IAjapan 第14回 迷惑メール対策カンファレンス

【OC2-08】
DMARCによる新しいメール認証と導入の留意点

講師：
北崎 恵凡
SoftBank 株式会社
ニコライ ボヤジエフ
株式会社コミュニティネットワークセンター
櫻庭 秀次
株式会社インターネットイニシアティブ

IA japan

IAjapan 第15回 迷惑メール対策カンファレンス

【TD1-09】
DMARCによる新しいメール認証と導入の留意点

講師：
北崎 恵凡
SoftBank 株式会社
ニコライ ボヤジエフ
株式会社コミュニティネットワークセンター
櫻庭 秀次
株式会社インターネットイニシアティブ

IA japan

本日の話

・ここ1年間の動向　（5分：北崎）
・DMARCのおさらい　（5分：櫻庭）
・DMARCの普及状況　（5分：北崎）
・導入する上での留意点
  - DKIM第三者署名問題　（3分：北崎）
  - 法的留意点　（5分：北崎）
  - 技術的留意点　（15分：ニコライ）
・質疑応答、ディスカッション　（2分）

本日の話

・ここ1年間の動向　（5分：北崎）

・DMARCのおさらい　（5分：櫻庭）

・DMARCの普及状況　（5分：北崎）

・導入する上での留意点

- DKIM第三者署名問題　（3分：北崎）
- 法的留意点　（5分：北崎）
- 技術的留意点　（15分：ニコライ）

・質疑応答、ディスカッション　（2分）

▶ 情報共有

Cloud & Messaging Day 2015カンファレンスでDMARC.orgのSteven Jonesさんから基調講演が行われました。

http://www.twofive25.com/cmd2015/pdf/CMD2015_twofive.pdf
https://dmarc.org/2015/11/dmarc-org-presenting-at-cloud-messaging-day-in-tokyo/

スペシャルゲストとしてDMARC.orgでDMARC技術の推進を強力に推し進めている、Steve Jones氏がDMARC技術の最新アップデートとワールドワイドでの普及状況についてお話いたします。

DMARC

HOME BLOG OVERVIEW RI

DMARC.org presenting at Cloud & Messaging Day in Tokyo

Steven Jones will be speaking at the Cloud & Messaging Day meeting in Tokyo the afternoon of Monday, November 16th.The meeting is organized and hosted by messaging and infrastructure specialists TwoFive of Tokyo. (A PDF version of the flyer in Japanese is available here.)

Jones will address all attendees in the first session on the need for greater DMARC adoption in order to protect customers – and increasingly, employees and partners – from email-borne abuse, as well as recent developments like the ARC protocol, which is designed to make DMARC more compatible with "indirect mailflows" like mailing lists. ARC was announced at the M3AAWG conference in Atlanta last month. In the closing session of the meeting, Jones will appear on a general Q&A panel alongside representatives from ReturnPath, Cloudmark, and IIJ.

This entry was posted in Blog. Bookmark the permalink.

カンファレンス後のプレス発表が記事になっています。

http://japan.zdnet.com/article/35073722/

“送信ドメイン認証”の普及が不正メールを減らす--DMARC.orgが意義を説明

日川佳三 2015年11月19日 07時30分

フィッシングメールなどの成りすましメールの被害を防ぐ仕組みとして、受け取ったメールが正規の送信者から送られているかどうかを調べる“送信ドメイン認証”と呼ぶ技術がある。DKIM（Domainkeys Identified Mail）とSPF（Sender Policy Framework）の2つが送信ドメイン認証技術の代表だ。

DKIMとSPFの送信ドメイン認証技術の認証結果をもとに自動でアクセスを制御したりレポーティングしたりできるようにする仕組みがDMARC（Domain-based Message Authentication, Reporting & Conformance）だ。認証に失敗したメールを機械的に処理できるようになるほか、認証結果をメール送信者に伝えて情報を共有できるようになる。

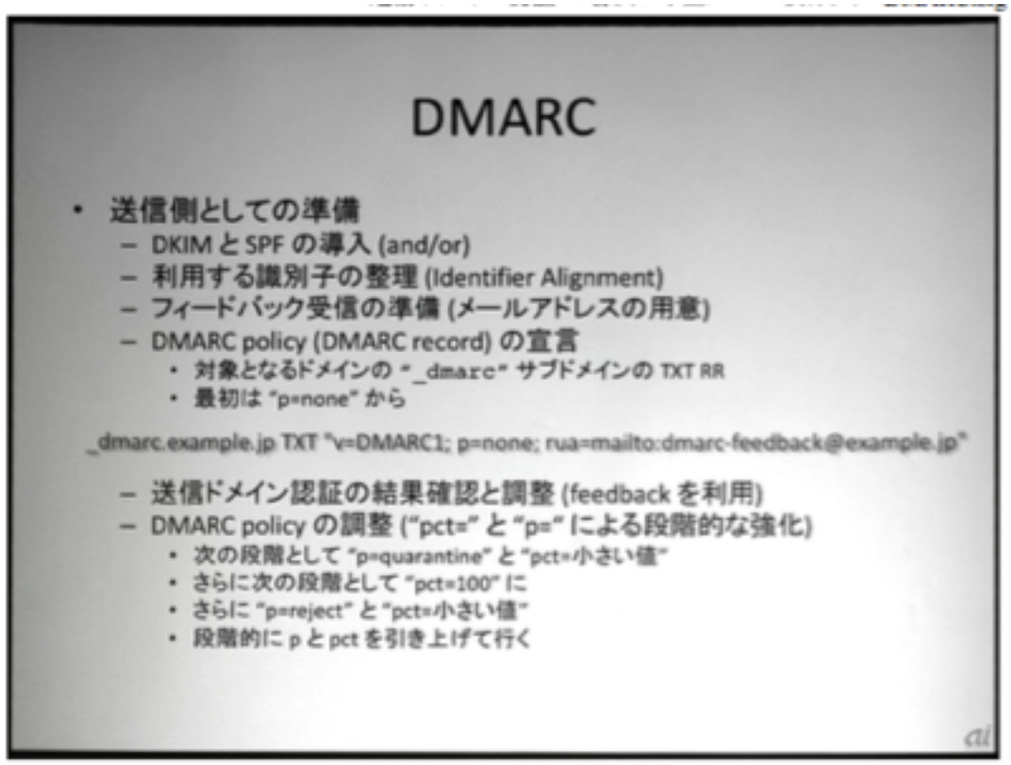
11月18日、DMARCの普及を推進する組織「DMARC.org」でエグゼクティブディレクターを務めるSteven M Jones氏が会見し、DMARCの意義を説明した。Jones氏は「迷惑メールとフィッシングメールは永遠の脅威」とメール送信者を認証することの必要性を説いた。この上で「送信者と受信者が協力しあえば、メール利用者を保護できる」とDMARCの意義を説明した。

DMARC.org エグゼクティブディレクター Steven Jones氏

メール送信側の対応は容易--受信側はメールを自動で処理可能に

DMARCに対応する労力と、その見返りは以下の通りだ。

まず、メール送信者がDMARCに対応するのは簡単だ。DKIMかSPFのいずれか、または両方に対応した上でDMARCの情報をDNSサーバに登録するだけでよい。DNSには、認証



DMARCに対応するために必要な準備

DMARCの前提の1つとなるDKIMは、電子署名で認証する。具体的には、受信メールのヘッダに含まれる電子署名をDNSから得た公開鍵で復号して検証する。仕組み上、メール送信者と受信者ともにメールサーバがDKIMに対応している必要がある。

もう1つの前提となるSPFは、IPアドレスで認証する。具体的には、DNSから得たIPアドレスと、送信サーバのIPアドレスが一致するかどうかを調べる。仕組み上、メール受信者側はメールサーバがSPFに対応する必要があるが、メール送信者はDNSへの登録だけでよい。

メール受信者がDMARCに対応するメリットの1つは、送信者がDNSで公開しているアクセス制御ポリシーに応じて、認証に失敗したメールを機械的に処理できること。DMARCの情報がDNSに登録されている（DKIMかSPFで認証できることを表明している）にもかかわらずDKIMやSPFで認証できなかった場合に、自動的に受信を拒否したり、迷惑メールとして隔離したりできるようになる。

DMARCは、DKIMとSPFの認証に加えて、DMARC独自の検証機能も持つ。DKIMが認証に使うドメイン名（メールのDKIMヘッダに書かれたドメイン名）やSPFが認証に使うドメイン名（SMTPセッションのMAIL FROMコマンドの引数）を、DMARCがDNSを参照する際に使うドメイン名（メールのFROMヘッダに書かれたドメイン名）と照らし合わせ、これらが一致するかどうかを確認する。部分一致や完全一致を確認し、DMARCの最終的な認証結果とする。

Yahoo!, AOLに引き続きGMailも2016年6月からStricter(p=reject)へ移行することが発表され、2016年7月に実施済を確認しています。

https://dmarc.org/2015/10/global-mailbox-providers-deploying-dmarc-to-protect-users/

DMARC

HOME BLOG OVERVIEW RI

Global Mailbox Providers Deploying DMARC to Protect Users

Berkeley, California – October 19, 2015 – The Domain-based Message Authentication, Reporting, & Conformance (DMARC) specification has proven its value in combating fraudulent email since its introduction three and a half years ago. Thousands of companies use it to prevent billions of messages fraudulently using their Internet domains from reaching inboxes, thereby protecting their customers and employees from phishing and other abuse. And now two of the largest mailbox providers in the world – Google (NASDAQ: GOOG) and Yahoo (NASDAQ: YHOO) – have announced that they are extending that protection to cover more of their Internet domains

Google To Adopt Stricter DMARC Policies in 2016

To further bolster the proven utility of DMARC, Google has announced that they will be moving their hosted mailbox services to a similarly strict DMARC policy in 2016. "Google is committed to email authentication. In June of 2016, we will be taking a big step by moving gmail.com to DMARC policy p=reject." said John Rae-Grant, Lead Product Manager for Gmail. "We are pleased to be supporting the ARC protocol to help mailing list operators adapt to the need for strong authentication."

"More and more companies have been adopting DMARC and email authentication over the past few years, with more vendors and service providers adding the necessary support to their offerings in order to make that adoption simpler," said Steven Jones, Executive Director of DMARC.org. "With new protocols like ARC emerging to address the traditional email use cases that were problematic under some DMARC policies, and the leadership of forward-thinking companies like Google, Microsoft and Yahoo, I expect to see the rate of adoption accelerate globally."

本日の話

・ここ1年間の動向　（5分：北崎）

・DMARCのおさらい　（5分：櫻庭）

・DMARCの普及状況　（5分：北崎）

・導入する上での留意点

- DKIM第三者署名問題　（3分：北崎）
- 法的留意点　（5分：北崎）
- 技術的留意点　（15分：ニコライ）

・質疑応答、ディスカッション　（2分）

本日の話

・ここ1年間の動向　（5分：北崎）

・DMARCのおさらい　（5分：櫻庭）

・DMARCの普及状況　（5分：北崎）

・導入する上での留意点

- DKIM第三者署名問題　（3分：北崎）
- 法的留意点　（5分：北崎）
- 技術的留意点　（15分：ニコライ）

・質疑応答、ディスカッション　（2分）

▶ DMARC普及状況

source: https://eggert.org/meter/dmarc

Global DMARC Deployment
46.7%
500 sites tested
22 DNS errors
223 with DMARC

China
20.1%
500 sites tested
43 DNS errors
92 with DMARC

Germany
22.6%
500 sites tested
5 DNS errors
112 with DMARC

Finland
22.7%
500 sites tested
6 DNS errors
112 with DMARC

India
29.9%
500 sites tested
31 DNS errors
140 with DMARC

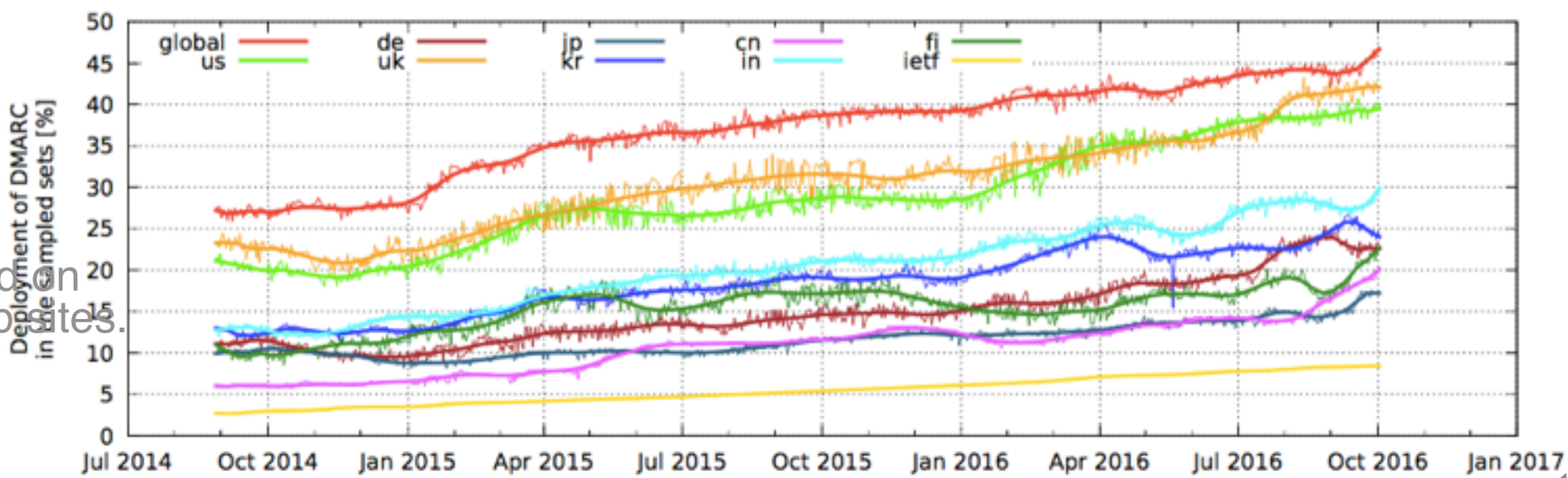
IETF
8.4%
3083 sites tested
0 DNS errors
260 with DMARC

Japan
17.2%
500 sites tested
75 DNS errors
73 with DMARC

South Korea
24.0%
500 sites tested
108 DNS errors
94 with DMARC

United Kingdom
42.1%
500 sites tested
65 DNS errors
183 with DMARC

United States
39.5%
500 sites tested
6 DNS errors
195 with DMARC



This investigation is based on alexa.com's TOP 500 websites.

▶ DMARCレコード普及状況（集計方法とタイプ）

ドメイン数ベース
流通数ベース
ドメイン数ベース *(TOP500ドメイン)*
流通数ベース *(TOP500ドメイン)*

Type	*DMARCレコード*	*SPFレコード*
A	あり(正常)	あり
B	あり(誤り)	あり
C	あり(正常)	なし
D	あり(誤り)	なし
E	なし	あり
F	なし	なし

ドメイン数: n=40,077,226 /日

流通数: n=199,198,510 /日

▶ DMARCレコードの記述ミス（例）

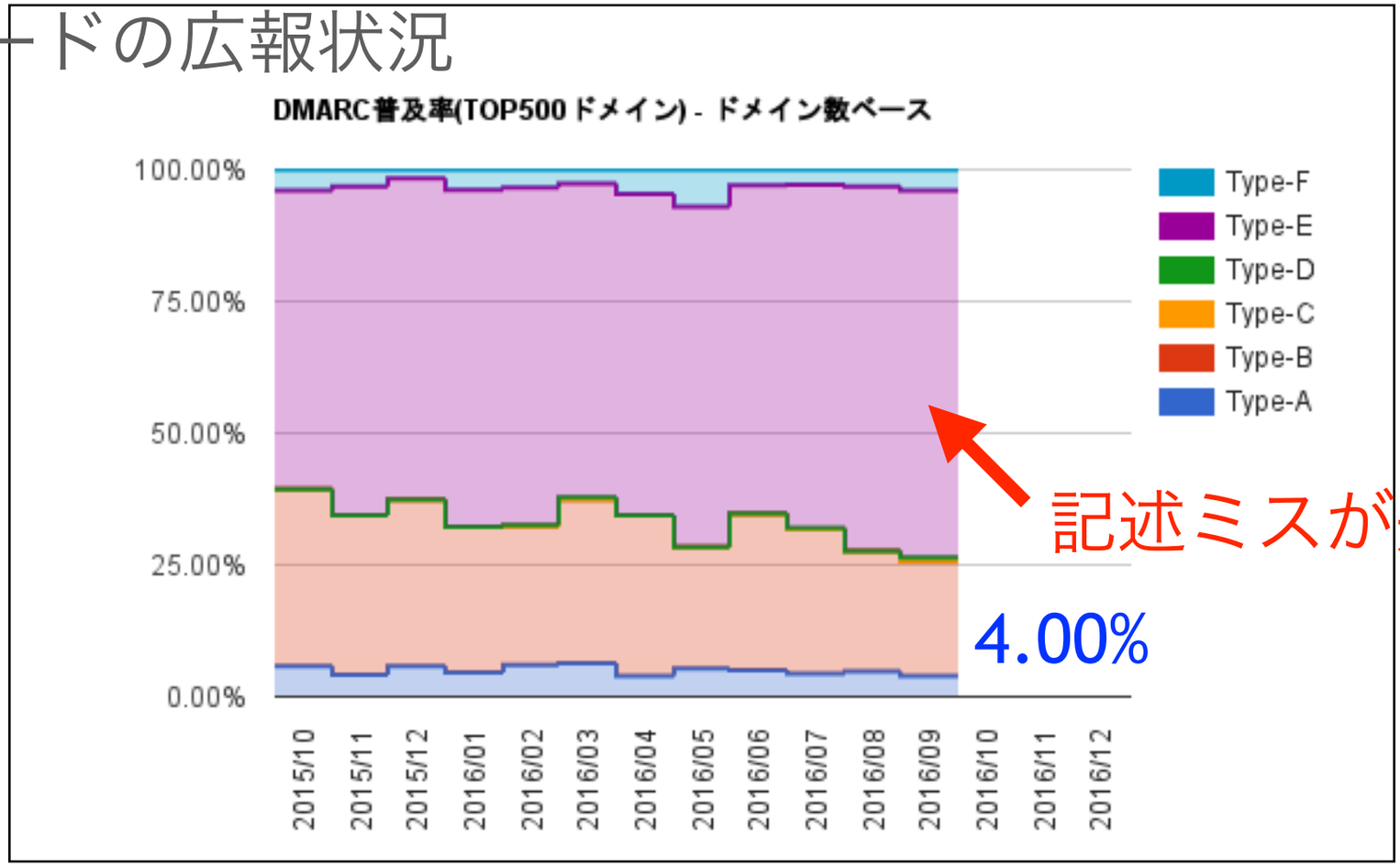
・誤ったDNS実装（SPFレコードを広報）

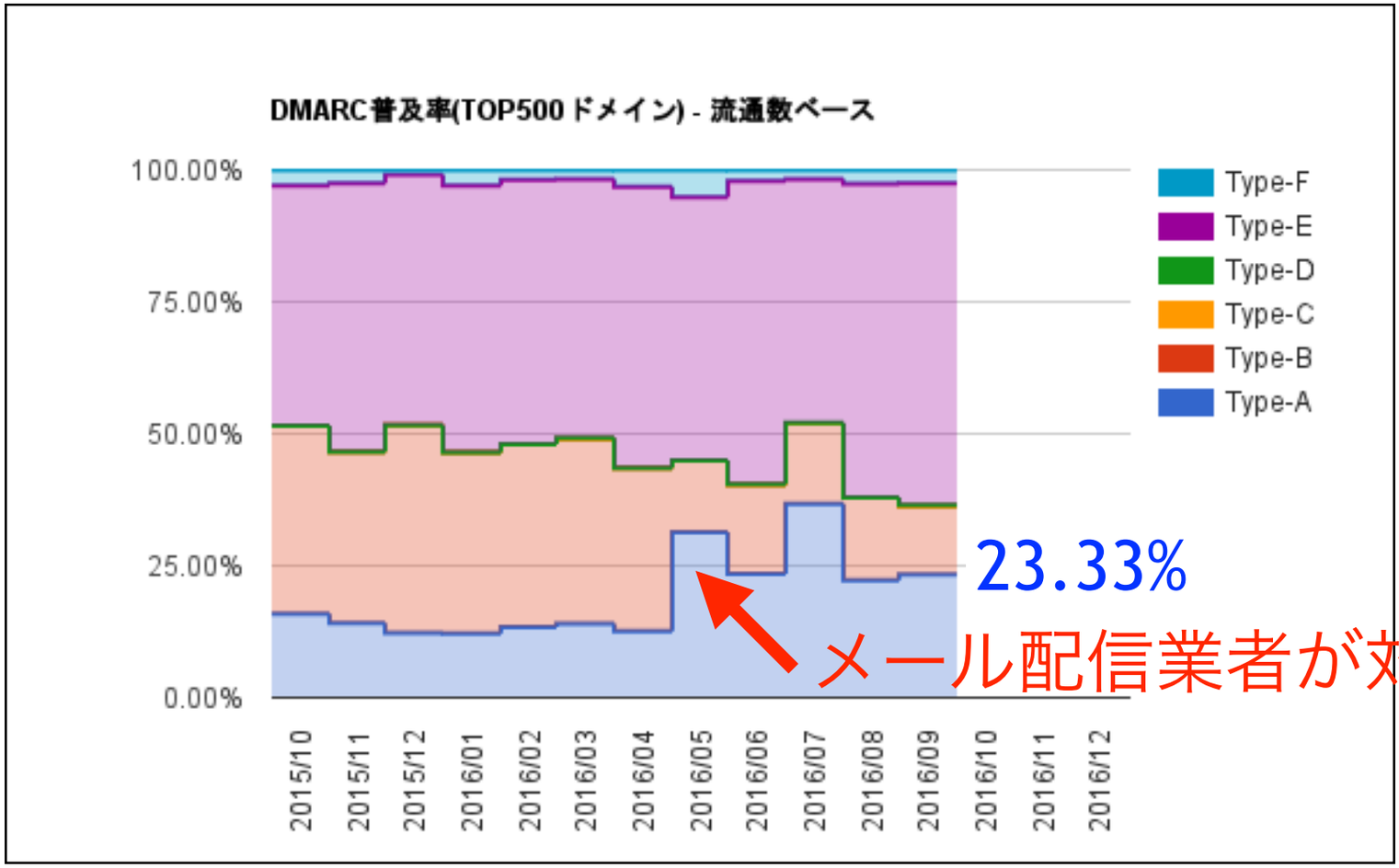
・vタグのみ（pタグが無い）

・typo（セパレータが：(コロン)、p=monitor、quarentenaなど）

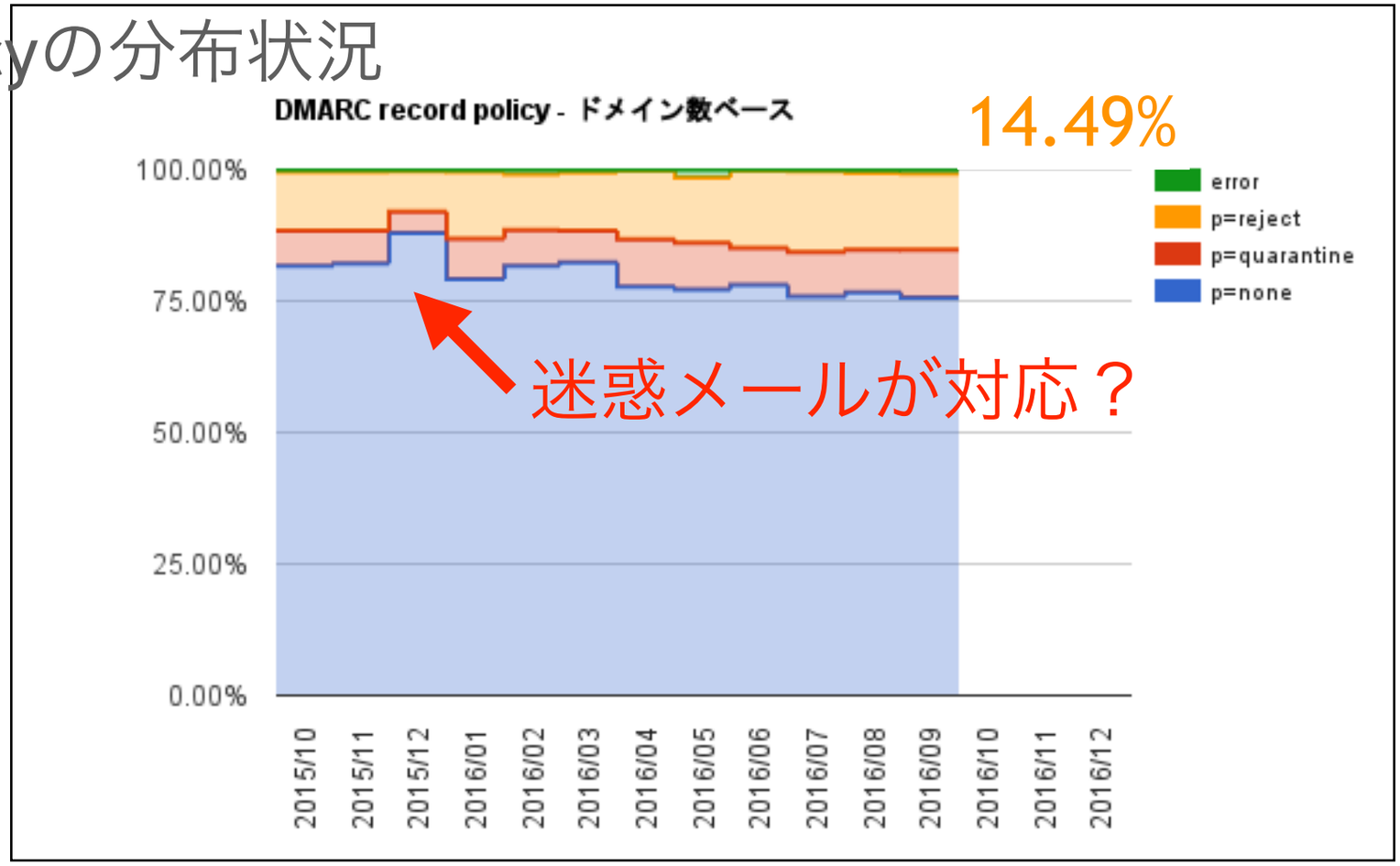
（参考）https://dmarc.org/2016/07/common-problems-with-dmarc-records/

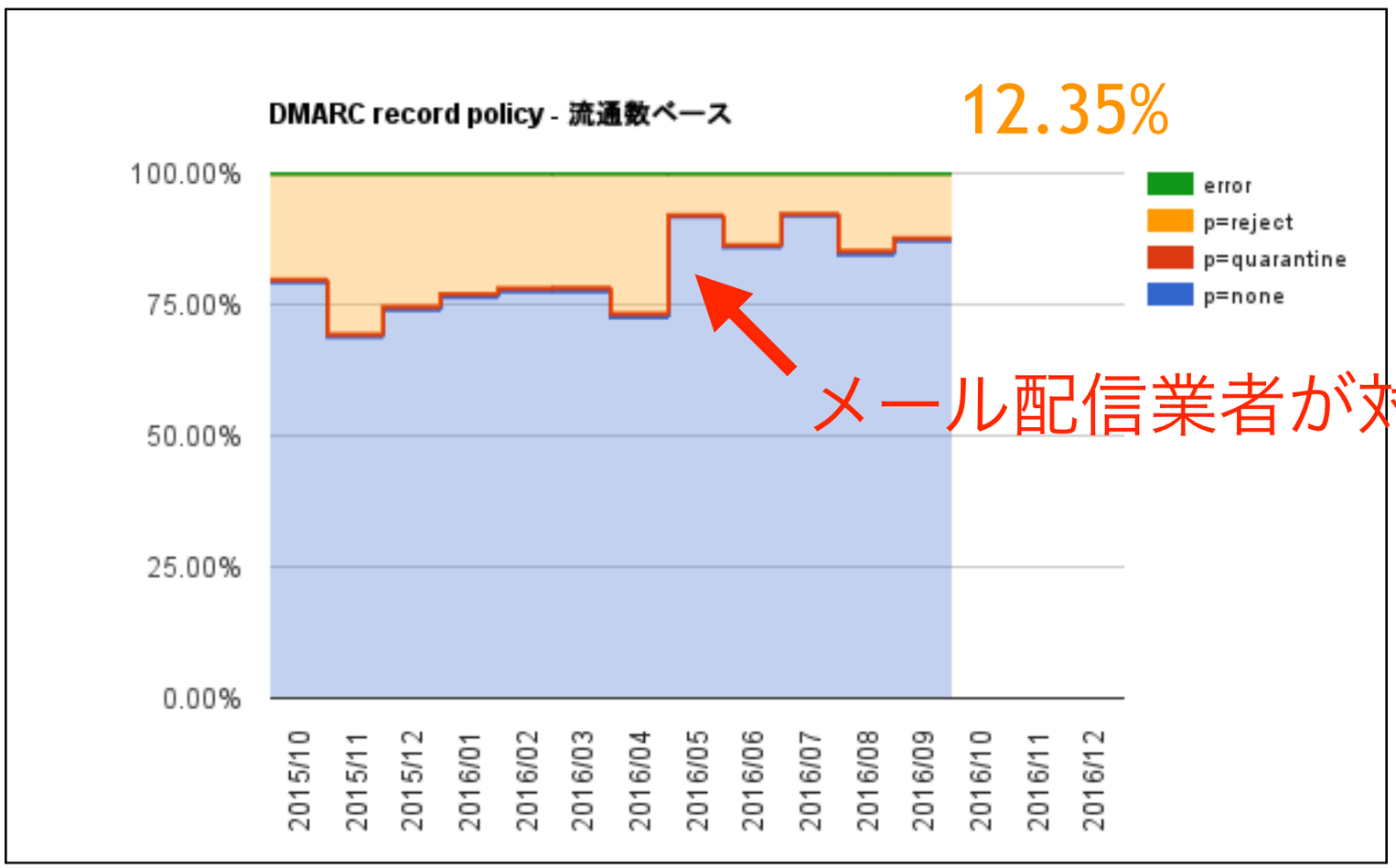
▶ DMARCレコードの広報状況



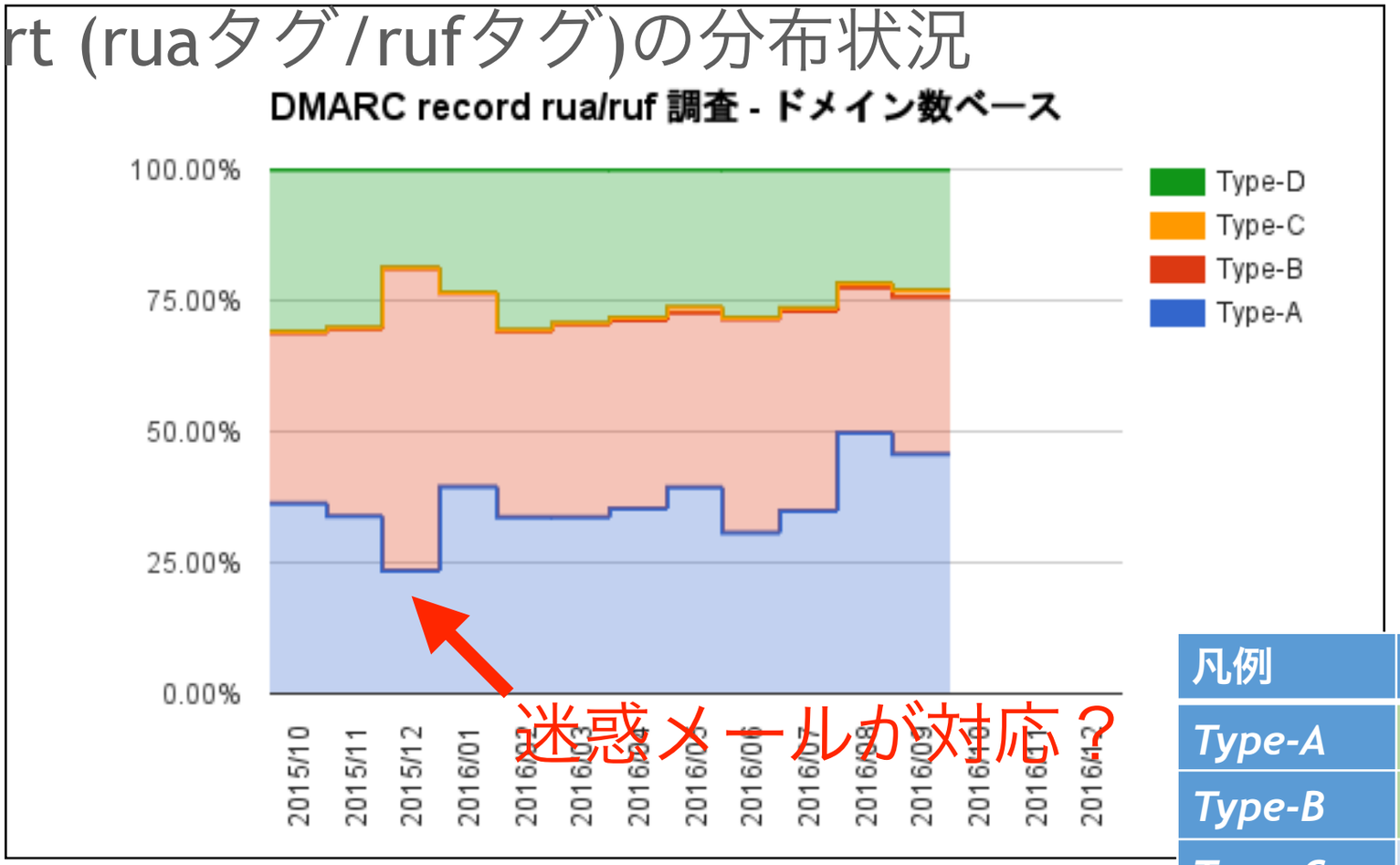


▶ DMARC Policyの分布状況

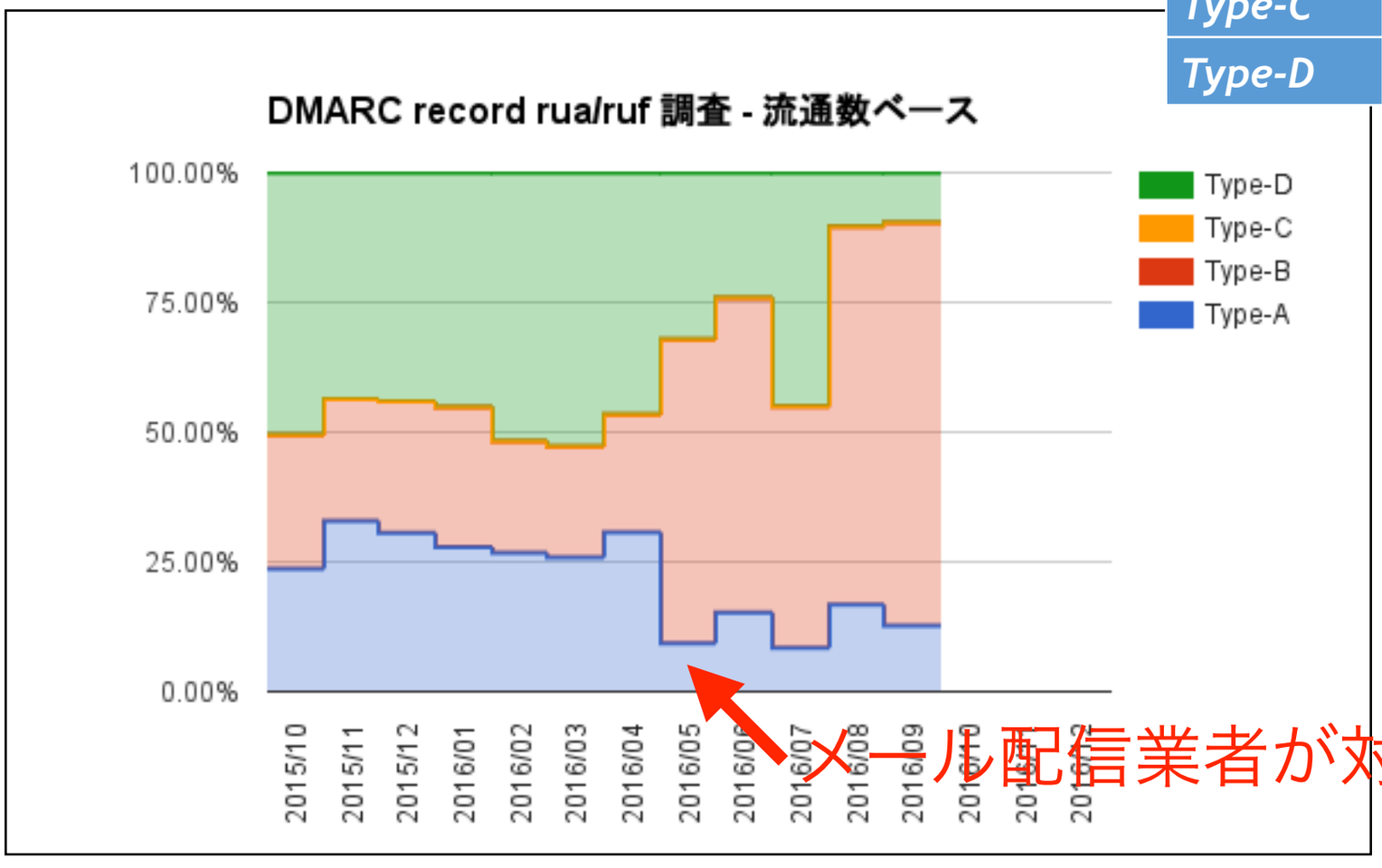




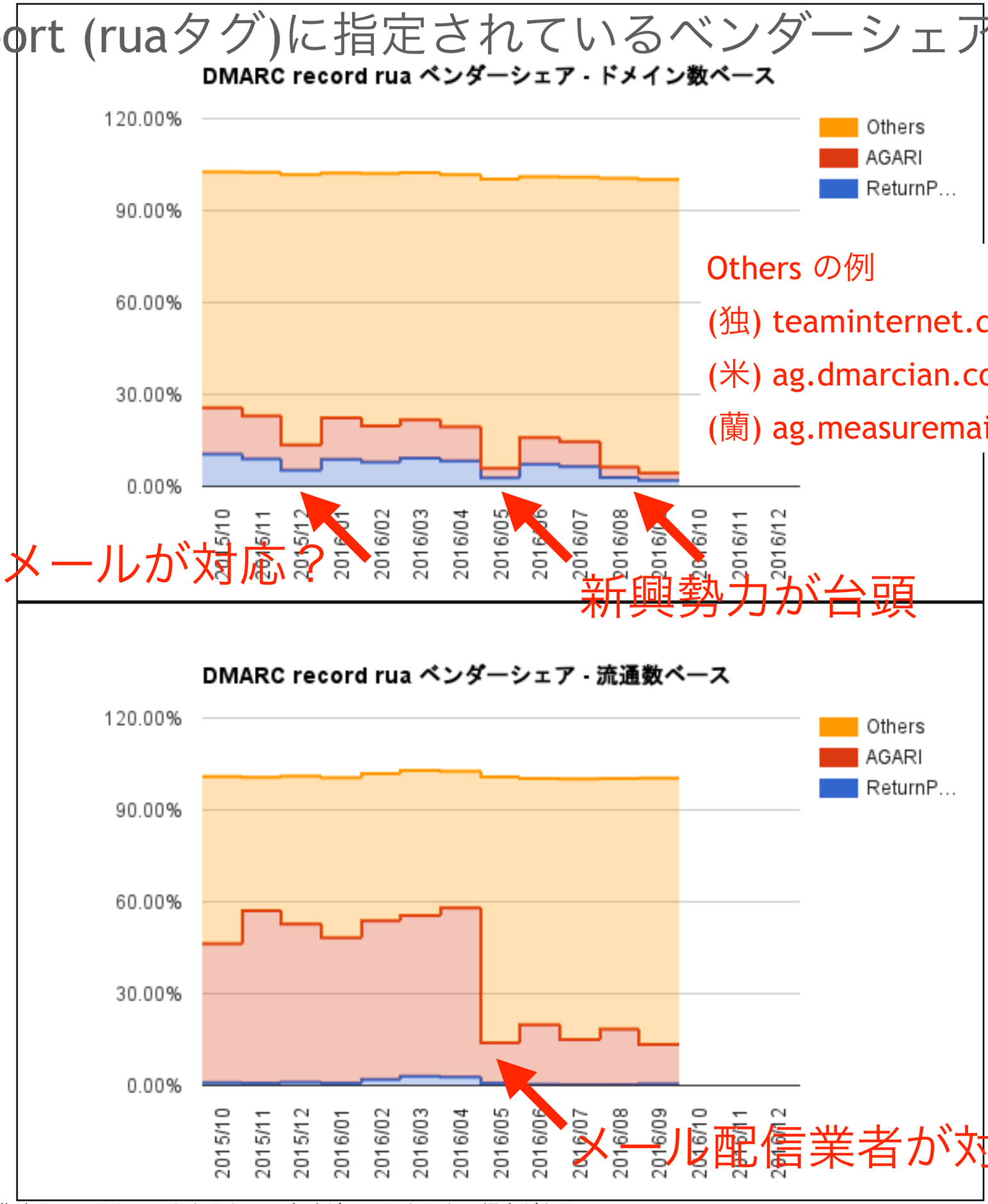
DMARC Report (ruaタグ/rufタグ)の分布状況



凡例	ruaタグ	rufタグ
Type-A	あり	あり
Type-B	あり	なし
Type-C	なし	あり
Type-D	なし	なし



▶ DMARC Report (ruaタグ)に指定されているベンダーシェア



Others の例

(独) teaminternet.de

(米) ag.dmarcian.com

(蘭) ag.measuremail.com

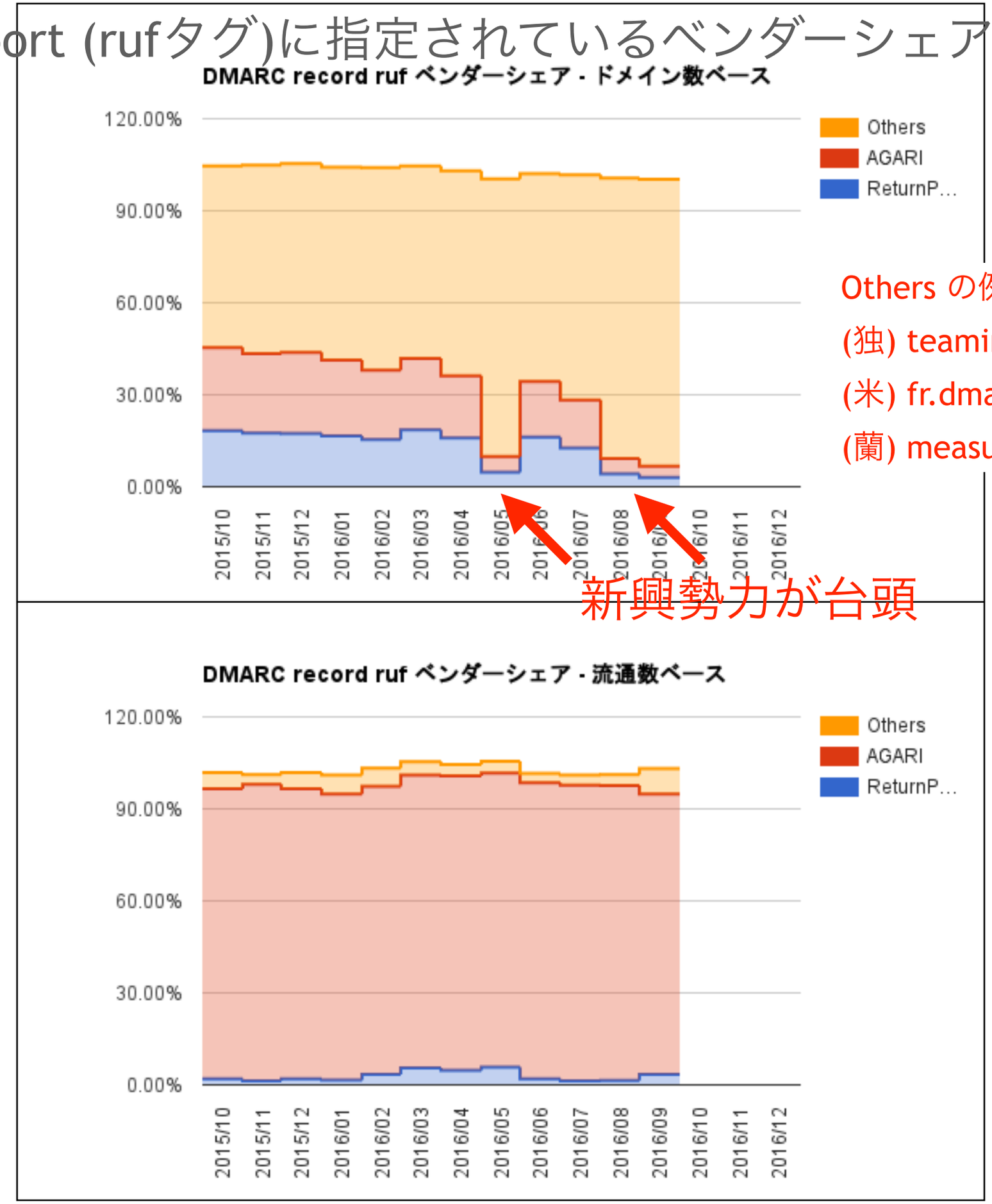
迷惑メールが対応？

新興勢力が台頭

メール配信業者が対応

※ReturnPath, AGARI, 自社の複数を指定しているケースもあるため、合計が100%にならない場合がある。

▶ DMARC Report (rufタグ)に指定されているベンダーシェア



Others の例

(独) teaminternet.de

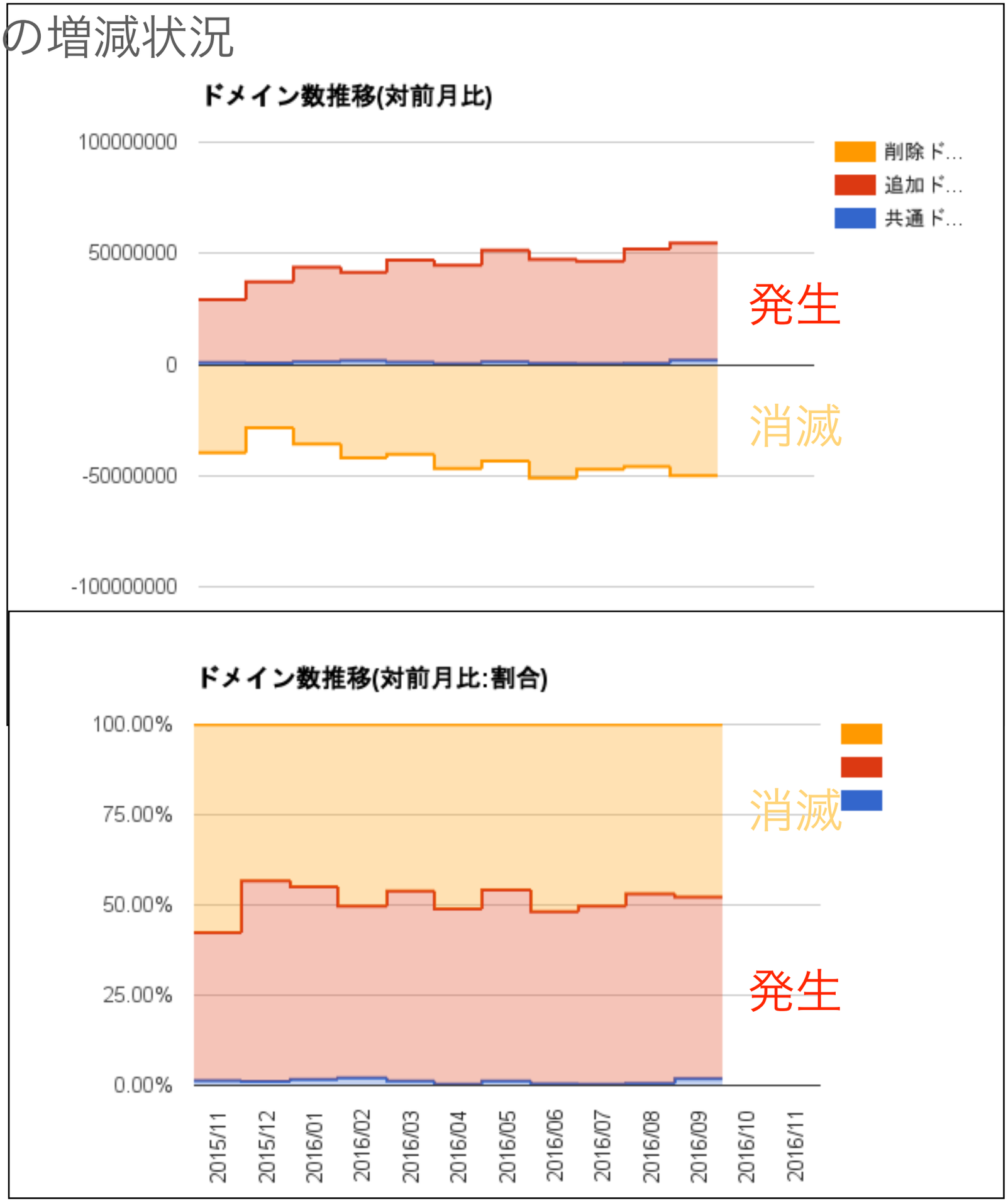
(米) fr.dmarcian.com

(蘭) measuremail.com

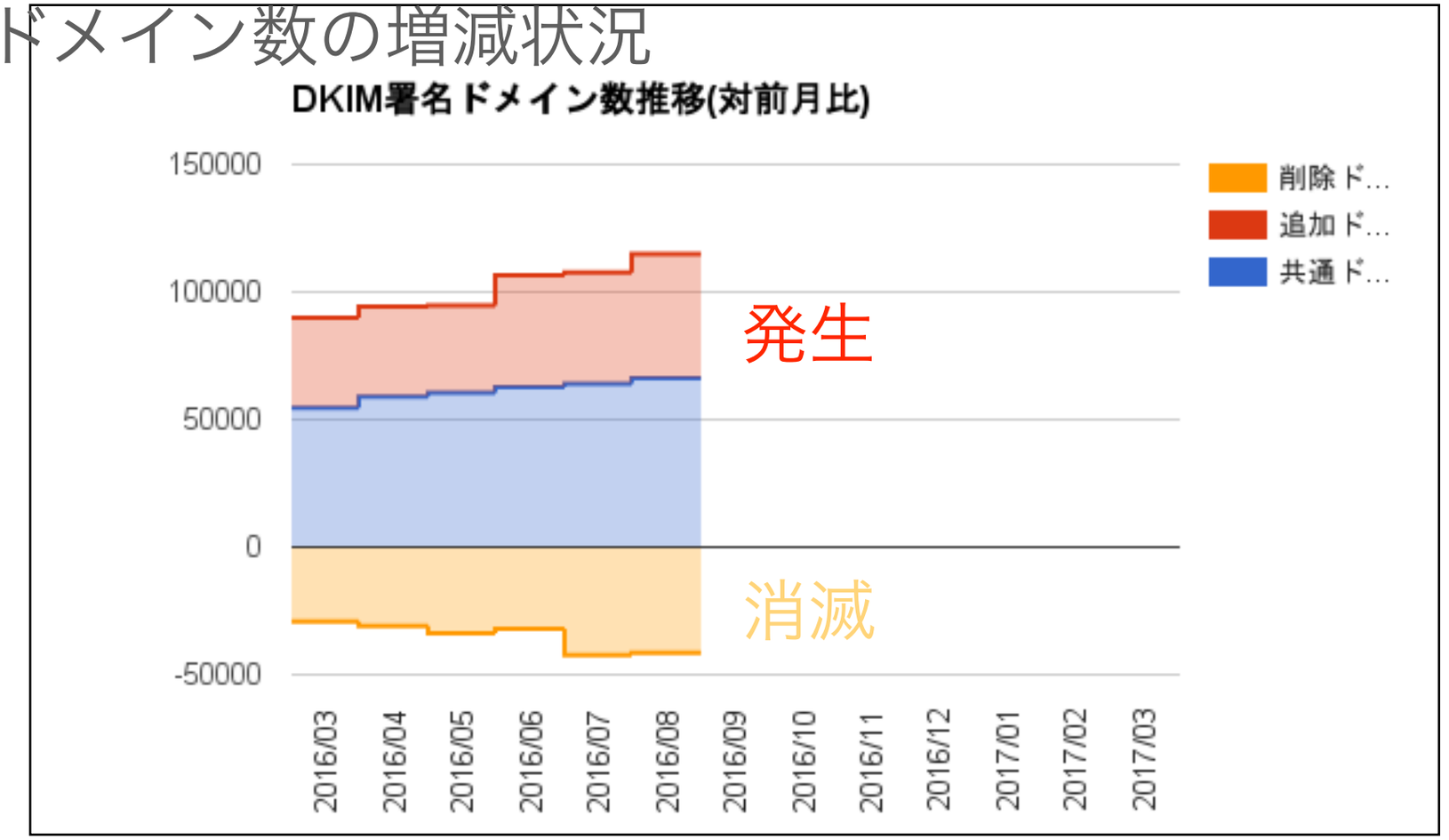
新興勢力が台頭

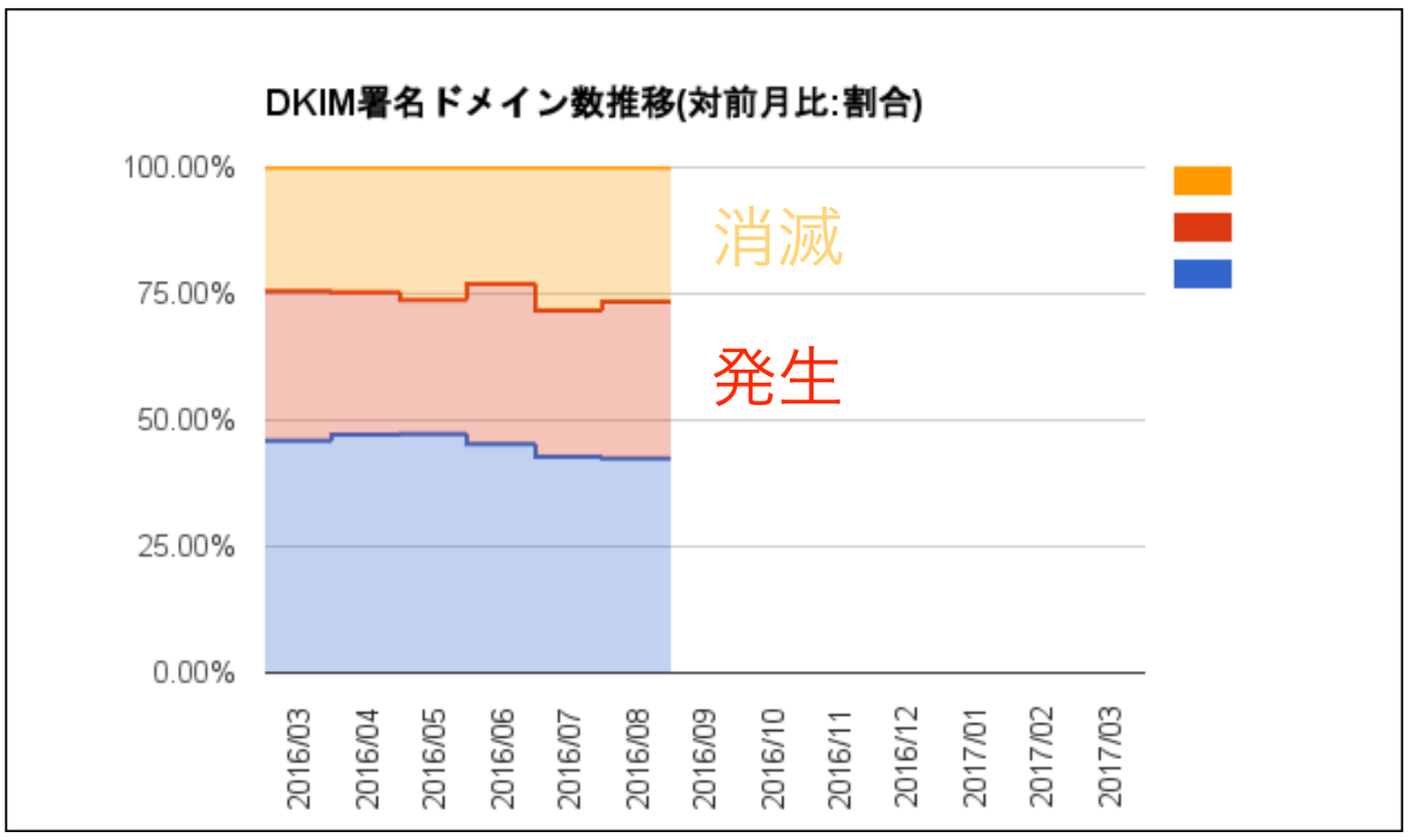
※ReturnPath, AGARI, 自社の複数を指定しているケースもあるため、合計が100%にならない場合がある。

▶ ドメイン数の増減状況


ドメイン数推移(対前月比)
100000000
50000000
0
-50000000
-100000000
削除ド…
追加ド…
共通ド…
発生
消滅
ドメイン数推移(対前月比:割合)
100.00%
75.00%
50.00%
25.00%
0.00%
消滅
発生
2015/11
2015/12
2016/01
2016/02
2016/03
2016/04
2016/05
2016/06
2016/07
2016/08
2016/09
2016/10
2016/11

▶ DKIM署名ドメイン数の増減状況

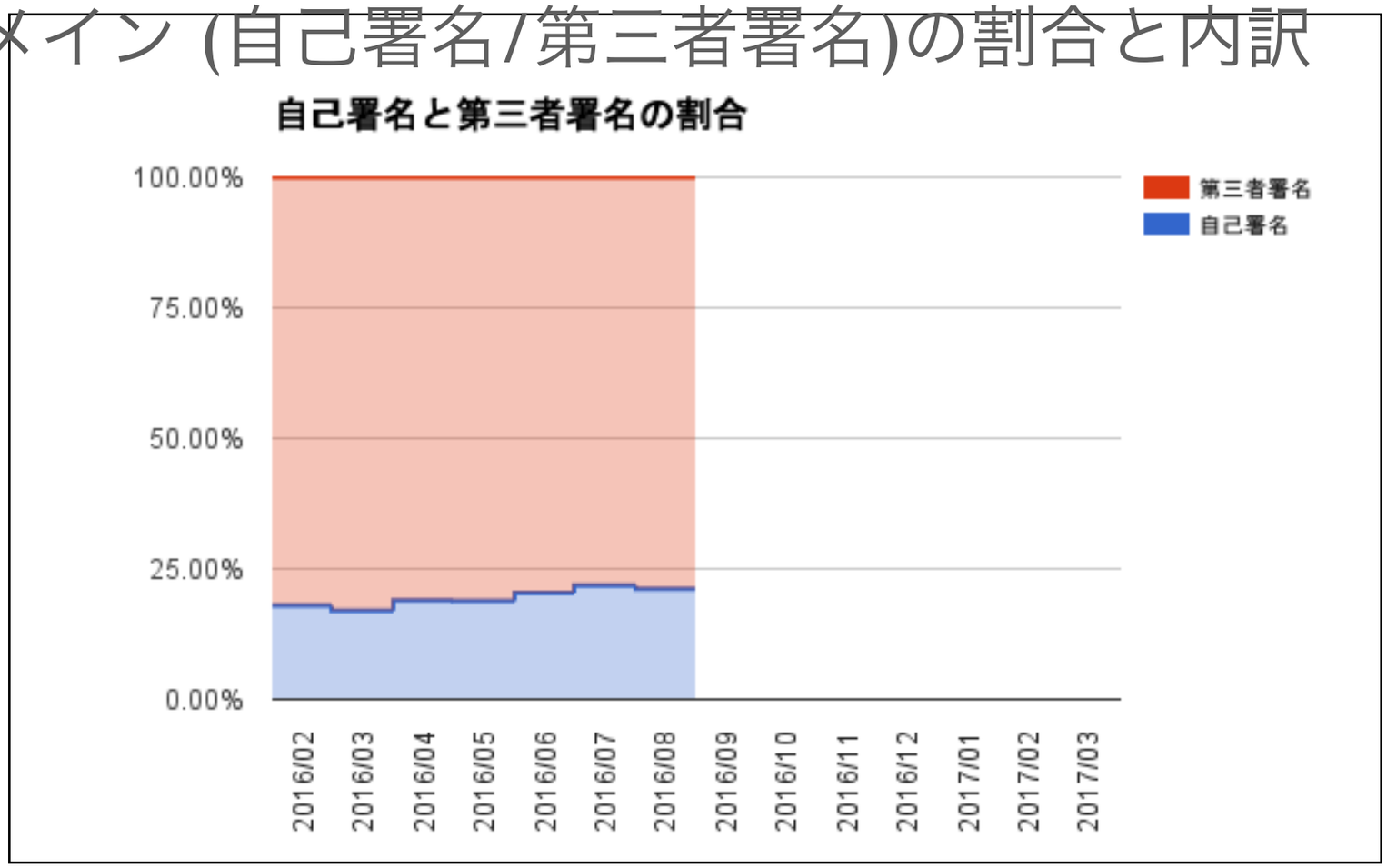


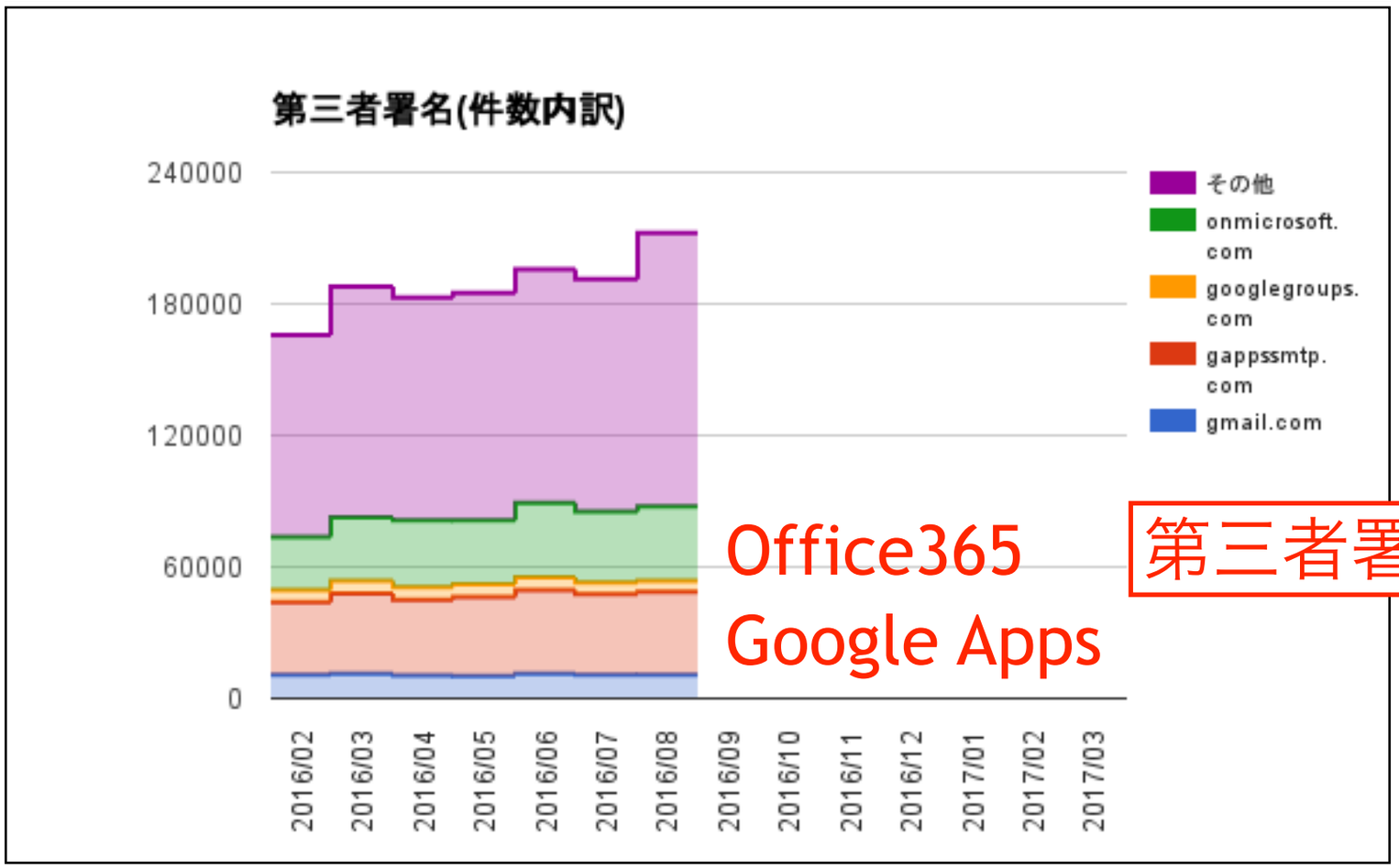


本日の話

・ここ1年間の動向　（5分：北崎）
・DMARCのおさらい　（5分：櫻庭）
・DMARCの普及状況　（5分：北崎）
・導入する上での留意点
  - DKIM第三者署名問題　（3分：北崎）
  - 法的留意点　（5分：北崎）
  - 技術的留意点　（15分：ニコライ）
・質疑応答、ディスカッション　（2分）

▶ DKIM署名ドメイン (自己署名/第三者署名)の割合と内訳





Office365
Google Apps

第三者署名問題あり

▶ 第三者署名問題の事例

２０１６年１月時点

	SPF	DKIM	DMARC
M 銀行様	pass (**bma.mpse.jp**) pass (direct-**.bk.mufg.jp)	none pass (direct-**.bk.mufg.jp)	**fail** (**mufg.jp**) pass (direct-**.bk.mufg.jp)
M 銀行様	pass (envelope.smbc.co.jp)	none	pass (ra.smbc.co.jp)
M 銀行様	none (dm*.mizuhobank.co.jp)	pass (n01.smp.ne.jp)	none (e-mail.mizuhobank.co.jp)

２０１６年７月時点

	SPF	DKIM	DMARC
M 銀行様	pass (*.bk.mufg.jp) pass (direct-**.bk.mufg.jp)	pass (mufg.jp) pass (direct-**.bk.mufg.jp)	pass (mufg.jp) pass (direct-**.bk.mufg.jp)
M 銀行様	pass (envelope.smbc.co.jp)	none	pass (ra.smbc.co.jp)
M 銀行様	none (dm*.mizuhobank.co.jp)	pass (n01.smp.ne.jp)	none (e-mail.mizuhobank.co.jp)

▶ 同業他社比較（1/2）

米国・銀行

BANKS

Show 10 entries　　Search:

Name	Domain name	DMARC	DKIM	SPF	DNSSEC
American Bankers Assoc...	aba.com	✗	✗	✓	🔑
Bank of America	bankofamerica.com	🔨	✗	✓	🔑
Citigroup	citigroup.com	🛡	✗	✓	🔑
JPMorgan Chase	chase.com	🛡	✓	✓	🔑
	jpmchase.com	🛡	✓	✓	🔑
	jpmorgan.com	🛡	✓	✓	🔑
	jpmorganchase.com	🛡	✗	✓	🔑
PayPal	paypal.com	🛡	✓	✓	🔑
PNC Financial Services	pnc.com	✗	✗	✓	🔑
U.S. Bancorp	usbank.com	🛡	✗	✓	🔑

Showing 1 to 10 of 11 entries　　Previous 1 2 Next

source: https://www.phishingscorecard.com/ScoreCard/United-States/Banks/NS0x

▶ 同業他社比較（2/2）

米国・メールサービス

MAILPROVIDERS

Show 10 entries　　Search:

Name	Domain name	DMARC	DKIM	SPF	DNSSEC
AOL	aol.com	✓	✗	✓	✗
Gmail	gmail.com	!	✓	✓	✗
Mail.ru	bk.ru	✓	✗	✓	✗
	inbox.ru	✓	✗	✓	✗
	list.ru	✓	✗	✓	✗
	mail.ru	✓	✗	✓	✗
Microsoft	hotmail.com	!	✗	✓	✗
	live.com	✗	✗	✓	✗
	outlook.com	!	✗	✓	✗
MineLight	minelight.ml	!	✗	✓	✗

Showing 1 to 10 of 19 entries　　Previous 1 2 Next

source: https://www.phishingscorecard.com/ScoreCard/International/Internet/Mailproviders/MTAtOS0zNw%3d%3d

本日の話

・ここ1年間の動向　（5分：北崎）
・DMARCのおさらい　（5分：櫻庭）
・DMARCの普及状況　（5分：北崎）
・導入する上での留意点
  - DKIM第三者署名問題　（3分：北崎）
  - 法的留意点　（5分：北崎）
  - 技術的留意点　（15分：ニコライ）
・質疑応答、ディスカッション　（2分）

▶ 送信ドメイン認証技術DMARC導入に関する法的留意点

・送信ドメイン認証技術の利用に関しては適法性が整理されている。

http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/jigyosha.html

・送信ドメイン認証技術のDKIMおよびSPFについては受信側における法的留意点が整理されているが、DMARCについては相互に情報交換することにより電子メールの疎通を確保することを目的とし、DKIMおよびSPFには含まれないポリシー機能およびレポーティング機能を含むため、その機能の利用に関して適法性が整理される必要がある。

検討する上で参考とした資料

Paper on DMARC and privacy laws in Germany and the EU
https://e-mail.eco.de/wp-content/blogs.dir/26/files/eco_dmarc_legal_report.pdf

送信ドメイン認証技術	*DKIM*	*SPF*	*DMARC*
電子メールの受信サーバにおいて、電子メールの送信ドメインを認証(チェック)し、認証できない場合には一定の措置を講ずる行為	整理済	整理済	整理可能 *(SPFとDKIMを利用しているため)*
ポリシー機能 (ドメイン所有者が受信者の「なりすましメール」の取り扱いに影響を与える)	ー	ー	**整理要**
レポーティング機能 (受信者がドメインに関する認証結果をドメイン所有者へ通知する)	ー	ー	**整理要**

当事者

・ドメイン所有者　(一般に、実際の電子メールの送信者とは異なる)

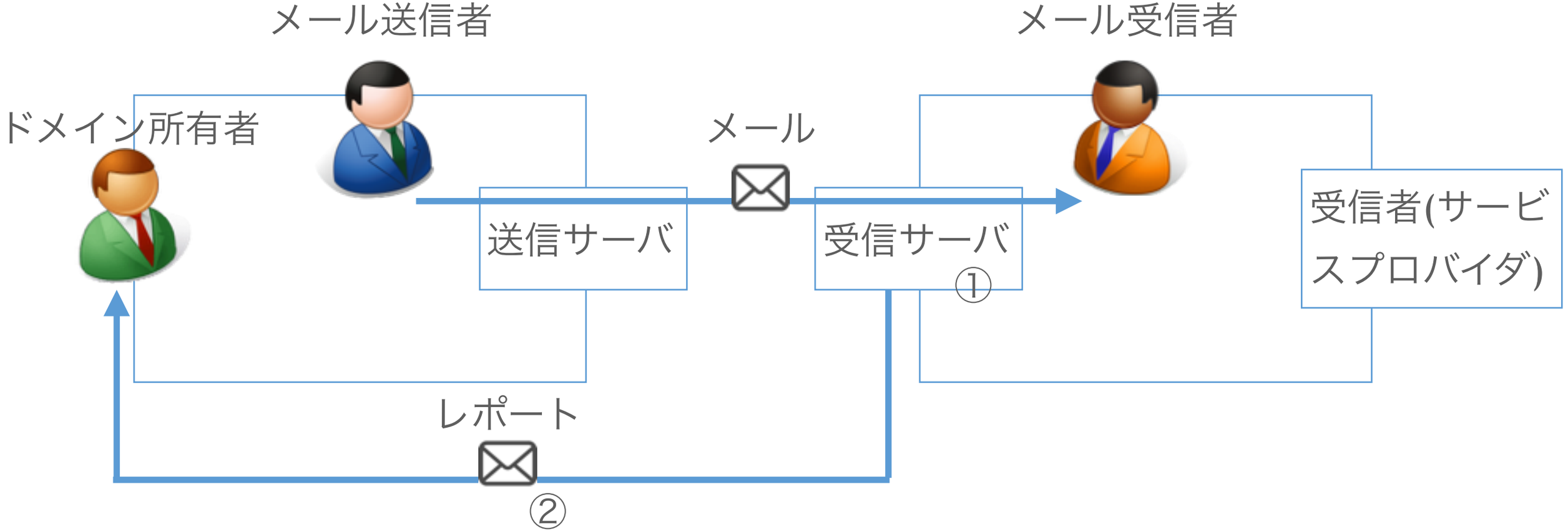
・メール送信者

・受信者(サービスプロバイダ)　(一般に、実際の電子メールの受信者とは異なる)

・メール受信者

①ポリシー機能

②レポーティング機能



論点
①ポリシー機能

受信サーバのラベリング結果等に基づくフィルタリングに影響を与えるが、受信側における法的留意点で整理されている。
http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/pdf/domain-j.pdf

→当事者の同意が必要。

→以下の5条件をすべて満たした場合、同意は不要。

1. 実施後、個別に設定変更が可能
2. フィルタリング以外は提供条件が同一
3. フィルタリング内容が明確
4. アンケートなどで合理性がある
5. 重要事項説明(電気通信事業法第26条)に準じた事前連絡

論点
②レポーティング機能

レポーティング機能には「集約レポート」と「失敗レポート」の2種類があり、それぞれについて検討する必要がある。

「集約レポート」はドメイン所有者が認証結果を分析する目的で使用される。
「集約レポート」には通信の構成要素に該当する送信ドメインおよび送信サーバのIPアドレスを含むため通信の秘密の保障を受けることとなるが、送信ドメインおよび送信サーバのIPアドレスに係る、ある一定期間の送信ドメイン認証結果の数が通知されるのであって、当事者(メール送信者またはメール受信者)の個別の通信に係る経路情報でなく、当事者の意思に反しての利用にも該当しないことから、通信の秘密の侵害(窃用)には当たらないと考えられる。

→通信の秘密に該当するが、通信の秘密を侵す行為には該当しないため、その利用は適法と認められるのではないか。

「失敗レポート」は通信上の問題点を特定する(認証失敗の理由と発信源を調べる)目的で使用される。通信上の問題点＝電子メール送受信上の支障とはメール送信者は正当なメールを送信したつもりでも、ドメイン所有者の送信サーバまたは受信者の受信サーバの問題により、メール受信者へ正当なメールが配信されないことである。

認証失敗結果の詳細がAFRFフォーマット(RFC6591: Authentication Failure Reporting Using the Abuse Reporting Format)を用いて受信者から送信者(ドメイン所有者)へ通知される。「失敗レポート」には「集約レポート」に含まれた送信ドメイン、送信サーバのIPアドレスに加え、当事者(メール送信者またはメール受信者)の個別の通信に係る、日時、送信者メールアドレス、受信者メールアドレス、メールの件名、メールの本文が含まれる場合があるため、通信の秘密の保障を受けることとなる。
認証失敗結果だけとはいえ、ドメイン所有者へ通信の秘密(の一部)を通知する行為は当事者の意思に反して利用することに当たり、通信の秘密の侵害(窃用)に当たると考えられる。

違法性阻却事由についての検討
正当業務行為に該当するには、(1)目的の必要性、行為の正当性、(2)手段の相当性を満たす必要がある。

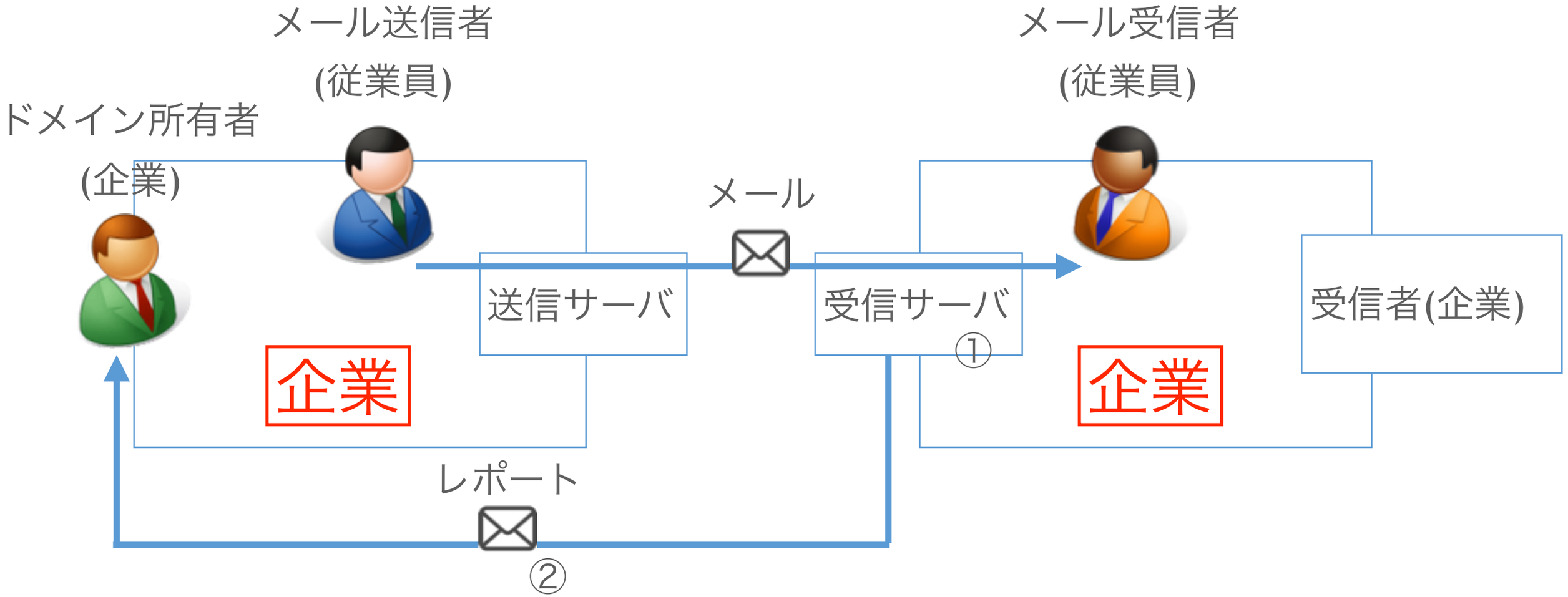
(1) 送信ドメイン認証を導入および利用を継続する上で、認証失敗が大量に発生している場合、特段の事情(送信元を偽装した迷惑メールが常時大量に送信されている状況)がない限り、電子メール送受信上の支障が生じている可能性が容易に想定され、正当な理由において支障を取り除く必要がある。

(2) 失敗レポートは認証失敗結果に関してのみ詳細を通知する行為であり、認証成功を含むすべてのメールを対象とせず、電子メール送受信上の支障を取り除くのに必要最小限な通信の秘密の構成要素に限れば、目的達成のために必要な限度を超えるものではないと考えられる。
認証失敗結果を当事者へ通知する方法も考えられるが、一般に当事者はドメイン所有者とは異なり、ドメイン所有者から貸与された送信者メールアドレスを使用して電子メールを送受信しているため、支障を取り除くことが困難であることから、ドメイン所有者へ通知する行為は必要かつ相当な方法と考えられる。

不当な差別的取扱いについての検討
正当業務行為として許されると解されることから、不当な差別的取扱いとはいえない。

▶ 問題無いと想定されるケース

メール送信側、およびメール受信側ともに通信当事者の同意を得ていると考えられるため、①、および②ともに問題無いと考えられる。

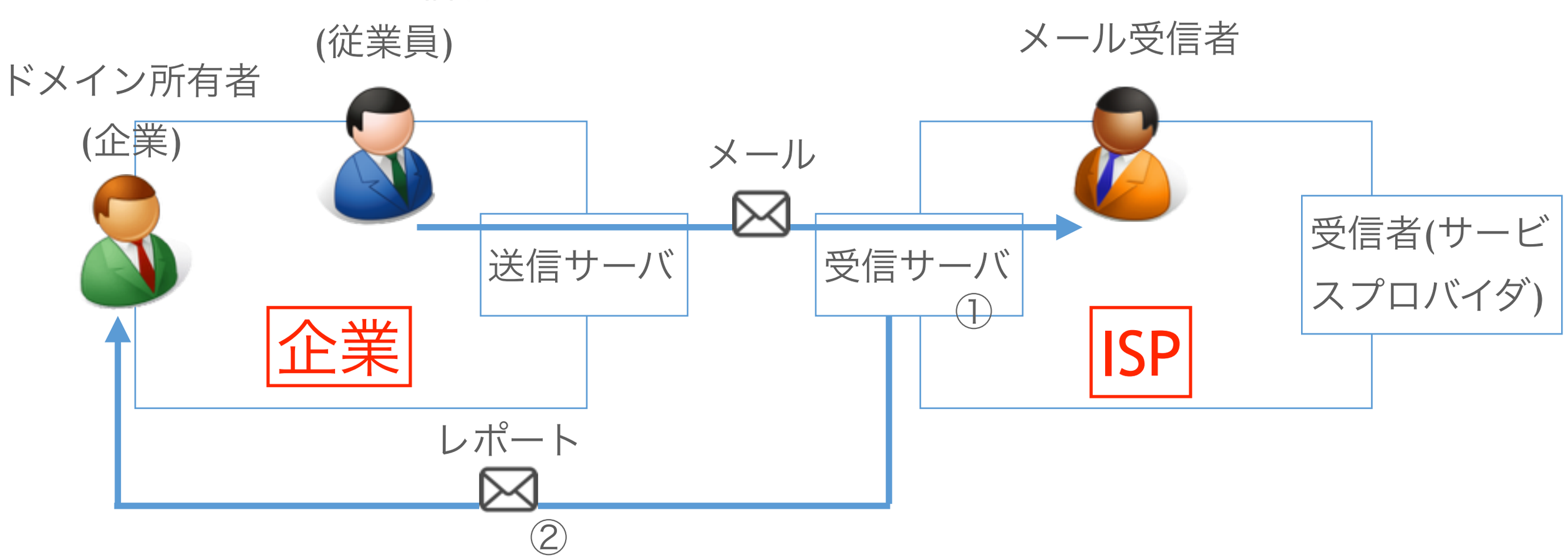


▶ 同意、または5条件を満たす必要があると想定されるケース

メール送信側はメール送信者の同意を得ていると考えられるため、①は問題無いと考えられる。

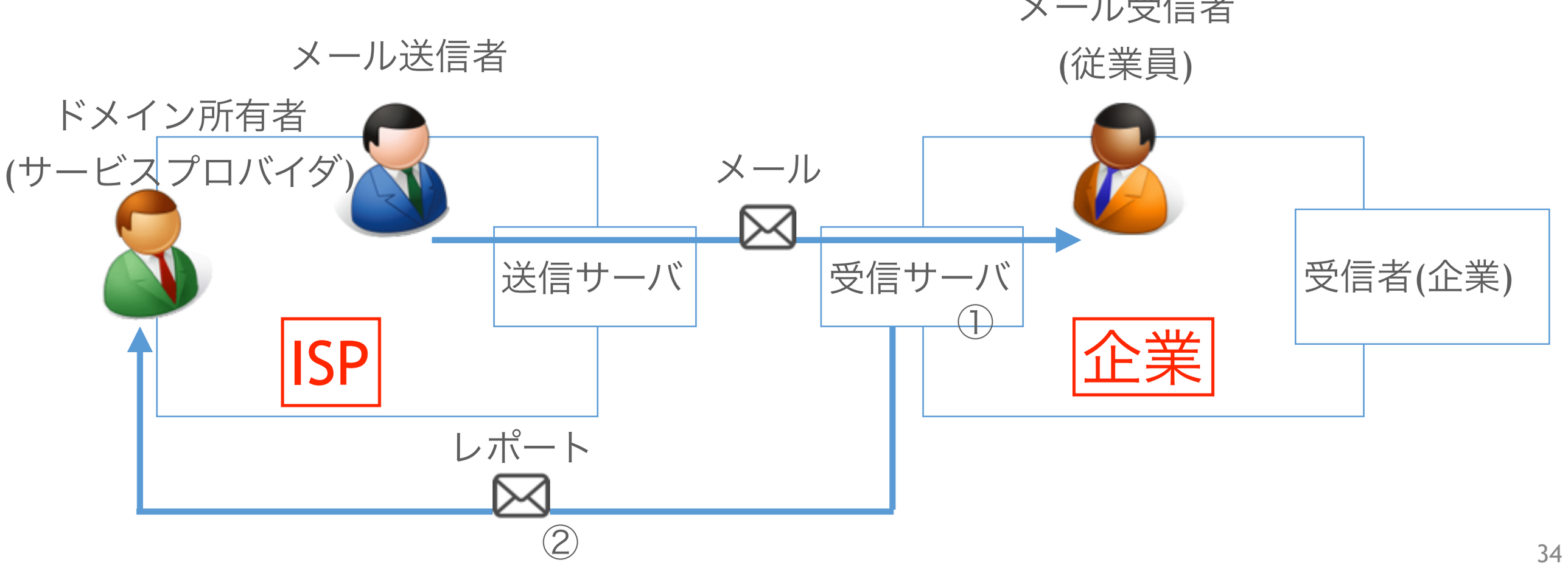
メール受信側はメール受信者の同意を得る、または5条件をすべて満たした場合は①、および②は問題無いと考えられる。

同意を得ていない、または5条件を満たしていない通信に係る情報を②へ含めることは整理が必要と考えられる。



▶ 整理が必要と想定されるケース

メール送信側はメール送信者の同意を得た場合は、①は問題無いと考えられる。
メール受信側は通信当事者の同意を得ていると考えられるため、①、および②は問題無いと考えられる。
①はドメインに係り、メール送信側は5条件のうち、
1. 実施後、個別に設定変更が可能
を満たせないため、整理が必要と考えられる。



メール受信者

送信ドメイン認証技術	*DKIM*	*SPF*	*DMARC*
電子メールの受信サーバにおいて、電子メールの送信ドメインを認証(チェック)し、認証できない場合には一定の措置を講ずる行為	整理済	整理済	整理可能 *(SPFとDKIM*を利用しているため)
ポリシー機能 (ドメイン所有者が受信者の「なりすましメール」の取り扱いに影響を与える)	ー	ー	企業 整理可能 *ISP*等 整理要
レポーティング機能 (受信者がドメインに関する認証結果をドメイン所有者へ通知する)	ー	ー	企業 整理可能 *ISP*等 整理要

本日の話

・ここ1年間の動向　（5分：北崎）
・DMARCのおさらい　（5分：櫻庭）
・DMARCの普及状況　（5分：北崎）
・導入する上での留意点
  - DKIM第三者署名問題　（3分：北崎）
  - 法的留意点　（5分：北崎）
  - 技術的留意点　（15分：ニコライ）
・質疑応答、ディスカッション　（2分）

本日の話

・ここ1年間の動向　（5分：北崎）
・DMARCのおさらい　（5分：櫻庭）
・DMARCの普及状況　（5分：北崎）
・導入する上での留意点
  - DKIM第三者署名問題　（3分：北崎）
  - 法的留意点　（5分：北崎）
  - 技術的留意点　（15分：ニコライ）
・質疑応答、ディスカッション　（2分）

▶ お知らせ

予告

RFCとMAAWG BCPの英日翻訳物を公開します。

http://salt.iajapan.org/wpmu/anti_spam/admin/tech/rfc/

・DMARC (RFC7489)

https://www.rfc-editor.org/rfc/rfc7489.txt

・Anti-Phishing Best Practices for ISPs and Mailbox Providers (MAAWG)

https://www.m3aawg.org/sites/default/files/M3AAWG_AWPG_Anti_Phishing_Best_Practices-2015-06.pdf

・M3AAWG Sender Best Common Practices (MAAWG)

https://www.m3aawg.org/sites/default/files/document/M3AAWG_Senders_BCP_Ver3-2015-02.pdf

(Backup)