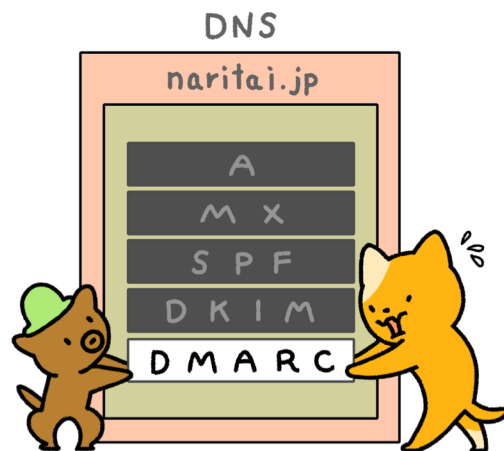


送信ドメイン認証技術 DMARC と DMARC レポートの活用



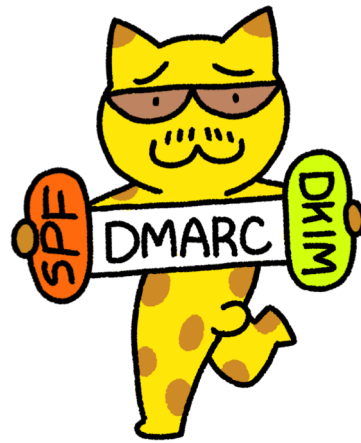
北川 直哉（国立大学法人 東京農工大学）

平野 善隆（株式会社 クオリティア）

本セッションの概要

- 講演者紹介
 - 北川 直哉：国立大学法人東京農工大学 大学院工学研究院・助教
 - 平野 善隆：株式会社クオリティア クラウドサービス開発本部・チーフエンジニア
- DMARC（およびSPF・DKIM）の概要解説（北川）
- DMARCの導入にあたっての技術的Tips（平野）
- DMARCレポートの概要解説とレポート分析（北川）
- パークドメインで受信したDMARCレポートについて（平野）
- 実際にレポートを受け取ってみましょう（北川）

DMARCとは



- Domain-based Message Authentication, Reporting, and Conformance

- <DMARCの2つの機能>

- ① SPF/DKIM検証のエラー状況(ruf)・統計情報(rua)のレポート機能

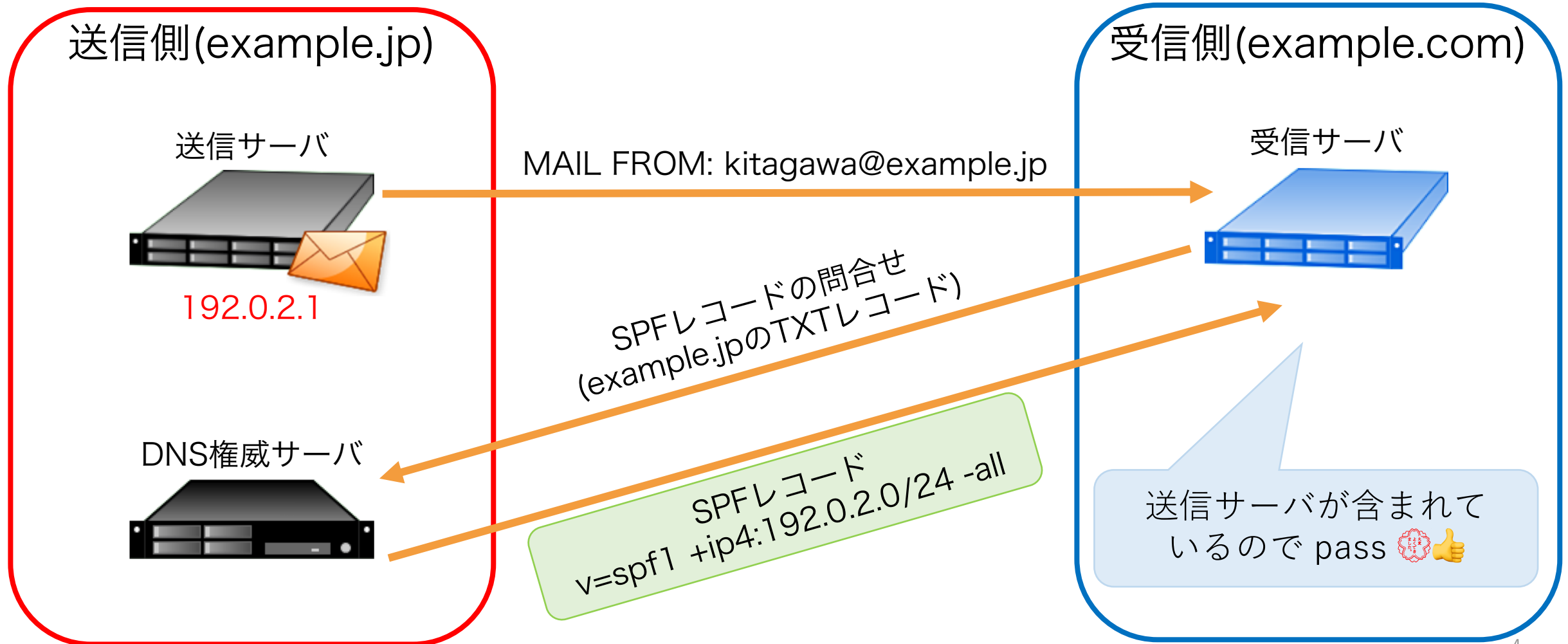
- 自ドメインにおけるSPF/DKIM検証の効果
 - 自ドメインをなりすましたメールの状況

- ② SPF/DKIM検証失敗メールの取扱いを送信側が指定する機能

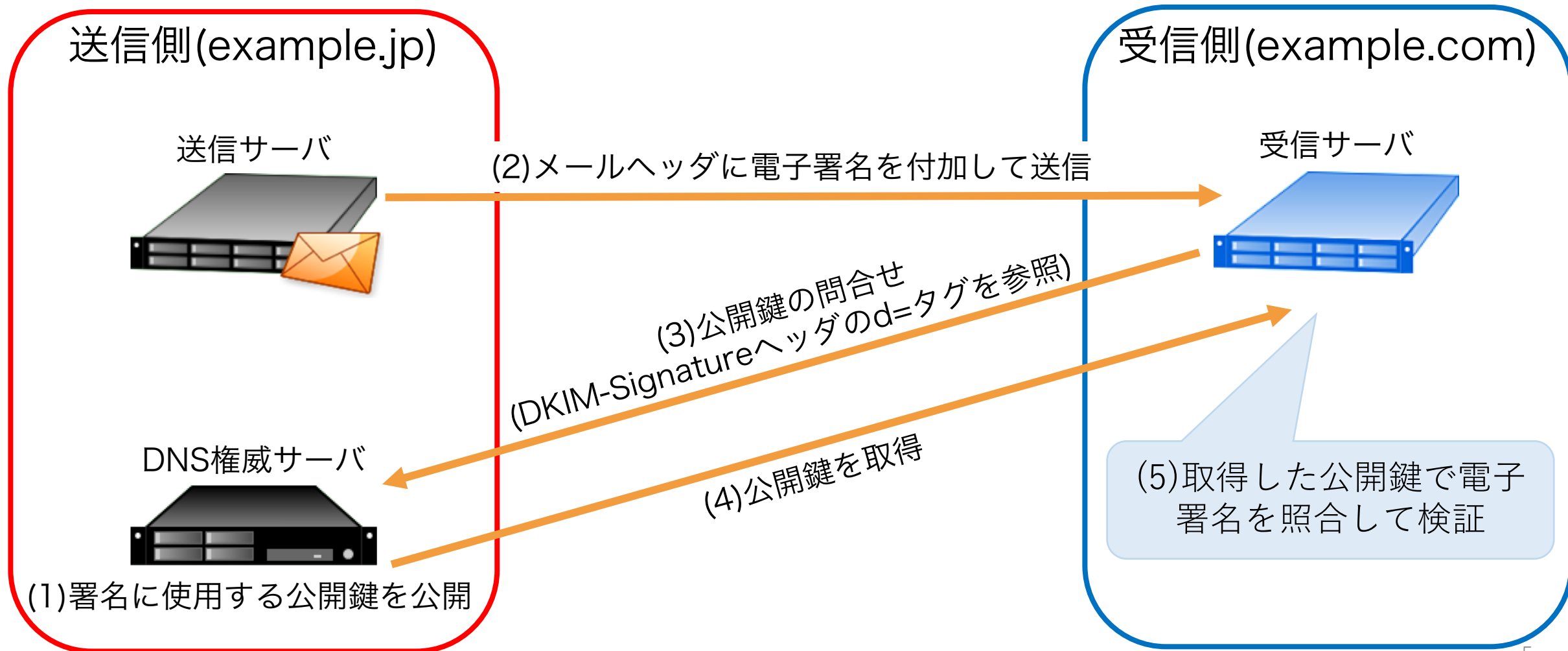
- none (処理方法を指定しない)
 - quarantine (隔離する)
 - reject (受信拒否する)

受信側はポリシーに基づいて
取扱い方法を決定

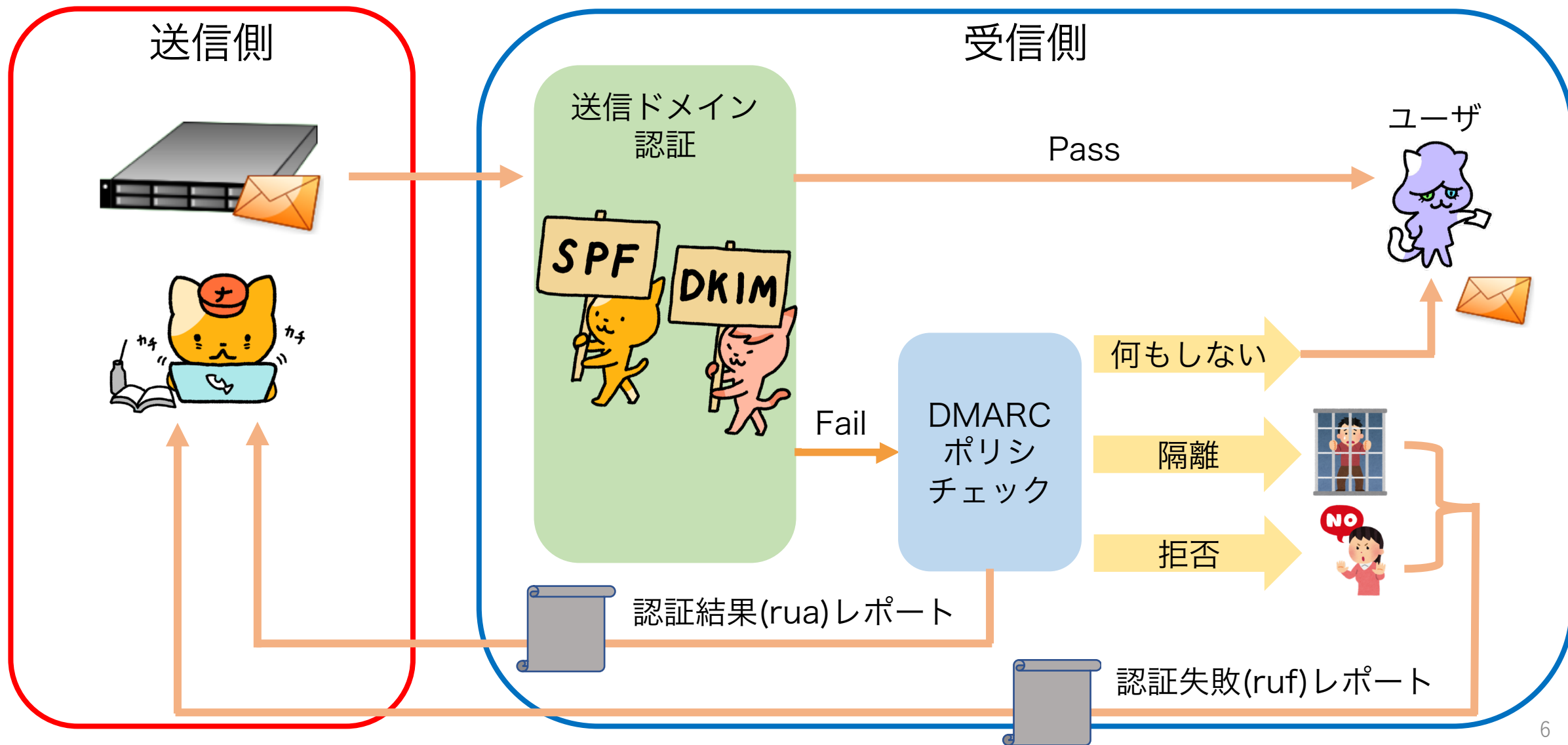
SPF(Sender Policy Framework)とは



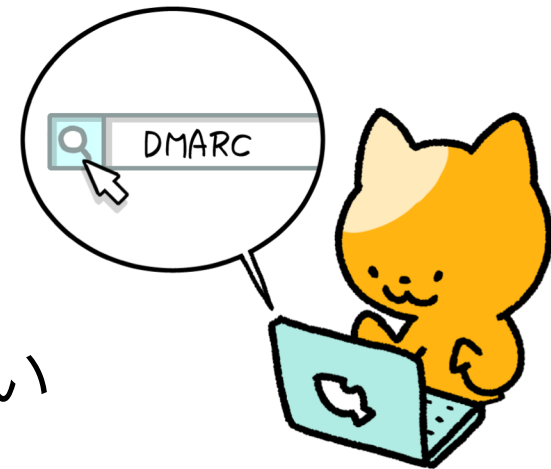
DKIM(Domainkeys Identified Mail)とは



DMARC検証とレポート送信の流れ



DMARC のアラインメント



- SPF/DKIMでは,
送信元ドメイン と **検証用ドメイン** は無関係でも良い
(第三者署名を許可)
 - 東京農工大学の例:
 - RFC5321.From(Header From)ドメイン = cc.tuat.ac.jp
 - DKIM検証ドメイン = cctuat.onmicrosoft.com

正しいドメインの組を知る術がないため
偽の署名がついたなりすましメールも
検証に成功してしまう恐れがある

- DMARCでは第三者署名を許可しない = 認証失敗(fail)となる
→ **より強固な送信ドメイン認証**といえる

DMARCレポート (rua)の構造

XML形式

Report generator metadata

DMARC policy

DKIM and SPF results

All the authentication results

レポートのメタデータ
組織名, メールアドレス,
レポートID, 期間, など

DMARCポリシー
ドメイン名, ポリシ(p=),
レート(pct=), アライメント, など

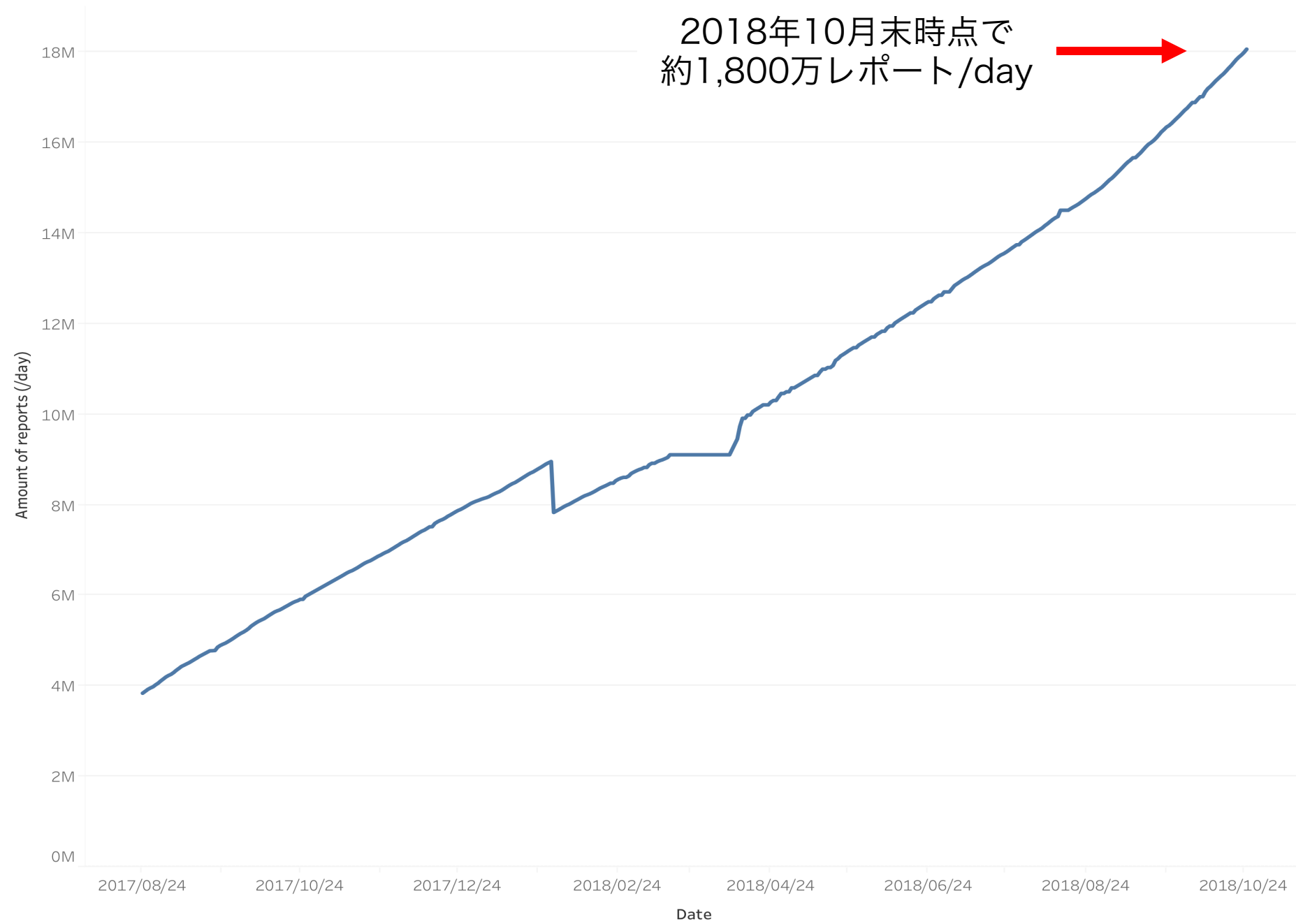
評価結果
ドメイン名, IPアドレス,
評価内容, 理由, 各認証結果, など

ドメイン認証結果
認証ドメイン, 鍵のセクタ,
認証結果, など

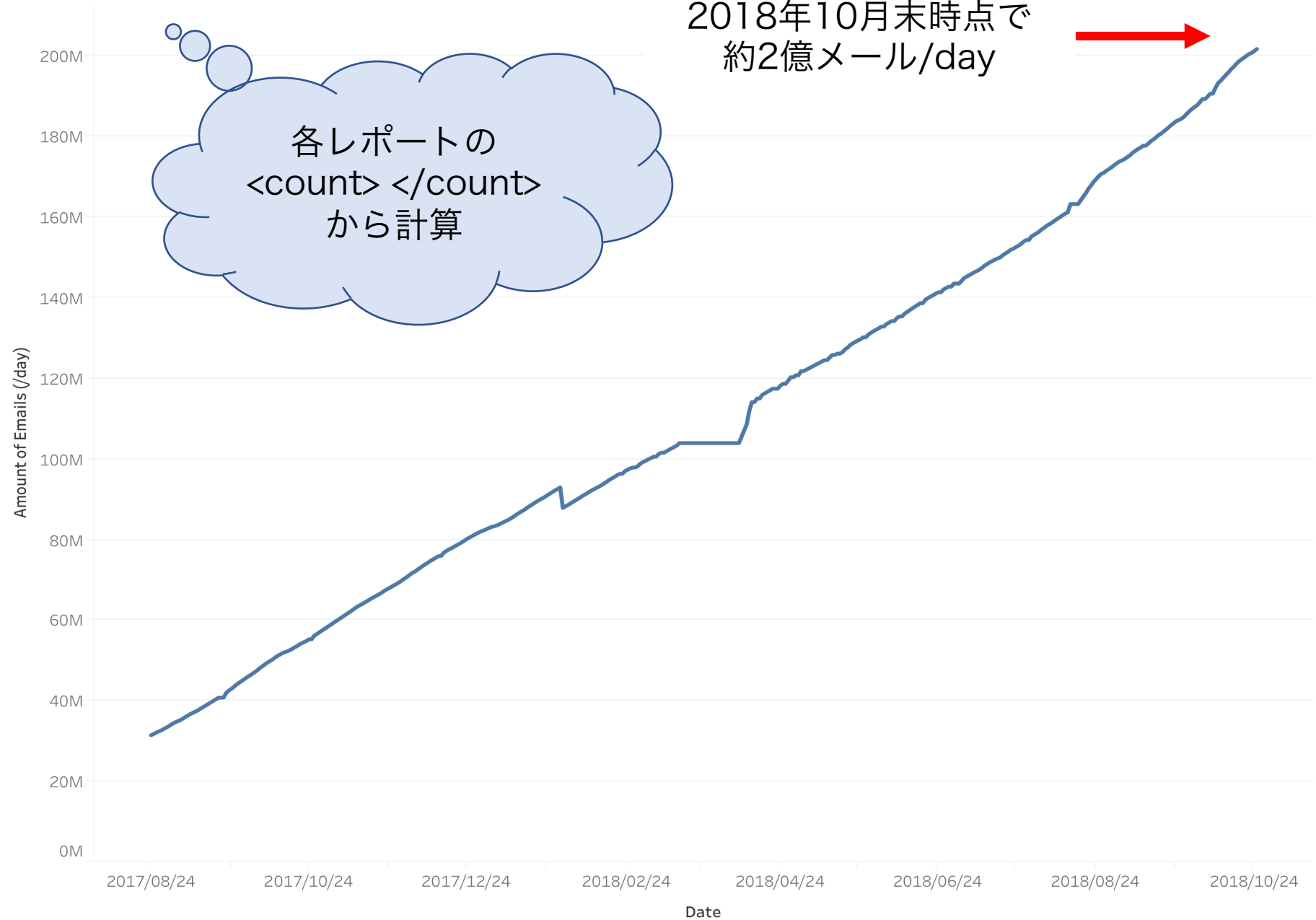
DMARCレポートの統計分析

ある組織に送られてきたDMARCレポートを約14ヶ月分分析してみました
(p=none のドメイン)

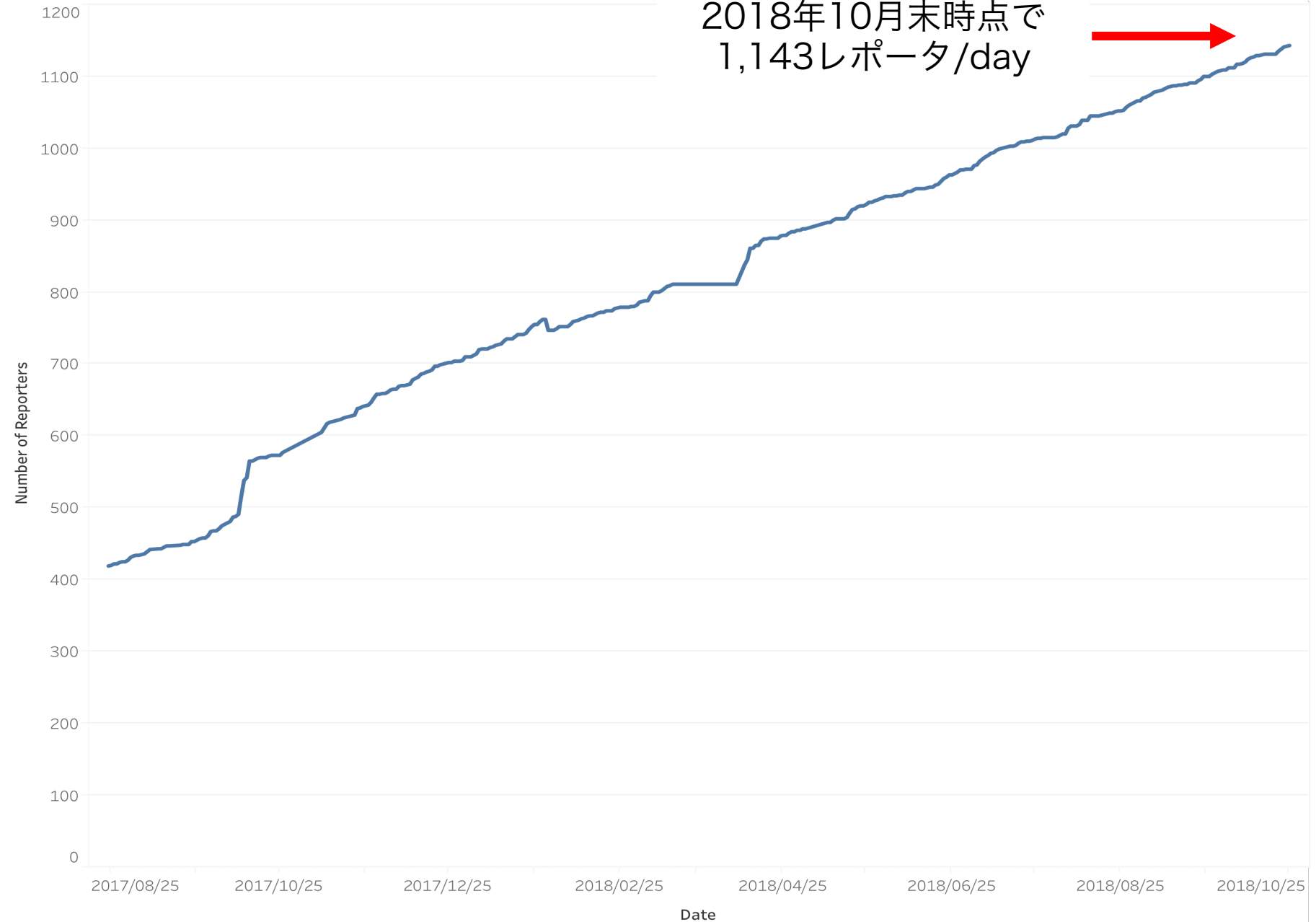
<総DMARCレポート数>



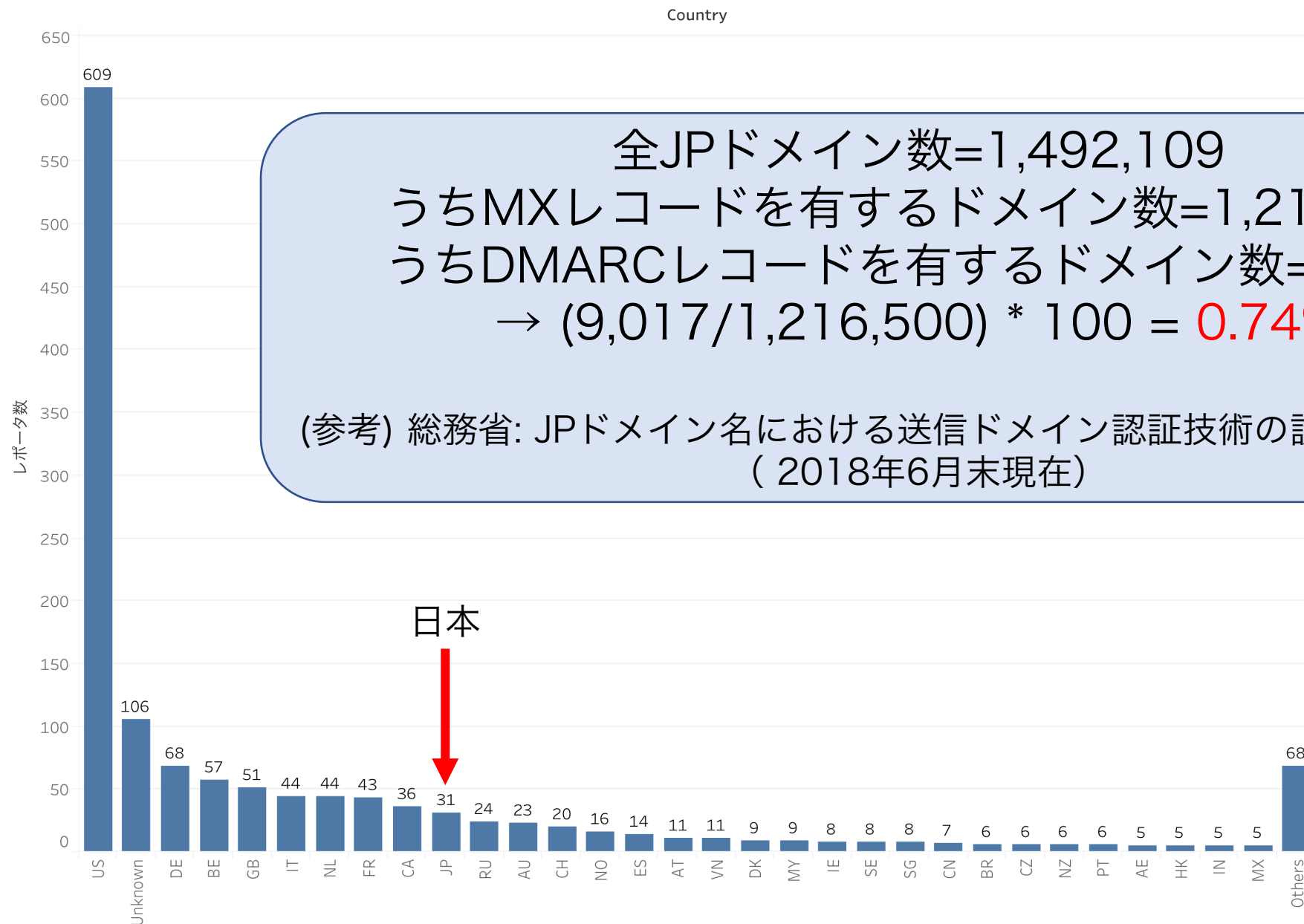
< 総メール通数 >



<総レポート数の推移>



<国別レポート数(2018/10/25)>



全JPドメイン数=1,492,109

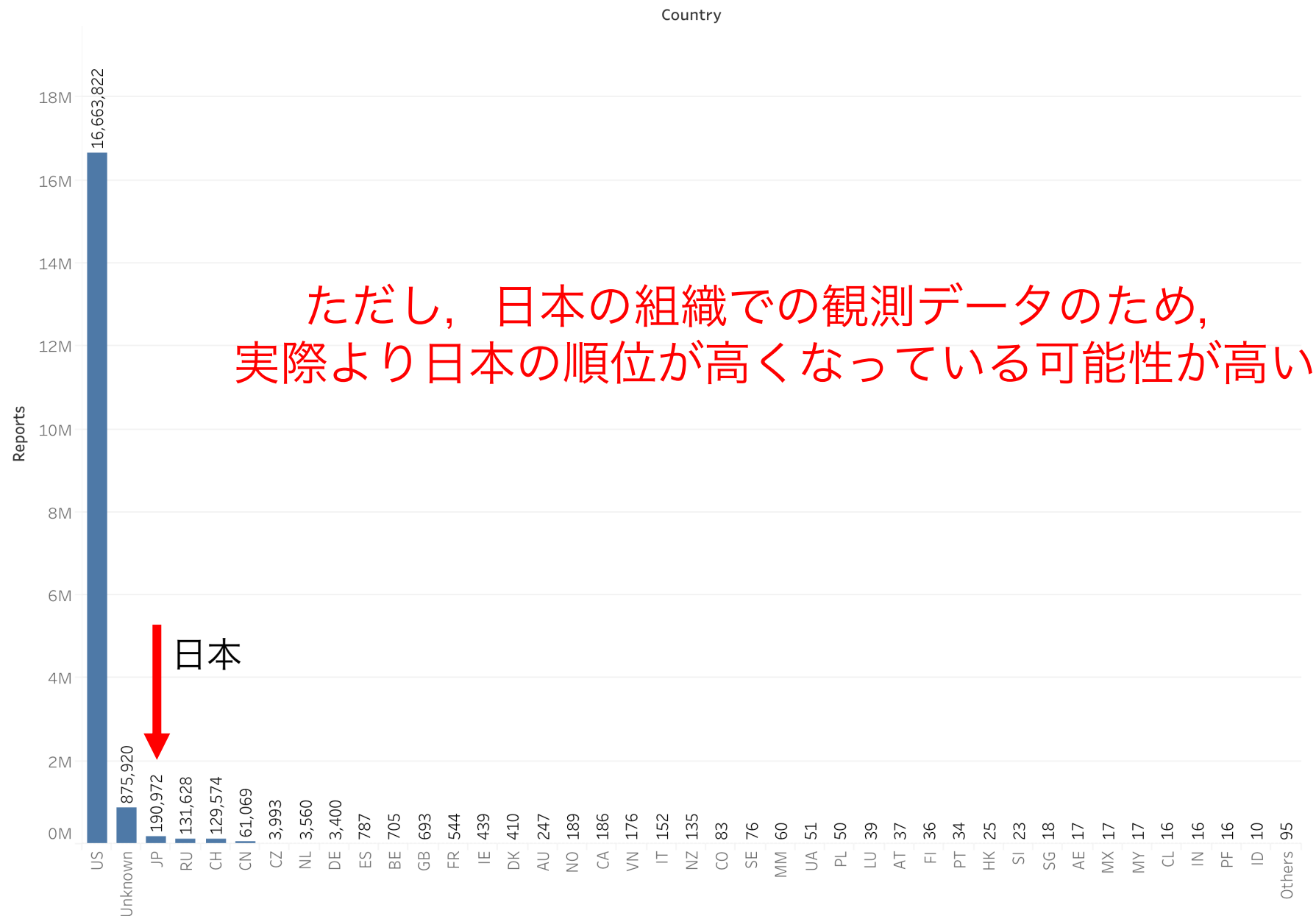
うちMXレコードを有するドメイン数=1,216,500

うちDMARCレコードを有するドメイン数=9,017

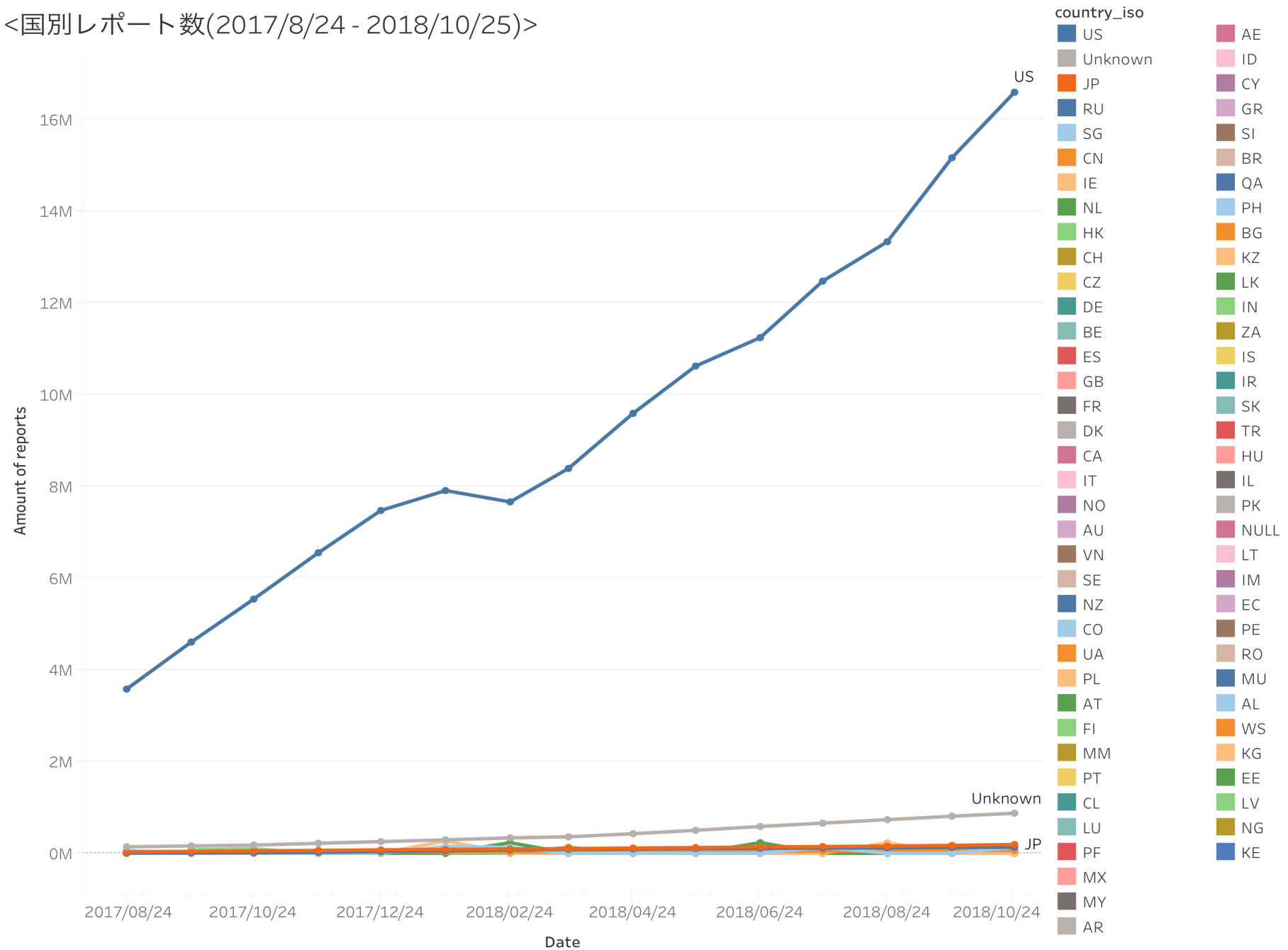
→ $(9,017 / 1,216,500) * 100 = 0.74\%$

(参考) 総務省: JPドメイン名における送信ドメイン認証技術の設定状況の調査
(2018年6月末現在)

<国別レポート数分布>



<国別レポート数(2017/8/24 - 2018/10/25)>



DMARCレポートをよく見ると…

- DMARCの処理に矛盾が生じているレポートの存在
- 送信側が宣言している policy と実際の処理の違い
(p=quarantine, p=reject を宣言している場合のみ)

なども見えてきます

DMARC処理に矛盾が生じているレポートの例

```
<?xml version="1.0" encoding="UTF-8" ?>
```

```
<feedback>
```

(snip)

```
<policy_evaluated>
```

```
<disposition>none</disposition>
```

```
<dkim>pass</dkim>
```

```
<spf>pass</spf>
```

(snip)

DMARC-SPF
の結果

DMARC-DKIM
の結果

(snip)

```
<auth_results>
```

```
<spf>
```

SPF の結果

(snip)

```
<result>fail</result>
```

```
</spf>
```

```
<dkim>
```

(snip)

```
<result>fail</result>
```

(contd)

DKIM の結果

DMARC-SPFの処理に矛盾があったレポート

(2018/10/25日分：1,143レポート中12レポートで矛盾あり)

レポート A	7,525/10,738 通
レポート B	4/46 通
レポート C	227/228 通
レポート D	1/452 通
レポート E	1/3 通
レポート F	1/1 通
レポート G	1/5 通
レポート H	21/142,627 通
レポート I	1/1 通
レポート J	6/21 通
レポート K	31/31 通
レポート L	4/4 通

DMARC-DKIMの処理に矛盾があったレポート

(2018/10/25日分：1,143レポート中35レポートで矛盾あり)

レポート 1	177/301,529 通
レポート 2	103/109,427 通
レポート 3	3/3 通
レポート 4	246/373 通
レポート 5	2/2 通
レポート 6	2/25 通
レポート 7	8,478/10,738 通
レポート 8	3/4 通
レポート 9	7/13,255 通
レポート10	78/380 通
レポート11	18,725/192,395,820 通
レポート12	2/5 通

(contd)

DMARCポリシーと実際の処理の違い

- ここまでとは別の組織(p=reject)に送られてきたレポートで調査
(レポータ数13, レポート数8,155, メール総数24,081/day(2018/10/25))
- 強いポリシー(p=reject や p=quarantine)を宣言した場合でも,
例えば以下の理由で, より弱いポリシーに下げられることがあります
(この理由もDMARCレポートのdescription欄に書かれています)
 - ホワइटリストに含まれているから
 - 転送サーバリストに含まれているから など
- 反対に強いポリシーに変更される場合はこれまで観測していません
 - 例: none → quarantine or reject
quarantine → reject

公開ポリシーvs解釈と実際の処理(2018/10/25)

レポート名	合計メール数	r_r	r_q	r_n	q_r	q_q	q_n	n_r	n_q	n_n
レポート a	12			12						
レポート b	14	14								
レポート c	415			415						
レポート d	75	75								
レポート e	80	47				19				14
レポート f	990	990								
レポート g	1									1
レポート h	118	1	1			19				97
レポート i	1						1			
レポート j	22,312	8098	5569	93		230	3611			4711
レポート k	1									1
レポート l	61	26		11		7				17
レポート m	1	1								

DMARCレポートからわかること・できること

【基礎編】

- 自ドメイン名を偽称したメールがどこにどれだけ送られているのか
- 自ドメインの送信ドメイン認証の効き目や設定の正確性

【応用編】

- データ解析による False Positive / False Negative の軽減
(例えば転送や ML 配送で生じていた False Positive の検出)
- 機械学習や確率論等を用いて上記の解析で得られた情報を高度化

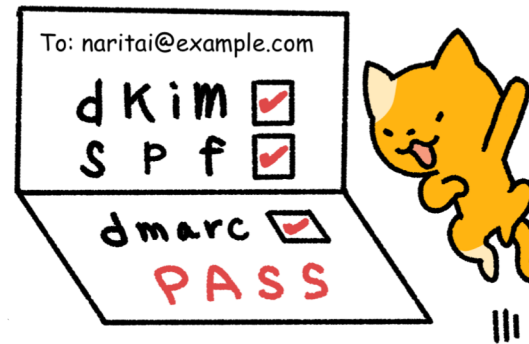
(レポート受信のためにも)まずは弱いポリシーから始めて
徐々に強いポリシーに変更していくのがオススメです

DMARC レポートを受け取ってみましょう

1. レポートを受信するメールアドレスを準備する
例：rua@example.jp (rua レポート用アドレス)
ruf@example.jp (ruf レポート用アドレス)
2. DNS に DMARC レコードを追加し， メールアドレスを記述する
例：_dmarc.example.jp IN TXT “v=DMARC1; p=reject;
rua=mailto:rua@example.jp; ruf=mailto:ruf@example.jp”
3. DMARC レポートを送ってくれる組織(ナリタイ等)にメールを送る
4. ワインを飲みに行く 🍷 🍷 (一日ほど待つ)
5. 1.で設定した受信用メールアドレスを確認する

なりすまし対策ポータル「ナリタイ」

- 今日お話した DMARC をはじめ，SPF や DKIM の解説も充実
(方式の解説から設定方法まで網羅的に解説)
- 「DMARC/DKIM/SPF CHECK」で設定確認が可能
 - さらに今秋，check@naritai.jp に空メールを送ると， rua/ruf レポートを送信する機能が追加されました！



- 詳しくは <https://www.naritai.jp/> をご覧ください