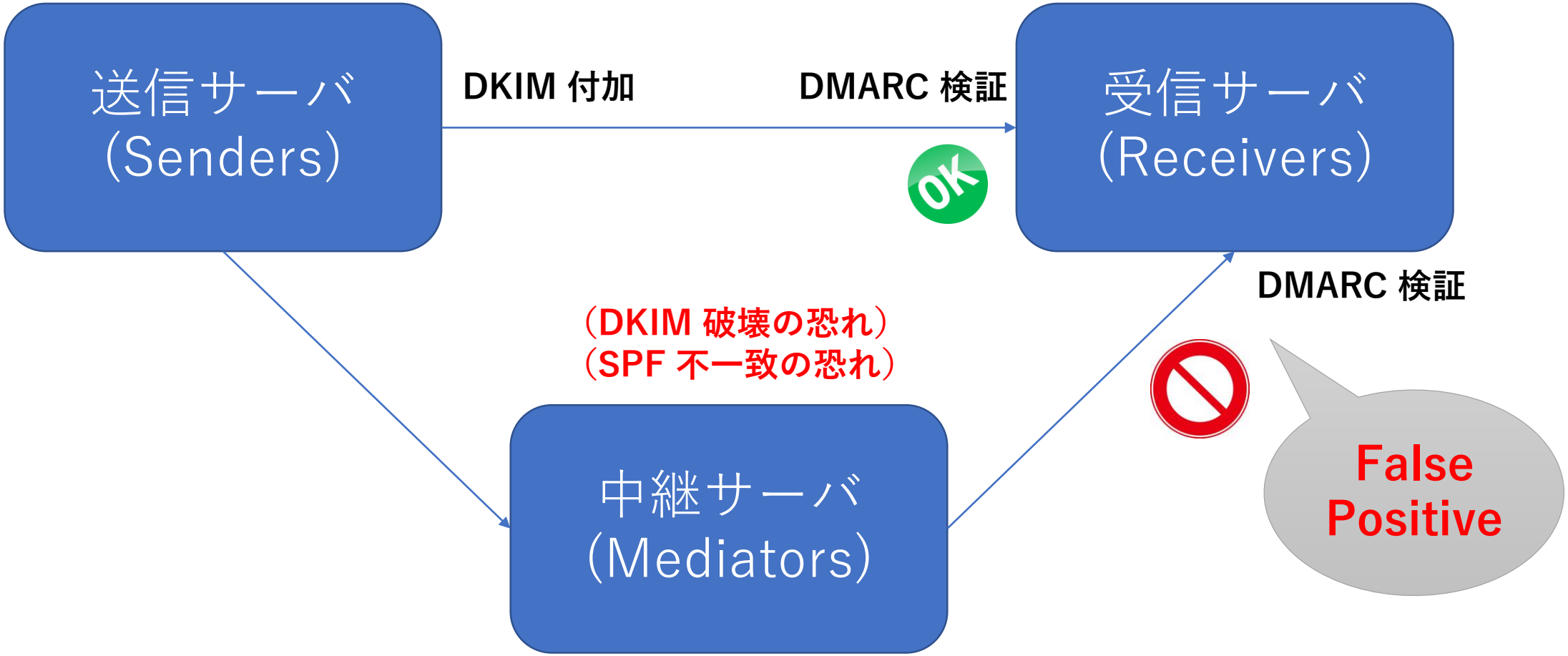
ARC とその実際

- 主にML（中継者）による DMARC 失敗を防止する技術
- ARC はそれ自体では、コンテンツの安全性を担保したり、レピュテーションスコアを提供するものではない
- 認証結果を伝播させるだけ
- DMARC の破壊の原因となる Mediators で実装することが必要
- 一方で、レピュテーションや救済リストと組み合わせた運用が必須

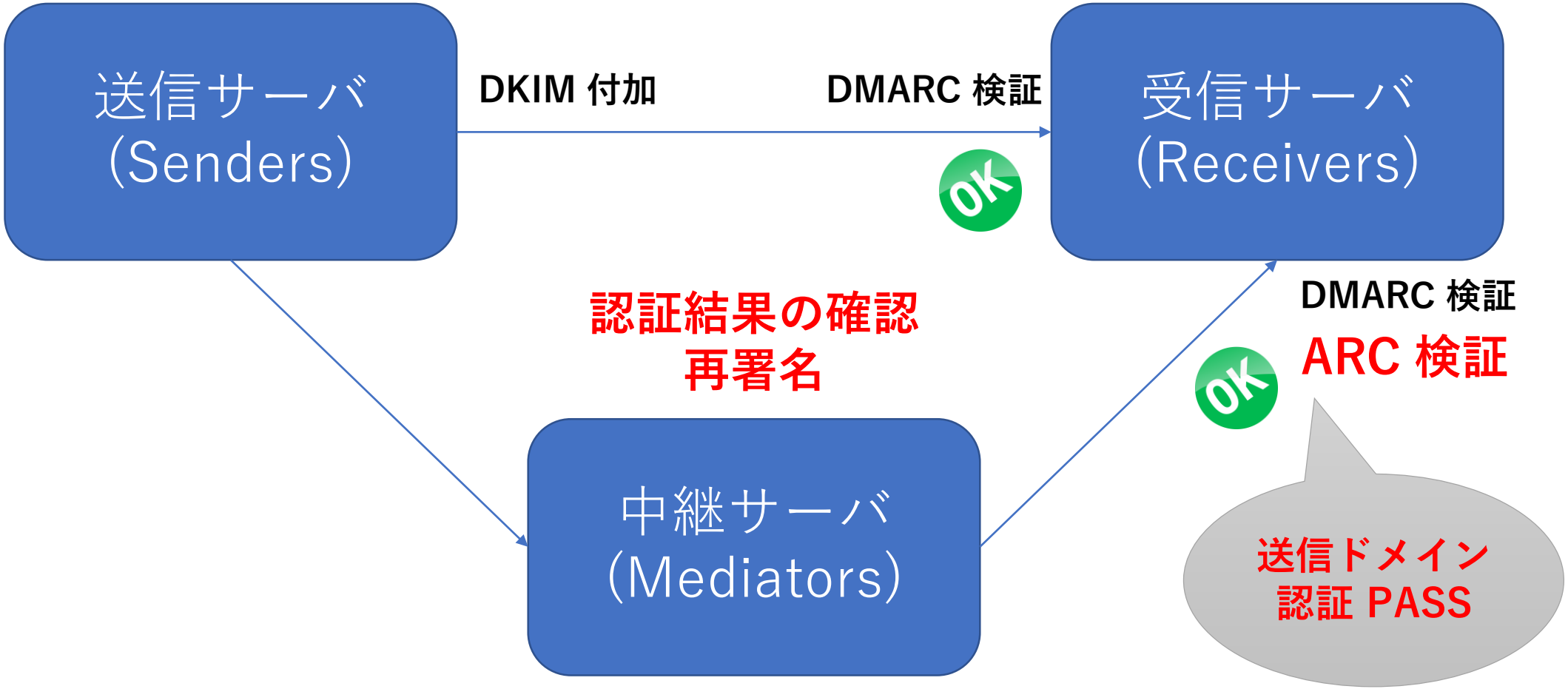
ARC 情報

- ARC プロトコルについて
  - draft-ietf-dmarc-arc-protocol-18
- ARC 利用について
  - draft-ietf-dmarc-arc-usage-06

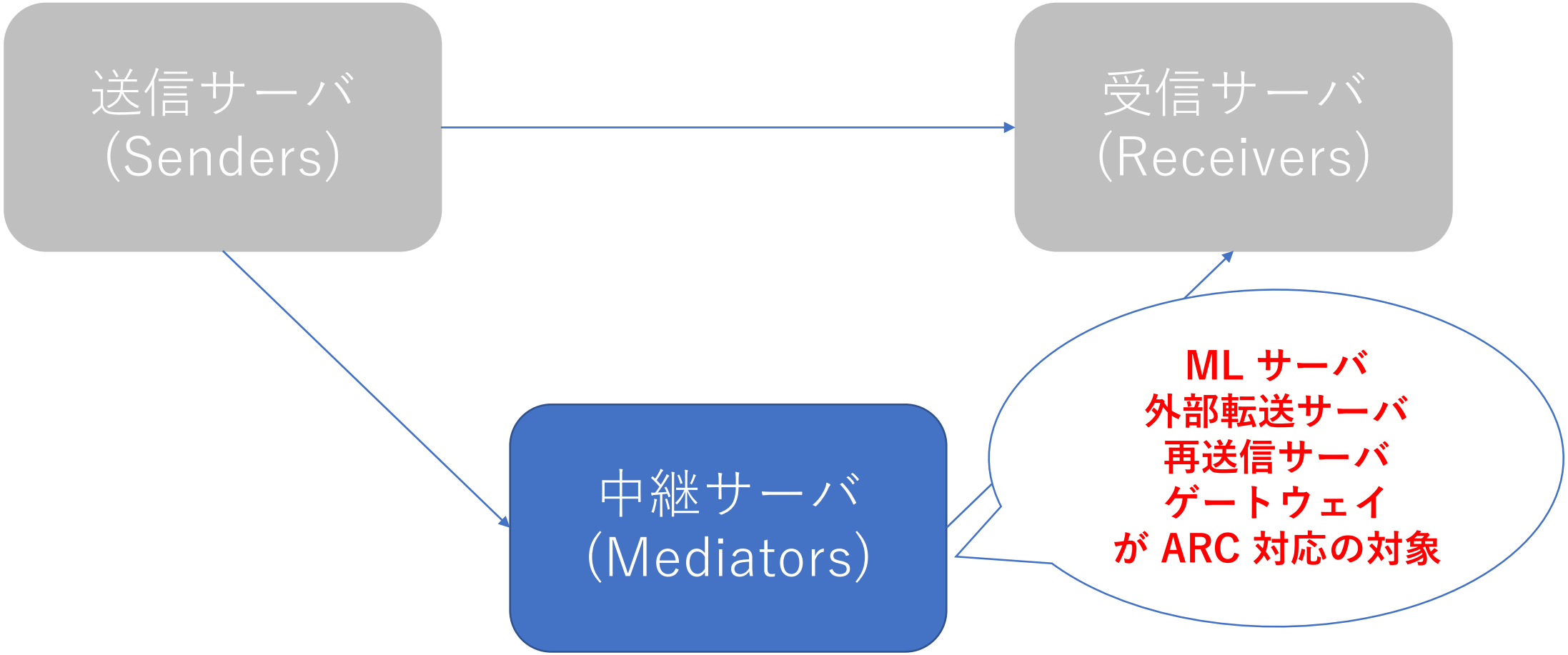
ARC システム


送信サーバ
(Senders)
DKIM 付加
DMARC 検証
OK
受信サーバ
(Receivers)
DMARC 検証
(DKIM 破壊の恐れ)
(SPF 不一致の恐れ)
中継サーバ
(Mediators)
False
Positive

ARC システム


送信サーバ
(Senders)
DKIM 付加
DMARC 検証
OK
受信サーバ
(Receivers)
認証結果の確認
再署名
DMARC 検証
ARC 検証
OK
中継サーバ
(Mediators)
送信ドメイン
認証 PASS

ARC システム（中継サーバ）



ARC システム（受信サーバ）