DKIM and DMARC update

Sep 5th, 2013
Takehito Aakgiri

About me

赤桐 壮人 (あかぎり たけひと)

- 楽天株式会社
- DU (開発部) インターネットエンジニアリング推進室
- 室長

About me

2013

?

OP25B

dkim.jp

楽天

Openwave

ぷらら

JEAG

2003

NTT 東日本

※ロゴの使用は許可もらっていないので、テキストに置き換えました

1 前置き

の方が長いです！

テーマの確認

今日のテーマ

DKIM & DMARC

前提

メールのコミュニティ

送信ドメイン認証

メールのコミュニティ

Anti-spam

	名前	説明
1	MAAWG	Messaging Anti-abuse working group。元々は迷惑メール対策に特化した団体。最近は M3AAWG となって、Malware と Mobile にも Scope。2003 年に Openwave や IIJ が中心となり立ち上げ。 http://www.maawg.org/
2	JEAG	Japan Email Anti-abuse Working Group。2004 年に国内の ISP が中心となり立ち上げ。私も発起人の一人。OP25B や SPF の国内への展開など 2006 年くらいまでは精力的に活動。しかし、現在は活動していない（と思う）。 http://jeag.jp/
3	dkim.jp	Japan DKIM Working Group。DKIM の普及を目的として、2010 年に設立。私が初代議長。日本国内における DKIM の普及率を半年で 5% 以下から 30% にした。 http://www.dkim.jp/
4	dmarc.org	DMARC の仕様はここで議論されている。 http://www.dmarc.org/

dmarc.org

DMARC (“ディーマーク”と発音)

- Domain-based Message Authentication, Reporting and Conformance
- 2012年1月30日、電子メール関係の企業、組織で設立 (Sender, Receiver, その他)

※ 発表時はここに web のコピーがペーストされていましたが、起業のロゴが含まれるため、資料からは除外しました。
まったく同じ記述ですので、
http://www.dmarc.org を参照して下さい。

Sender Authentication (送信ドメイン認証)

モチベーション

送信者の「なりすまし」 対策

「なりすまし」 でないメールが分かる

「なりすまし」 メールが見抜ける

Sender Authentication (送信ドメイン認証)

送信者の種類

- Envelope From (RFC5321.From)
- Header From (RFC5322.From)
- Display name

最近の流行り

- Header From を守る

Sender Authentication (送信ドメイン認証)

送信ドメイン認証の種類

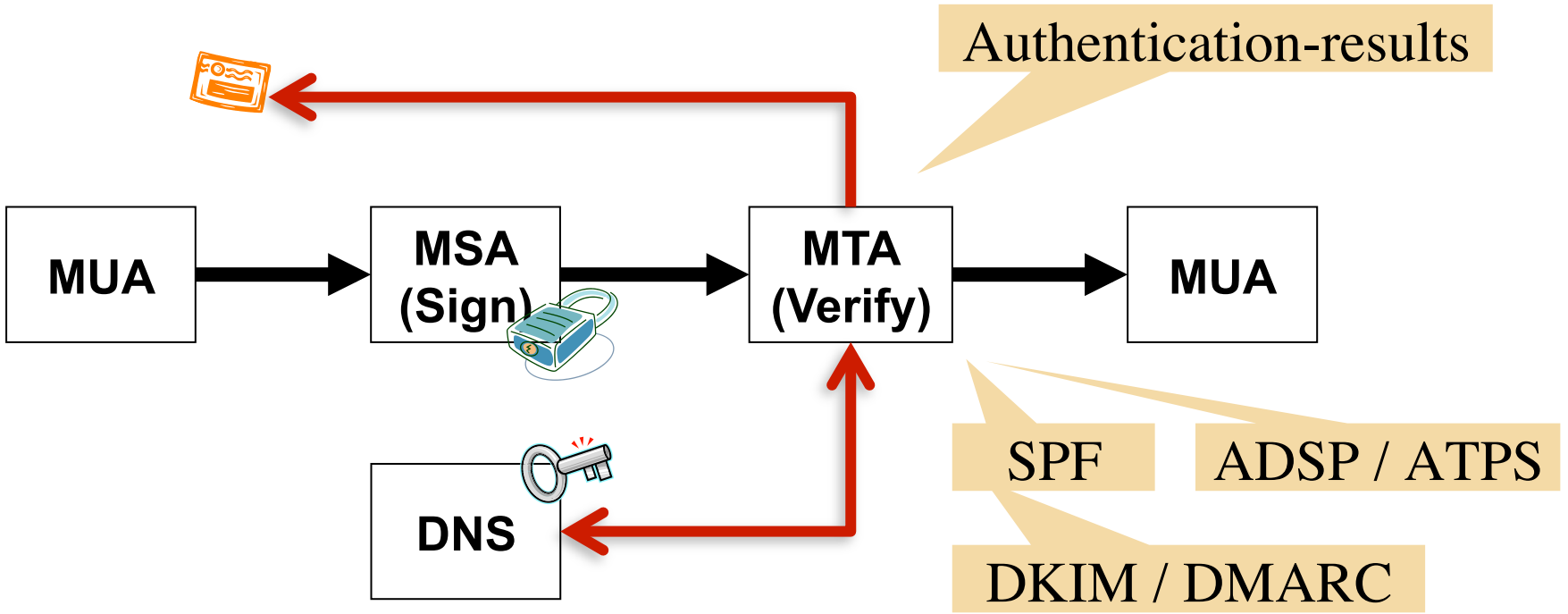
技術	RFC	守るもの	技術の説明	転送	ML
DKIM	6376	d=/Header From	電子署名を利用して送信元ドメインを認証する技術。メール 1 通ずつ対応が可能。作成者署名(Author signature)と第三者署名(3rd party signature) がある	○	△
SPF	4408	Envelope From	送信元の IP アドレスと Envelope From を検証して送信元を認証する技術。	×	○
Sender ID	4406 4407	SPF or PRA (*1)	送信元の IP アドレスと (*1) を検証して送信元を認証する技術。Microsoft が提唱してが、当初、IPR を主張したため総スカン状態。しかし、日本では Au や DoCoMo が採用。DoCoMo は PRA を From にしか適用しない。	○	○

(*1) Envelope From, Header From, Resent-sender, Resent-header のうちどれかひとつ

Header From を守る

DKIM (Author signature)

DKIM/DMARC



技術	RFC	タイトル
Authentication-results	5451	Message Header Field for Indicating Message Authentication Status
ADSP	5617	DomainKeys Identified Mail (DKIM) Author Domain Signing Practices (ADSP)
ATPS	6541	DomainKeys Identified Mail (DKIM) Authorized Third-Party Signatures

DMARC

http://www.dkim.jp/dkim-jp/wp-content/uploads/2013/06/DMARC201304.pdf

Header の例 (DKIM)

Header

From: =?ISO-2022-JP?B?GyRCM1pFNyVsJXMlPyVrJUslZSE8JTkbKEI=?=
rental@emagazine.rakuten.co.jp
…
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
d=emagazine.rakuten.co.jp; s=rkrm0220130400; t=1378280707;
bh=TpMjNSlv17RLwb5xYhUCbjlX+c/lPrMrGdZYCSpJfIg=;
h=Content-Type:Content-Transfer-Encoding:MIME-Version:From:To:
Subject:Message-ID:Sender:Date;
b=U6KJ2MU2ByiCWvpfvE1BdChIUlzyN8Kes5lNZnHii8aa6rJmFaTtlFZ0UGldyVKsq
XEMQ5/E87e3LyaxwHMeVA7khtBtNHhol++5YVnor51oOhgeMmEjiWL1mvb9aJK4LLZ
UXAYX/u9R+tBHHGKcZ9y2Dmdv3W8H0zbZRLiQ08Q=

Record の例 (DMARC)

DNS TXT RR

rkrm0220130400._domainkey.emagazine.rakuten.co.jp. 3600 IN TXT
"v=DKIM1\; k=rsa\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDDHh0NOXmnEC
+mUYo66dnwfE1x3+Wri8PWEWHf0difywbaGH/
IlQB7RL86sWvuyfWYeMbxDXgR3CcJVAL4iQU2ieF3M3TfiQdD8EHywXjca
+4zAH3nF2lFBqbn/
Ou1M2NXw8BKnLG5LaZ1NBgFdus6THcIckY3Xrp7qfqh1C8lpwIDAQAB"

ADSP

_adsp._domainkey.emagazine.rakuten.co.jp. 3600 IN TXT "dkim=all"

DMARC

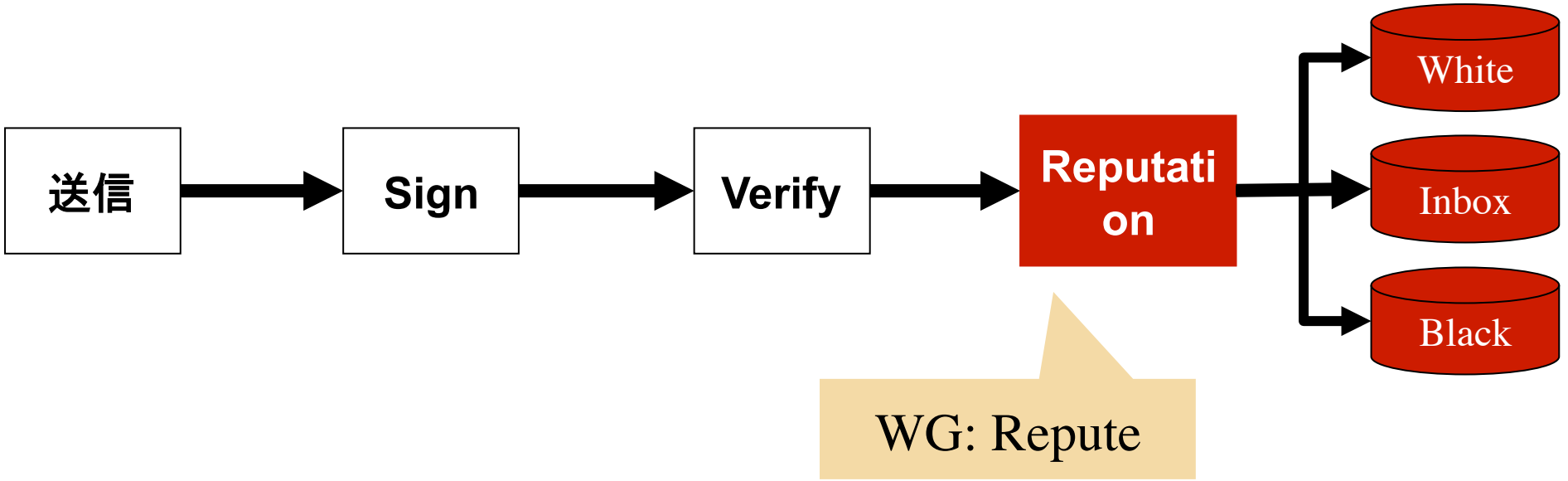
_dmarc.emagazine.rakuten.co.jp. 3579 IN TXT "v=DMARC1\; p=none\;
rf=afrf\; rua=mailto:dmarc-report-a@rx.rakuten.co.jp\; ruf=mailto:dmarc-report-
f@rx.rakuten.co.jp"

検証結果

Authentication-results

Authentication-Results: mta527.mail.kks.yahoo.co.jp
from=mkrm.rakuten.co.jp; domainkeys=neutral (no sig); dkim=pass (ok);
header.i=@emagazine.rakuten.co.jp

Reputation



2 IETF 87 の報告

まず、はじめに・・・

最近は IETF でメールの議論は
あまりされていません

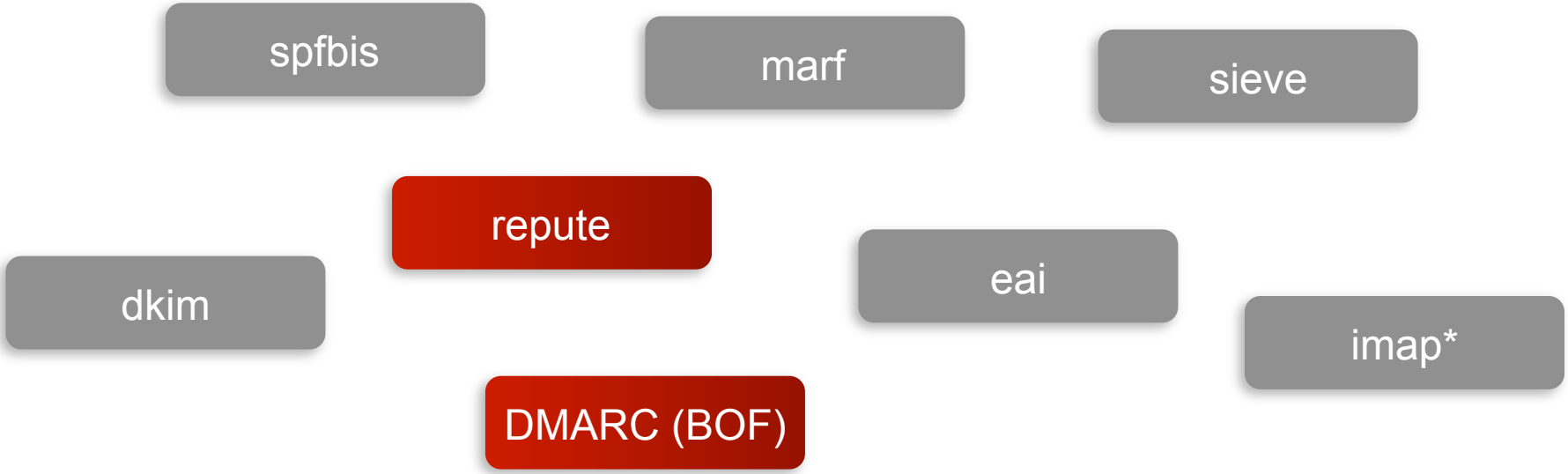
というと言いすぎかもしれませんが・・・

議論の場所

MAAWG や dmarc.org が中心？

これも言いすぎかもしれませんが・・・・

メールに関連する WG



何かが動くと何かが止まる？

最近の私の思い

Player の数が足りないのか？

日本から提案持って行かないと！

Topics (DKIM)

RFC and I-D

- https://datatracker.ietf.org/doc/search/?name=dkim&rfcs=on&activedrafts=on&sort=

Topics

- DKIM が Internet Standard (STD 76) になった (7/12)

- Ischedule のドメインの認証に DKIM を利用する提案 (IETF 86)
  - http://tools.ietf.org/html/draft-desruisseaux-ischedule-05
  - http://www.ietf.org/proceedings/86/slides/slides-86-saag-0

DMARC

RFC and I-D

I-D 名	タイトル
draft-kucherawy-dmarc-base-01	Domain-based Message Authentication, Reporting and Conformance (DMARC)
draft-crocker-dmarc-bcp-02	Using DMARC

https://datatracker.ietf.org/doc/search/?name=dmarc&rfcs=on&activedrafts=on&sort=

Topics

- BoF の開催 (IETF 87)

BCP が Scope (base には Scope しない)

DMARC

BoF

1. Murray (Facebook) から DMARC base の説明

2. Adams (Paypal) から Technical Issue の説明
http://www.ietf.org/proceedings/87/slides/slides-87-dmarc-4.pdf
- Display name, ML, report size, organizational domain

3. Dave Crocker から DMARC bcp の説明
http://www.ietf.org/proceedings/87/slides/slides-87-dmarc-5.pdf
- DMARC の設定の仕方、Policy の厳格化

4. Discussion

DMARC

BoF

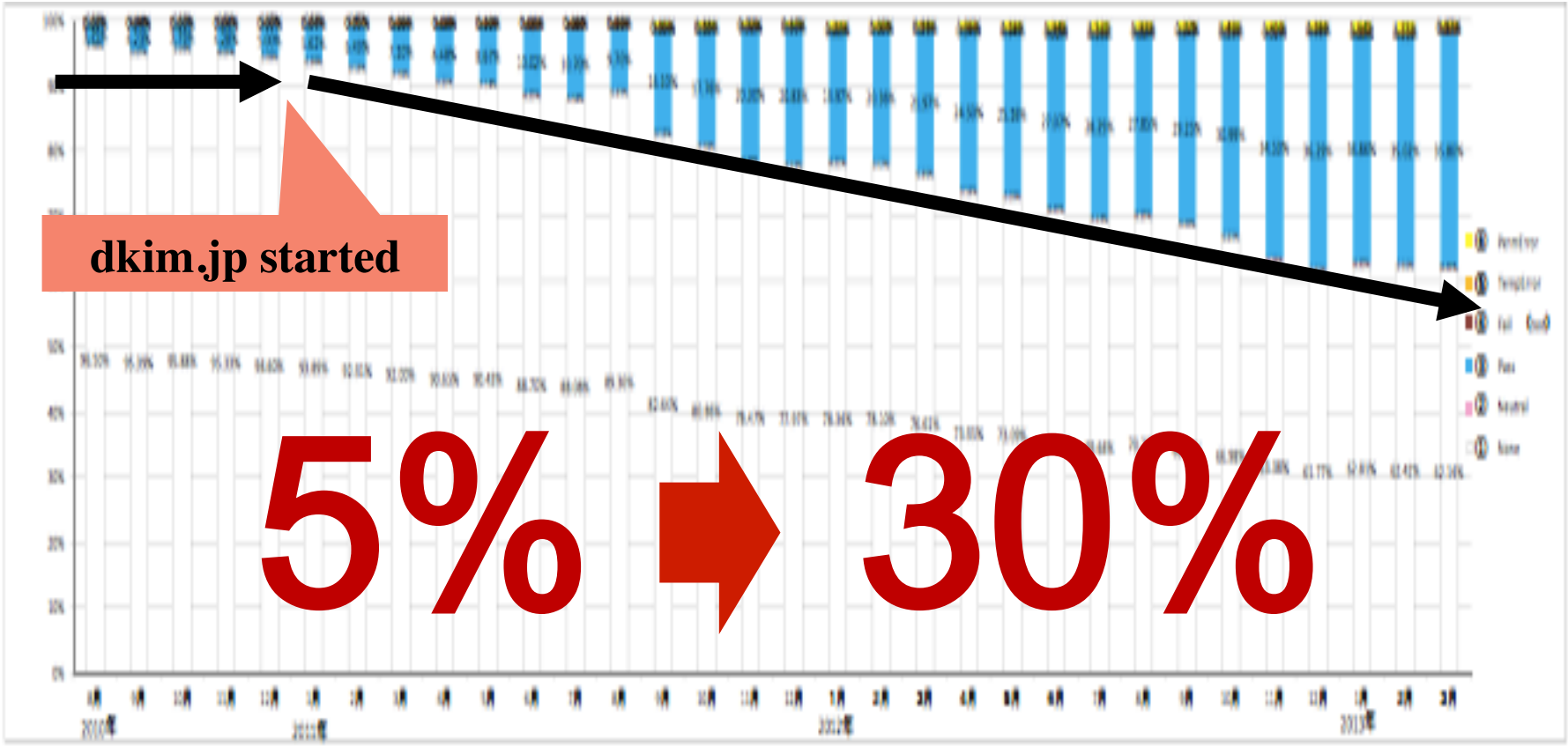
- (背景) DMARC の議論は dmarc.org で実施されている
- Barry は IETF で十分なコンセンサスになるまで base を IESG 取り扱わないと言っている
- Base の議論を「なんでしないんだ！」という意見は出ていた
- 「こんなの BoF じゃない」とか「BCP も dmarc.org でやれ」などの意見もあり
- Display name や ML などの課題について、base を拡張するか提案があったが、（たぶん）out of scope で決着
- 全般的に EAI への言及が多かった（正直、なんでそんなに拘るか分からない）
- 最終的に、base が RFC になるのを待たず、WG を start しようとコンセンサス

http://www.ietf.org/proceedings/87/minutes/minutes-87-dmarc

3 appendix

dkim.jp

DKIM の普及率



http://www.soumu.go.jp/main_content/000242082.pdf

dkim.jp

DKIM adaptation

Receiver

	ISP	Verify
1	its communications Inc.	○
2	NEC BIGLOBE, Ltd	○
3	NTT Plala Inc.	×
4	So-net Entertainment Cor	○
5	Technology Networks In	○
6	Dream Train Internet Inc.	予定あり
7	NIFTY Corporation	○
8	FreeBit Co., Ltd.	予定あり
9	Internet Initiative Japan	○
10	Yahoo Japan Corporation	○
11	Broadband Security, Inc.	○

2→10

大手 ISP はかなり対応が進んでいる

その他の取り組み

ネット選挙

※ Yahoo! メールのメールボックスの例