OD-07/D3-08

DMARCレポートの概要と利用方法の実際

2017年2月26日(大阪）、29日(東京)

JIPDEC（じぷでっく）
【法人番号：1 0104 0500 9403】
(一般財団法人日本情報経済社会推進協会)
インターネットトラストセンター　企画室
室長　大泰司　章（おおたいし　あきら）

概要

日本国内でもDMARCレポートを提供するサービスが立ち上がりつつあります。

このセッションでは、サービスを提供している側と、利用している側の両者の立場から、事例を紹介します。

また、将来の展望について語ります

講演者

加瀬　正樹（株式会社TwoFive）

畠山　昌録（Easy Solutions Japan 合同会社）

大泰司　章（JIPDEC）

本日の流れ

１．自己紹介など（3名、10分）

２．DMARC レポートを生データをもとに解説
（加瀬、10分）

３．DMARC レポートの活用と課題
（畠山、10分）

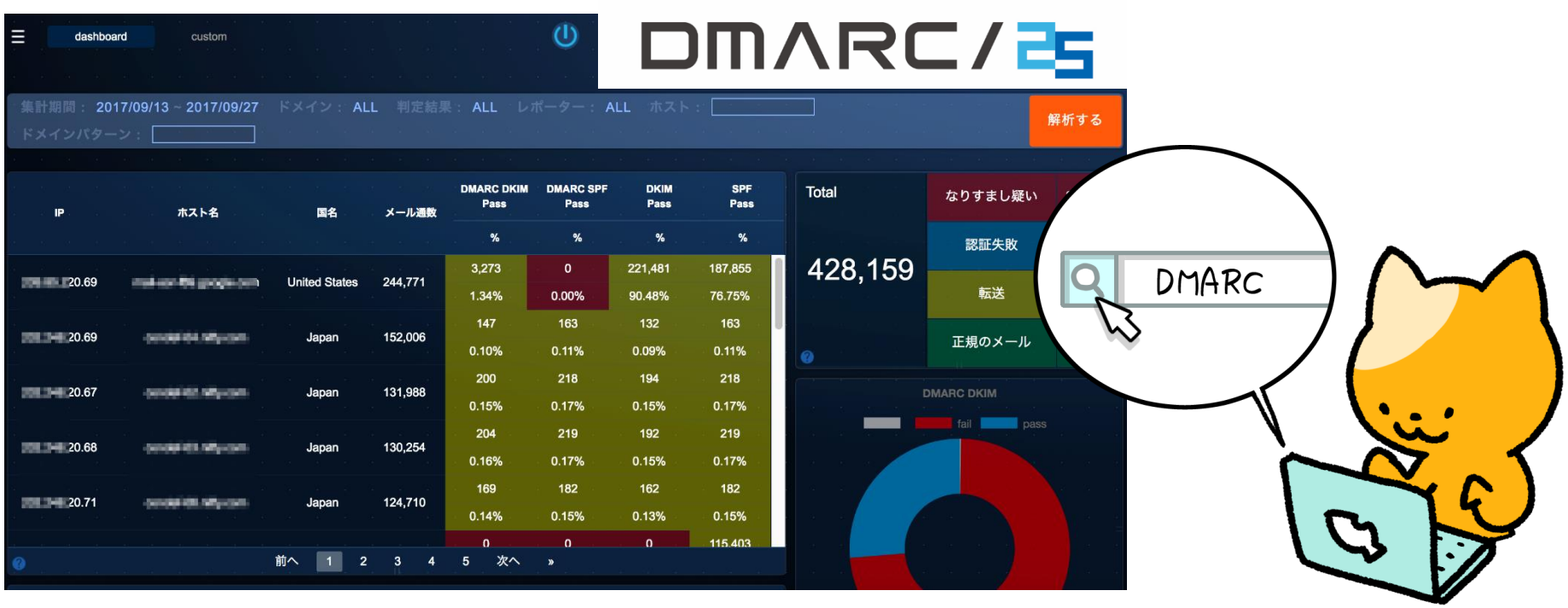
４．事例紹介や質疑応答など
（大泰司、10分）

株式会社TwoFive
TwoFive,Inc.

設立	2014年
本社所在地	東京 – 日本
フォーカス	大規模電子メールシステム向け 製品・コンサルティング インターネットレピュテーション情報
主要取引先 (敬称略/50音順)	■NECソリューションイノベータ株式会社 ■株式会社日立ソリューションズ ■東芝デジタルソリューションズ株式会社 ■日本ヒューレットパッカード株式会社 ■ブロードバンドセキュリティ株式会社

クラウド型サービス – DMARC / 25

“ DMARC でドメインを保護したい ”
“ なりすまし対策をはじめたい ”



自己紹介

加瀬　正樹（かせ　まさき）

2000年4月　　ニフティ株式会社入社

2017年5月　　株式会社 TwoFive 入社

その他

迷惑メール対策推進協議会 技術WG 副主査

迷惑メール対策委員会 メンバー

Email Security Conference プログラム委員

JIPDEC 客員研究員

会社概要

Easy Solutions, Inc

設立：	2007年
CEO：	Ricardo Villadiego
所在地：	アメリカ合衆国　フロリダ
営業拠点：	日本・アトランタ・ロンドン・ブラジル ボゴタ（コロンビア）・メキシコなど
主要株主：	Medina Capital Partners 2013年5月に$11 million/Series Bの出資
事業内容：	ネット詐欺対策ソリューションの提供 380社以上の事業者 1億人以上のユーザーを保護

連携している外部団体・協会など

AMERICAN BANKERS ASSOCIATION

APWG

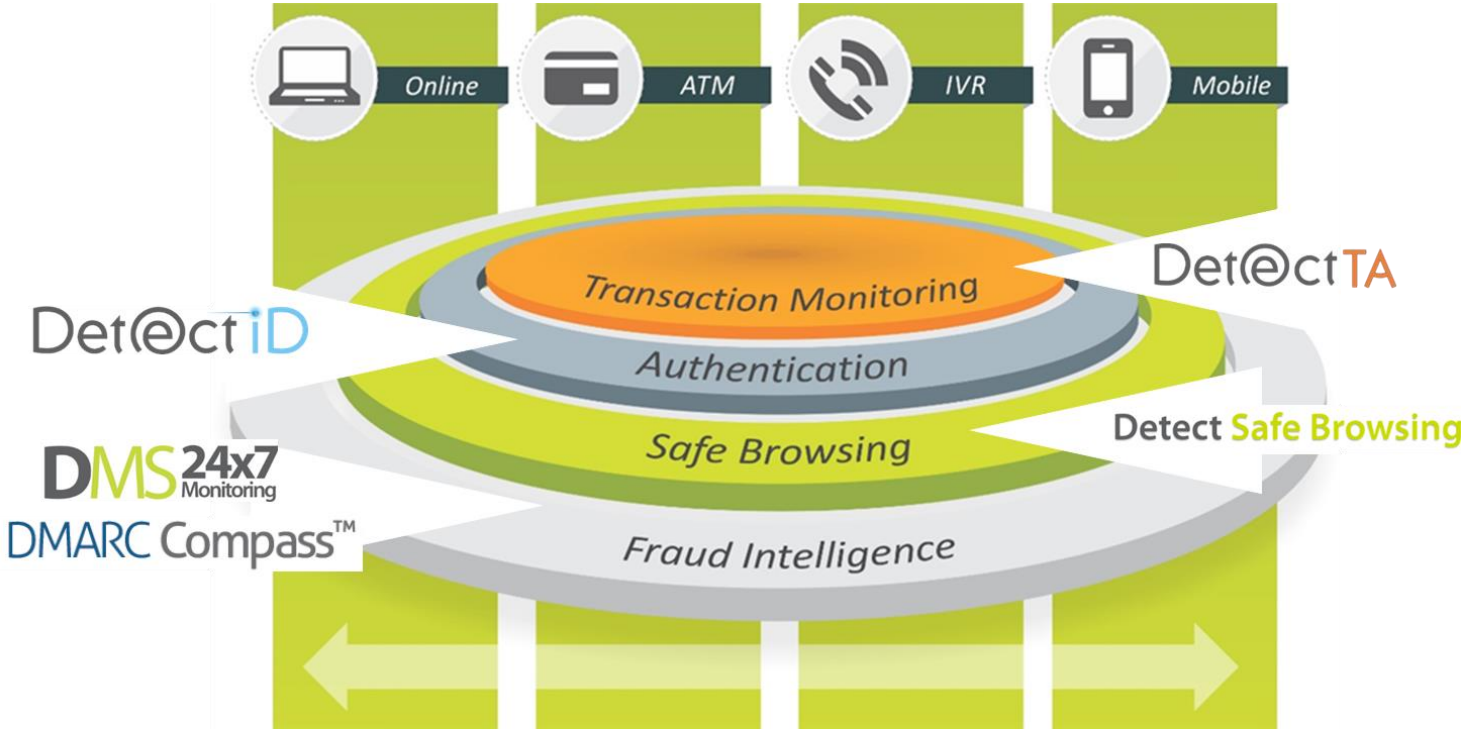
Anti-Phishing Working Group
（APWG）

fido alliance

FIDO Aliance
（First IDentity Online）

Our Approach: Total Fraud Protection®

進化する犯行には、完全な防御策は存在しません。
Total Fraud Protection:ネット詐欺総合対策（多層防御アプローチ）が当社の詐欺対策のコンセプトです。



マルチチャネル

マルチレイヤー

高い可視性

相互連携

自己紹介

畠山　昌録（はたけやま　まさふみ）

日本ベリサイン、シマンテック等のセキュリティベンダーで金融機関むけ営業

2014年10月　　Easy Solutions JAPAN
日本での事業展開開始

その他

金融ISAC / JC3 会員

日本カード情報セキュリティ協議会（JCDSC）ベンダー部会メンバー

迷惑メール対策推進協議会　技術WGメンバー

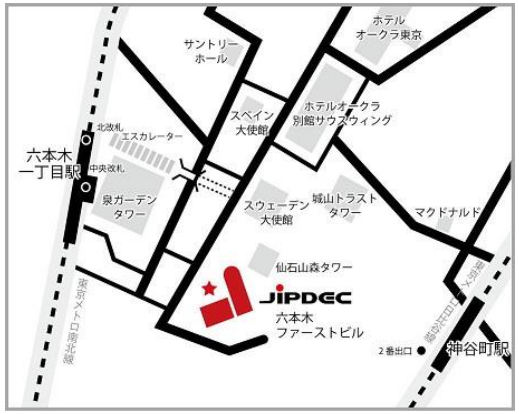
JIPDEC概要

- **名称**　JIPDEC【法人番号1010 4050 09403】（じぷでっく）
  一般財団法人日本情報経済社会推進協会
  Japan **I**nstitute for **P**romotion of **D**igital **E**conomy and **C**ommunity

  以前は、財団法人日本情報処理開発協会
  Japan **I**nformation **P**rocessing **DE**velopment **C**orporation

- **設立**　1967（昭和42）年12月20日

- **基本財産**　39億9,900万円
- **事業規模**　25億9,560万円（平成29年度予算）
- **職員数**　102名（平成29年7月現在）



JIPDEC事業案内

●制度

- プライバシーマーク制度の運用
- 電子署名・認証制度に基づく特定認定業務の調査
- ISMS/ITSMS/BCMS/CSMS適合性評価制度の運営

●サービス

インターネットトラストセンター

- **JCAN証明書の普及**
- **サイバー法人台帳ROBINSの運用**
- **JCANトラステッド・サービス登録**
- **メールなりすまし対策「安心マーク」の普及**

●提言

- 電子情報の利活用基盤の整備のための調査研究
- 産学官連携による課題の検討、政府への提言
- IT資産マネジメントに関する調査研究
- 電子情報利活用に関するさまざまな情報提供

プロフィール

JIPDEC（じぷでっく）
【法人番号：1 0104 0500 9403】
(一般財団法人日本情報経済社会推進協会)
インターネットトラストセンター　企画室
室長　大泰司　章（おおたいし　あきら）

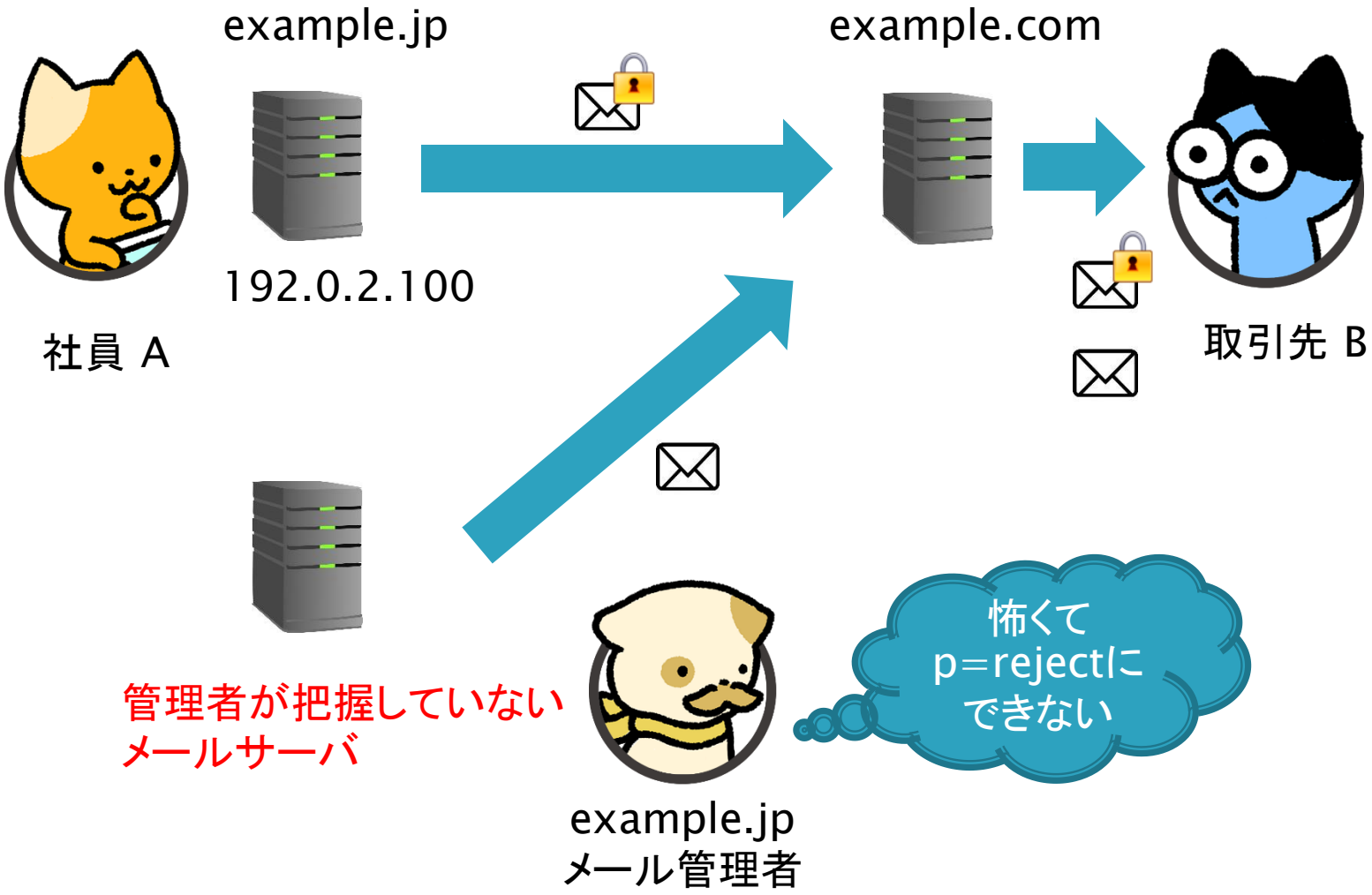
三菱電機（株）、日本電子計算（株）を経て、JIPDECに参画。

営業現場で長年にわたって大量の紙の契約書等取引文書と格闘し、社会インフラを変える必要性を痛感。JIPDECに移った後、電子契約元年プロジェクトを立ち上げ、全ての取引文書の電子化、あわせて取引慣行の改革を目指して活動中。

また、情報発信者の信頼性という観点から、取引文書だけでなく、インターネット上のメールやWebサイトのなりすまし対策を推進している。

DMARC レポートの意義

ドメインは適切に管理されているか？



DMARC 対応のステップ

1. DMARC を宣言し、レポートを受信する
2. メールサーバの管理を整える
3. p=quarantine / reject に切り替える

DMARC レポートの詳細

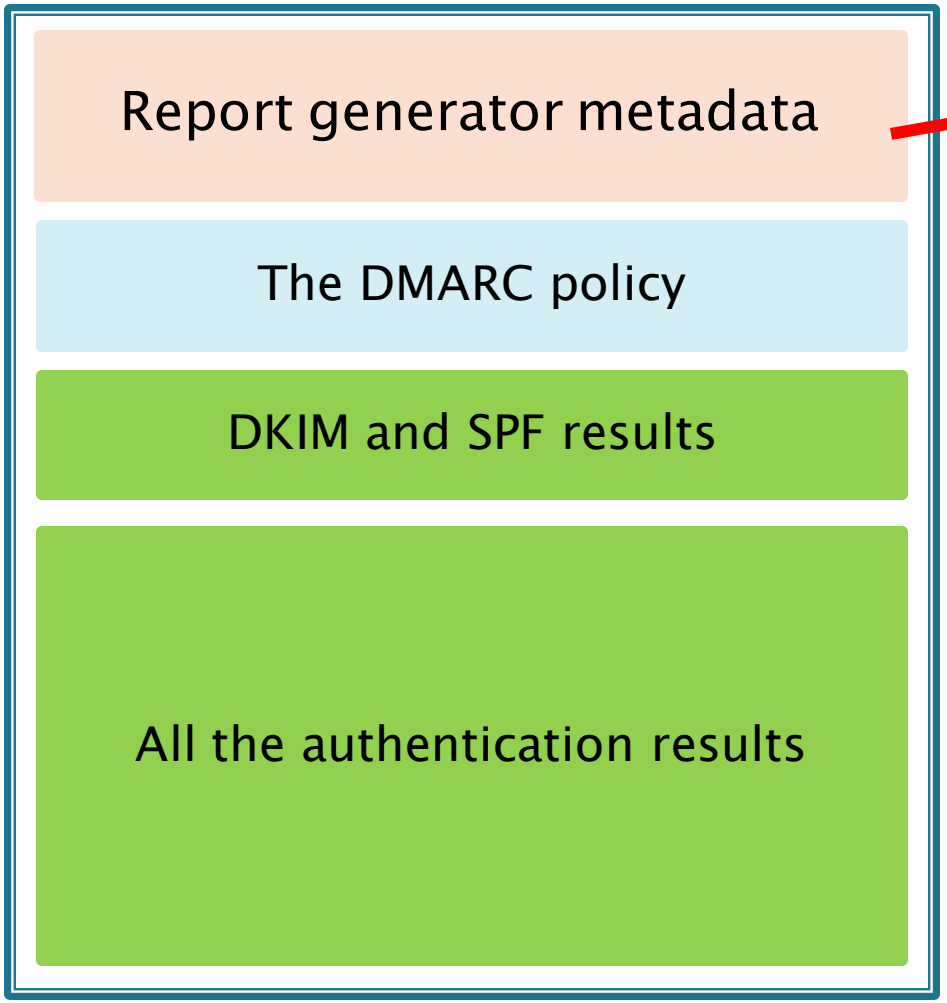
DMARC レポートを取得する方法

1. 受信用のメールアドレスを準備する
2. DNS にメールアドレスを記述する
3. Gmail などにメールを送信する

翌日まで待つ

4. 受信用メールアドレスを確認する

レポートの読み方（XML）

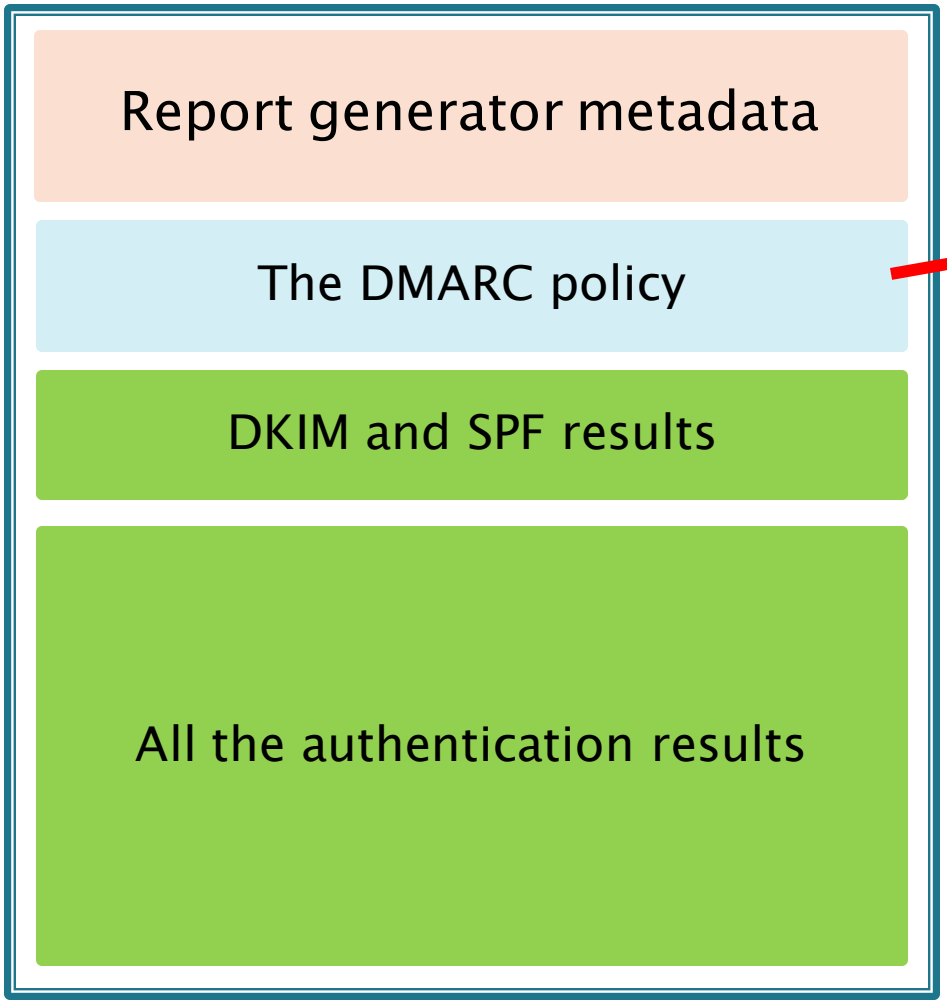


レポートのメタデータ

組織名
メールアドレス
レポート ID
範囲
etc

参考: https://dmarc.org/dmarc-xml/0.1/ru

レポートの読み方（XML）

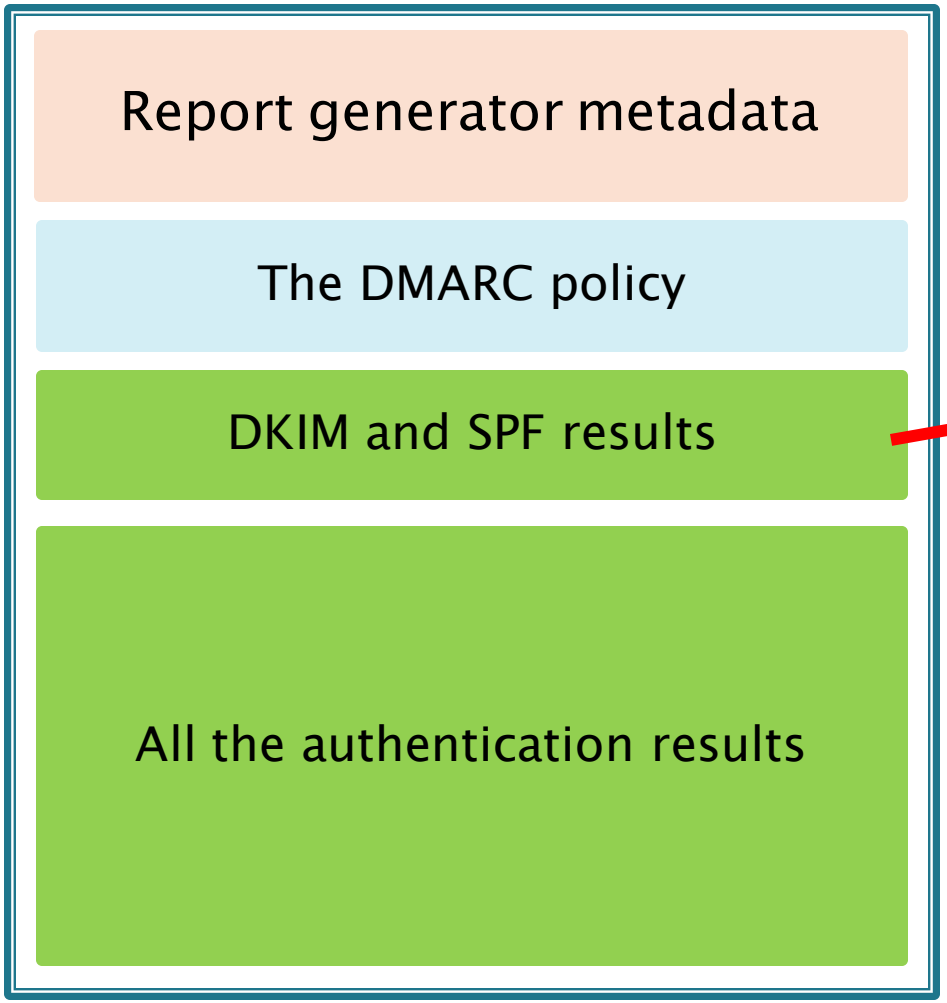


DMARC ポリシー

ドメイン名
ポリシー（p=）
レート（pct=）
アラインメント
etc

参考: https://dmarc.org/dmarc-xml/0.1/ru

レポートの読み方（XML）

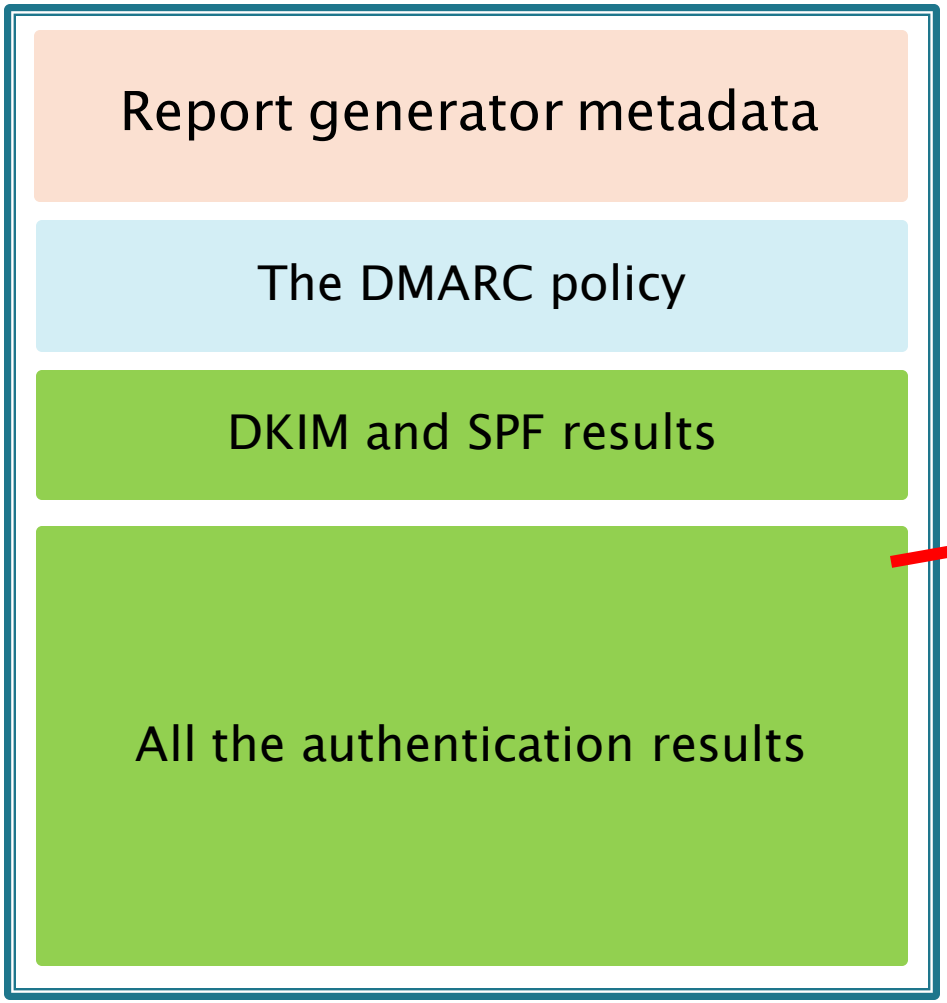


評価結果

ドメイン
IPアドレス
評価内容
処理内容
理由
それぞれの認証結果

参考: https://dmarc.org/dmarc-xml/0.1/ru

レポートの読み方（XML）



ドメイン認証結果

認証ドメイン
鍵のセレクター
認証結果

参考: https://dmarc.org/dmarc-xml/0.1/ru

レポートの読み方（XML）

DKIM and SPF results

```
<source_ip>192.0.2.123</source_ip>
<count>2</count>
<policy_evaluated>
  <disposition>none</disposition>
  <dkim>fail</dkim>
  <spf>fail</spf>
  <reason>
    <type>local_policy</type>
    <comment>xoar=pass</comment>
  </reason>
</policy_evaluated>
```

192.0.2.123 から2通のメールが着信。DKIM は fail SPF は fail した。なお、XOAR* は pass している模様。

* X-Original-Authentication-Result

参考: https://dmarc.org/dmarc-xml/0.1/ru

レポートの読み方（XML）

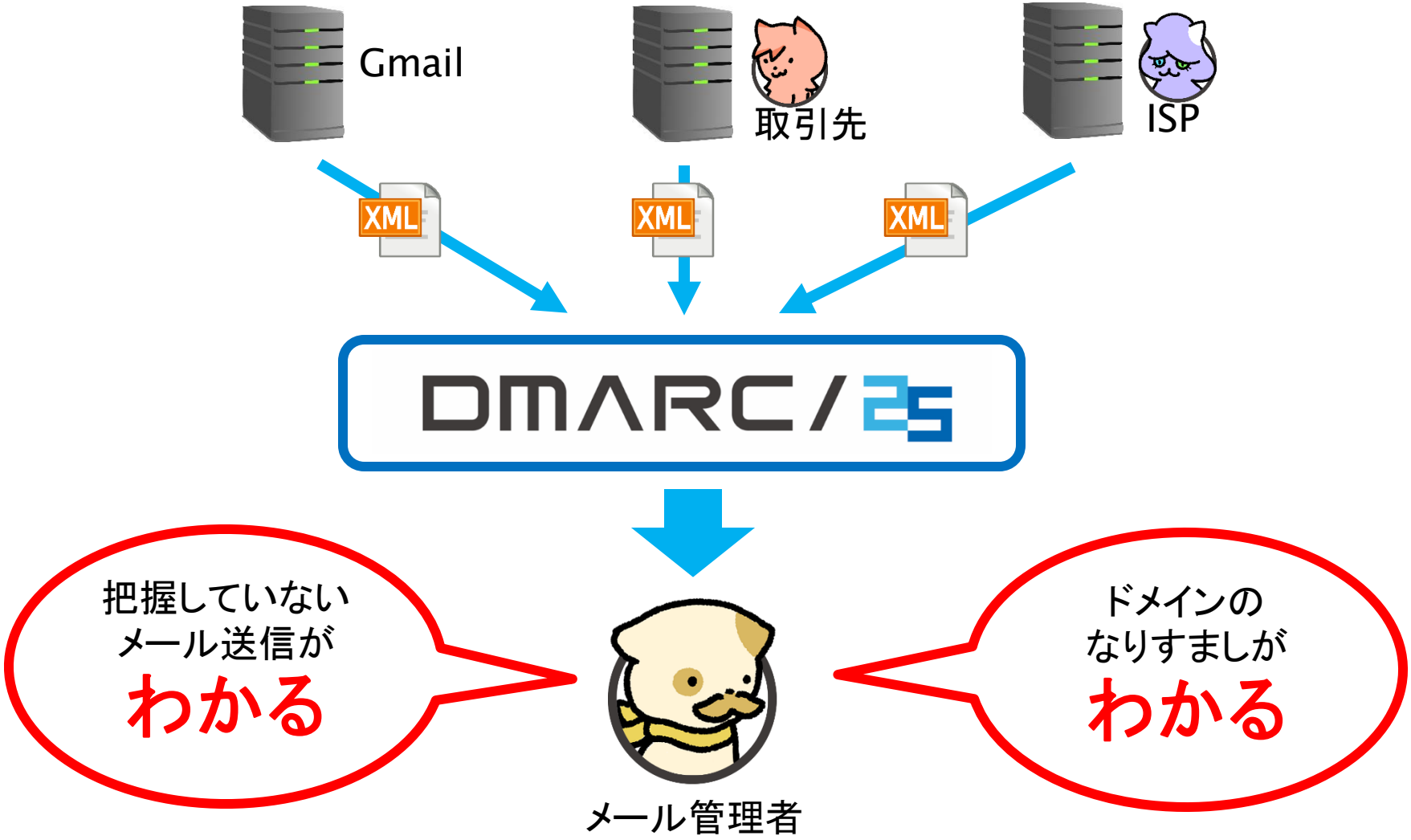
All the authentication results

ドメインは example.com DKIM は twofive25.example.com で署名され、pass した。セレクターは 20170901。SPF は example.net のドメインで pass した。

```
<identifiers>
  <header_from>example.com</header_from>
</identifiers>
<auth_results>
  <dkim>
    <domain>twofive25.example.com</domain>
    <result>pass</result>
    <selector>20170901</selector>
  </dkim>
  <spf>
    <domain>example.net</domain>
    <result>pass</result>
  </spf>
</auth_results>
```

参考: https://dmarc.org/dmarc-xml/0.1/ru

実際には SaaS サービスを活用



実際には SaaS サービスを活用

DKIM and SPF results

All the authentication results

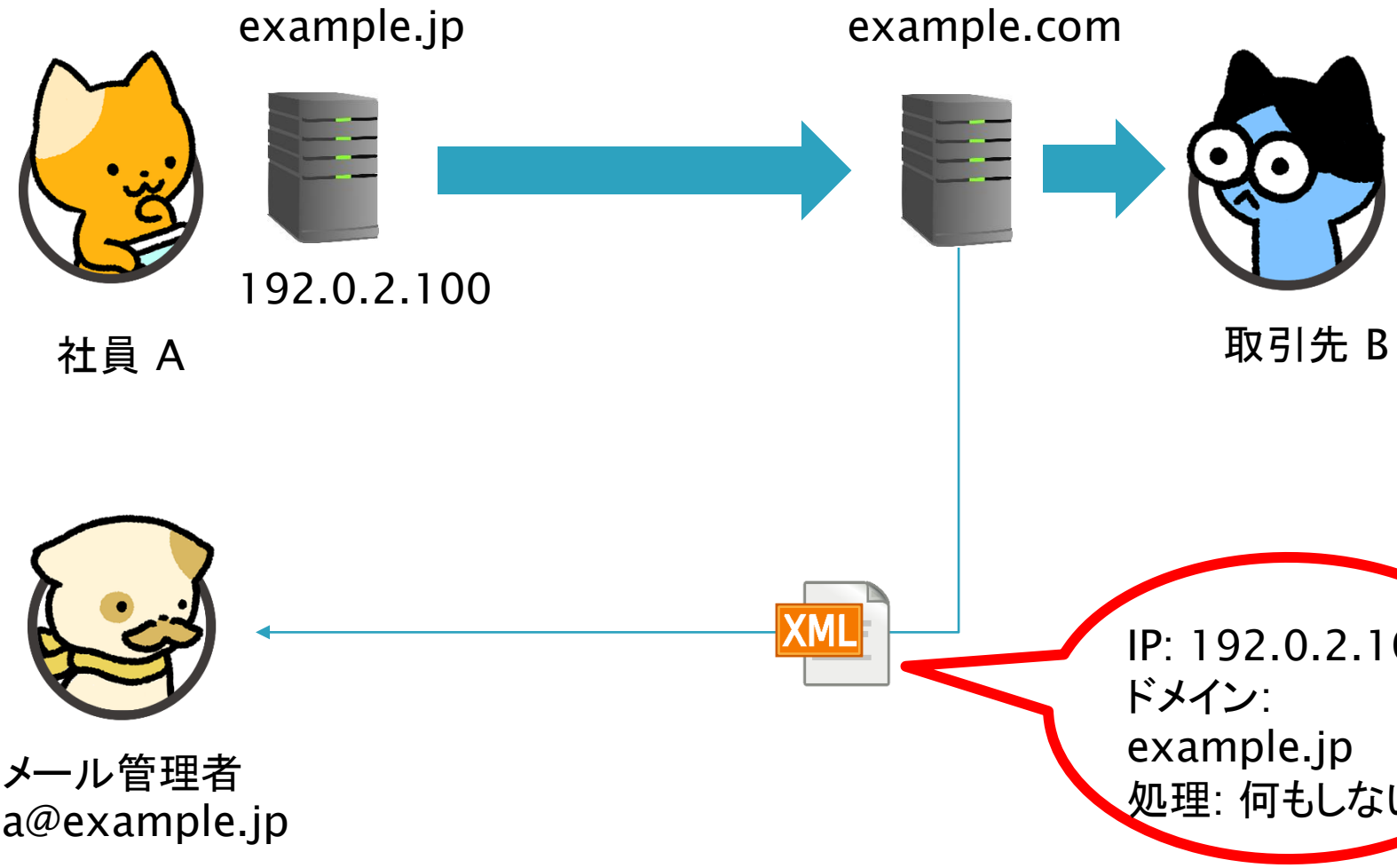
参考: DMARC / 25 ダッシュボードより

実際には SaaS サービスを活用

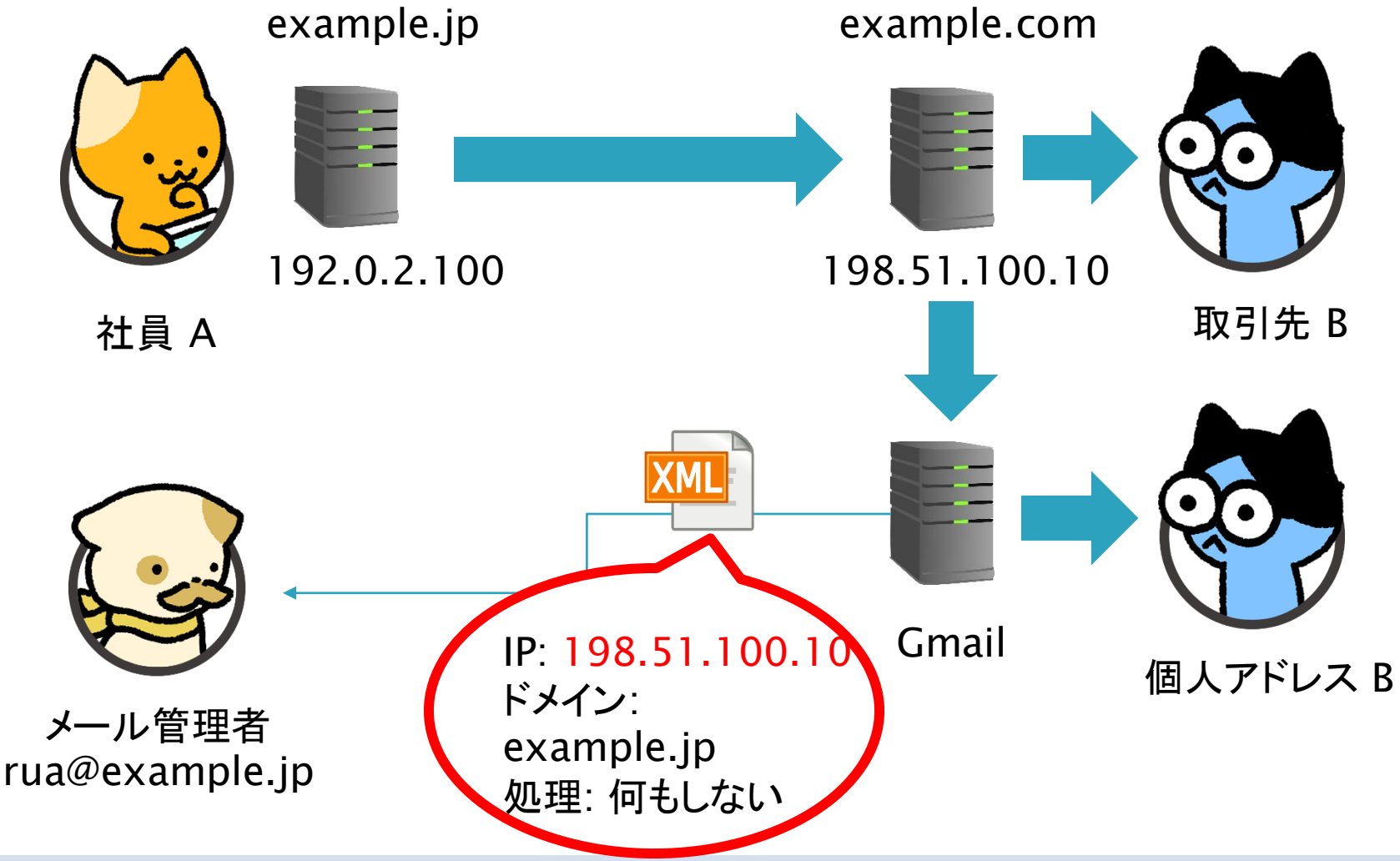
参考: DMARC / 25 ダッシュボードより

DMARC からわかる経路

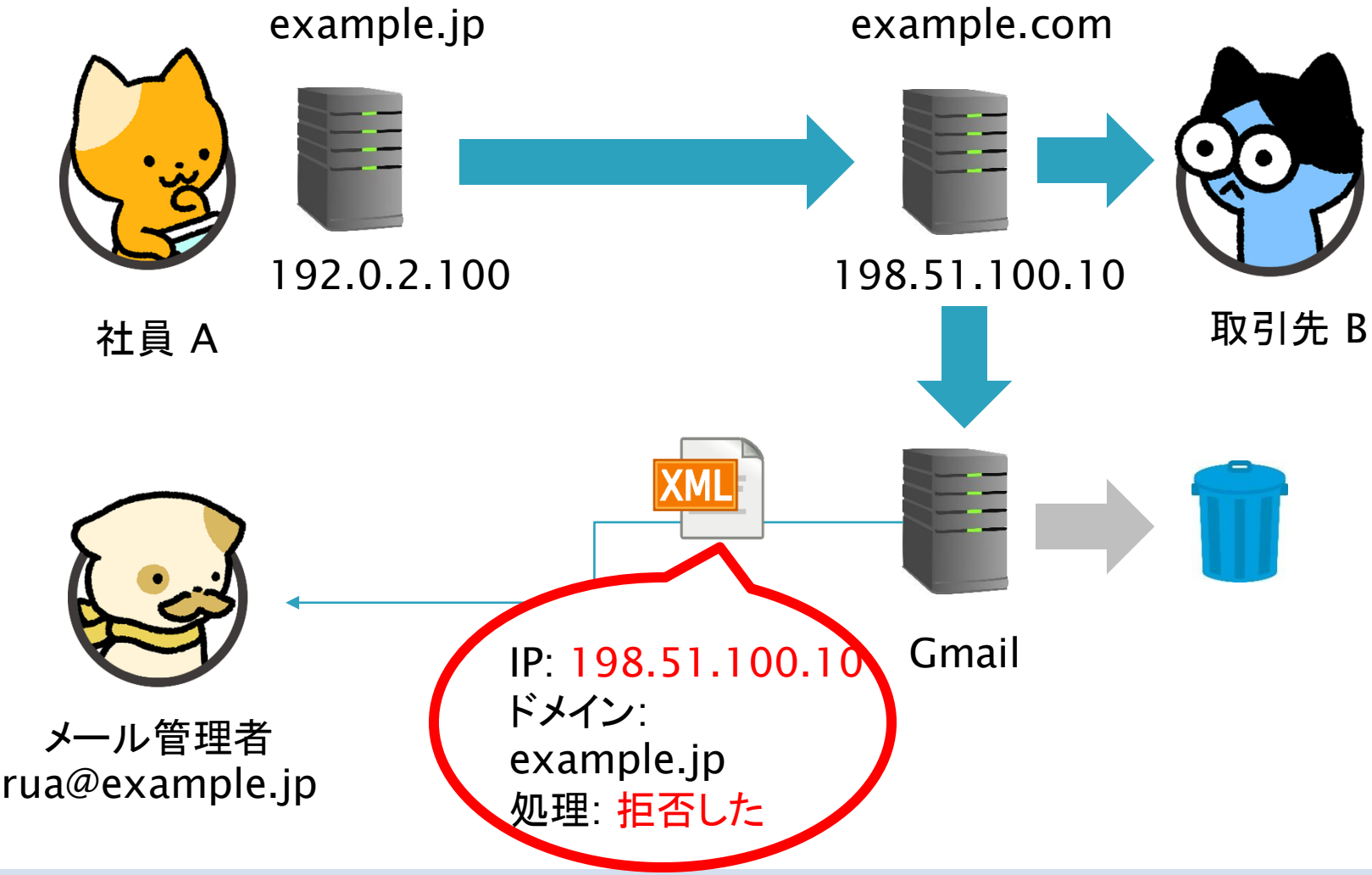
Case1: 通常


example.jp
example.com
192.0.2.100
社員 A
取引先 B
XML
メール管理者
rua@example.jp
IP: 192.0.2.100
ドメイン:
example.jp
処理: 何もしない

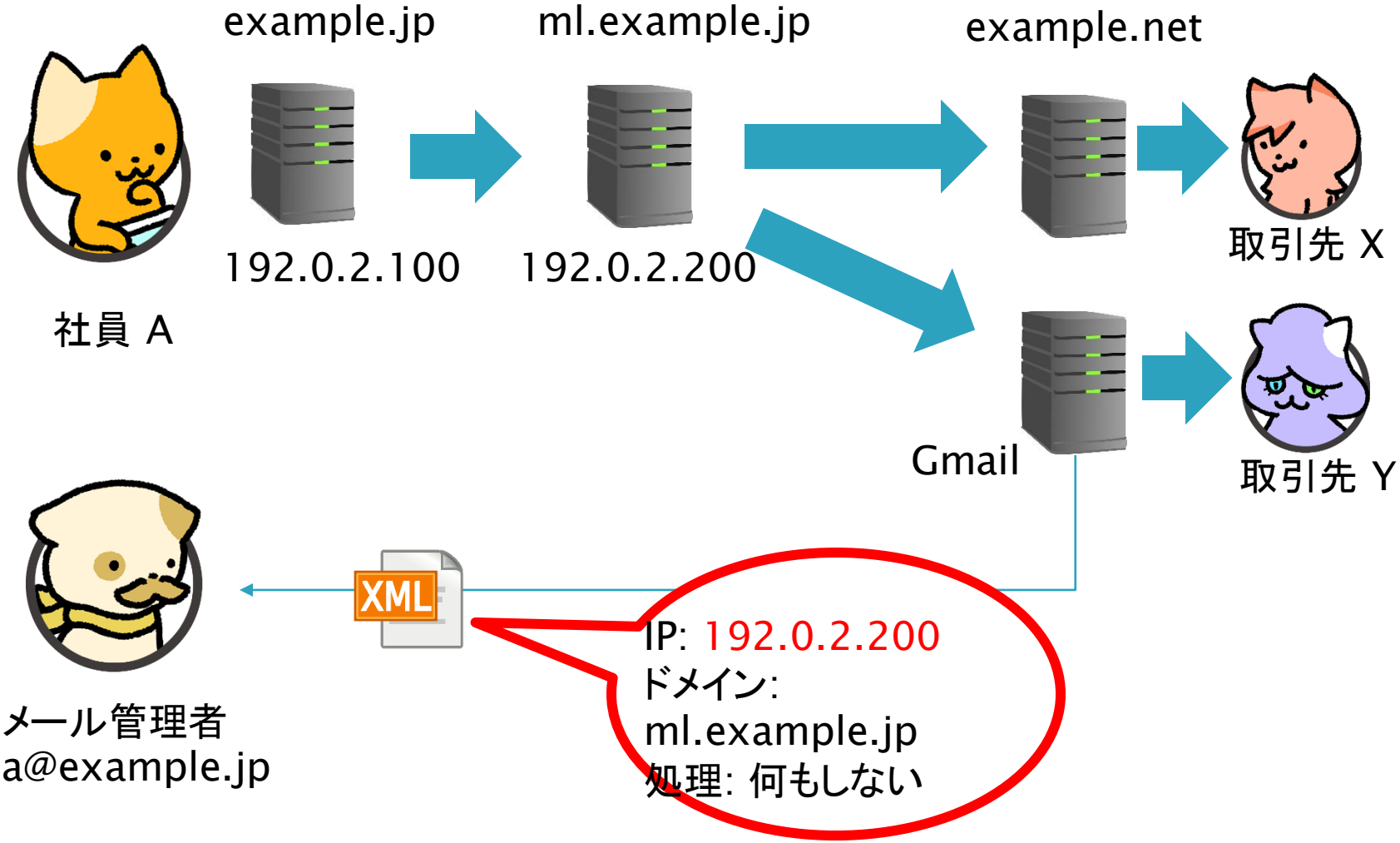
Case2: 転送


example.jp
example.com
192.0.2.100
198.51.100.10
社員 A
取引先 B
XML
Gmail
個人アドレス B
メール管理者
rua@example.jp
IP: 198.51.100.10
ドメイン:
example.jp
処理: 何もしない

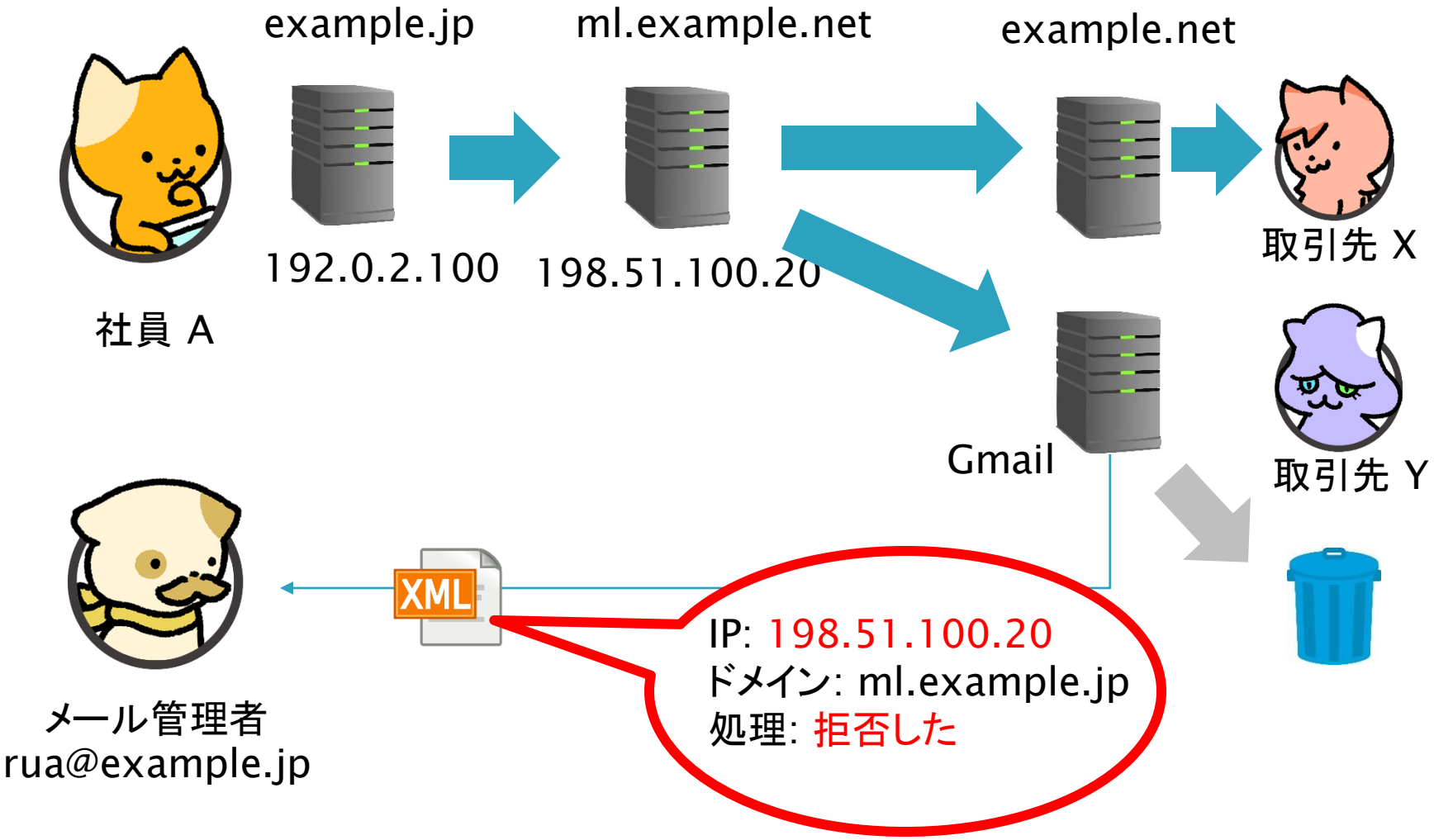
Case3: 転送（DKIM なし）



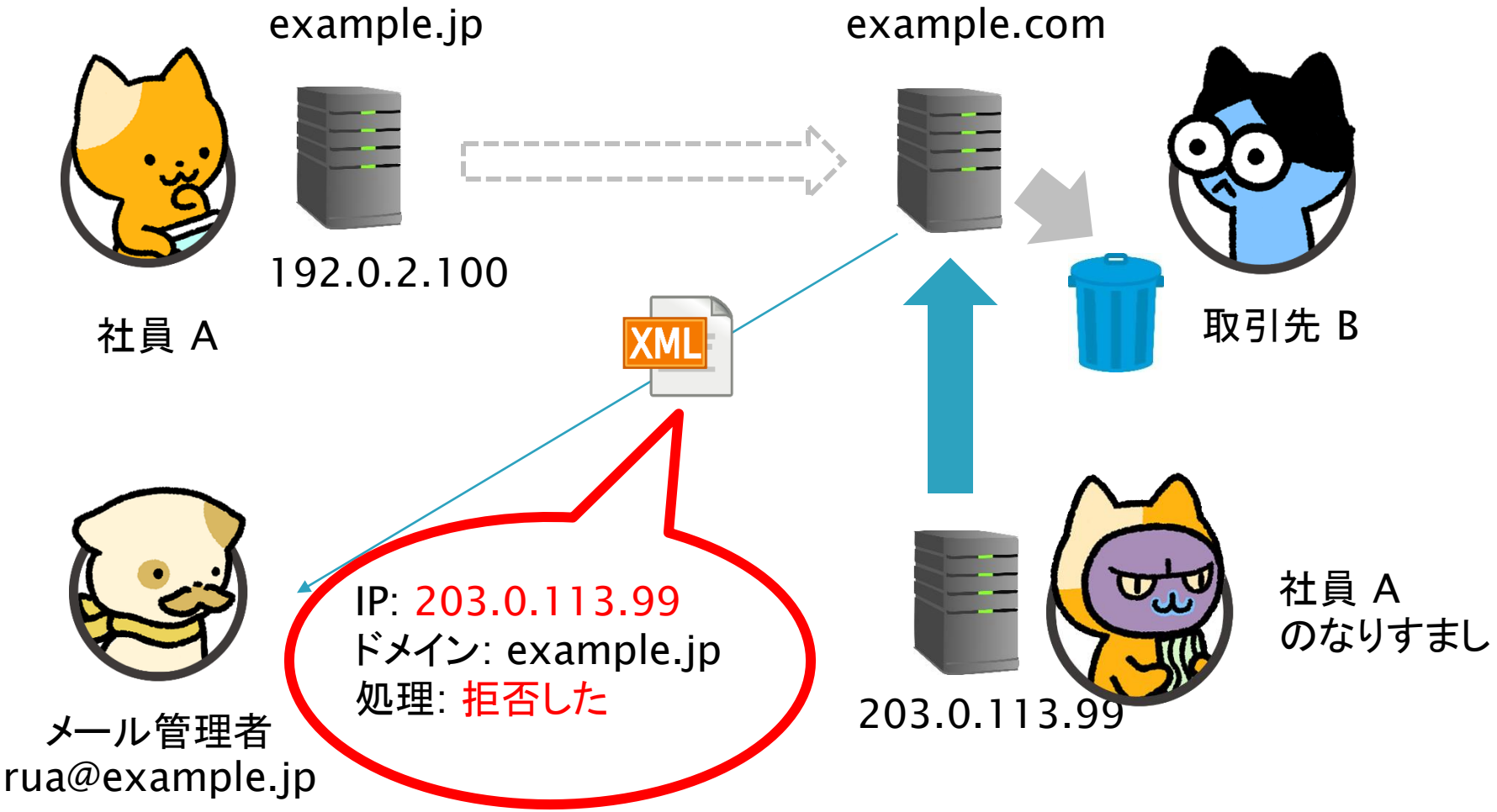
Case4: メーリングリスト（自社ドメイン）



Case5: メーリングリスト（他社ドメイン）



Case6: なりすまし


example.jp
example.com
192.0.2.100
社員 A
XML
取引先 B
IP: 203.0.113.99
ドメイン: example.jp
処理: 拒否した
メール管理者
rua@example.jp
203.0.113.99
社員 A
のなりすまし

各 Case まとめ

	Disposition	Source-IP	SPF	DKIM
Case1: 通常	何もしない	自社 IP	pass	pass
Case2: 転送	何もしない	取引先 IP	fail	pass
Case3: 転送（DKIMなし）	拒否した	取引先 IP	fail	fail
Case4: ML（自社ドメイン）	何もしない	自社 IP	pass	fail
Case5: ML（他社ドメイン）	拒否した	取引先 IP	fail	fail
Case6: なりすまし	拒否した	スパマー IP	fail	fail

* example.jp は p=reject を宣言

DMARC導入後に見える運用の課題

EASYSOLUTIONS®
TOTAL FRAUD PROTECTION

www.easysol.net

DMARC Compass –メール送信サーバ

送信サーバのIPアドレス、ドメイン名、SPF、DKIMの認証状況から
正規な送信サーバーをMySenderとして登録いただきます。

Sender	Domain	RDNS	Mail Count	SPF Pass & Aligned %
9.188.*	.co.jp	.com ...	89,845	99.99
3.100.2	.co.jp	.com	33,534	99.99
.38.140	.co.jp	.com	33,335	99.99
.23.0	.co.jp	.com	10,710	99.99
3.104.170	.co.jp	.com	10,468	99.99
7.13.*	.co.jp	+ 2 ...	6,262	0
48.20.*	.co.jp	+ 5 m ...	4,783	0
38.84.*	.co.jp	.jp + ...	2,496	0
6.156.*	.co.jp	+ 3 m ...	2,297	0
260:401:42f::*	.co.jp	ne.jp	1,779	0
f8b0:4002:c05::*	.co.jp	.com ...	1,425	0
2.90.*	.co.jp	il.ssk ...	1,155	0
87.230.*	.co.jp	et.jp ...	1,142	0
f8b0:400d:c09::*	.co.jp	.com ...	1,084	0
.240.*	.co.jp	p + ...	1,084	0
7800:5021::*	.co.jp	)	990	0
f8b0:4001:c0b::*	.co.jp	com ...	983	0
.106.*	.co.jp	) + ...	944	0

DMARC Compass -Unauthorized

DMARC認証失敗するケース

以下はUnauthorized 認証状況メトリクスとなります。

	SPF Pass & Aligned	SPF Pass & Not Aligned	SPF FAIL
DKIM Pass & Aligned	71.27% 177,902	4.85% 12,107	15.22% 37,998
DKIM Pass & Not Aligned	0.00% 0	0.60% 1,491	0.63% 1,563
DKIM FAIL	0.21% 532	2.05% 5,116	5.17% 12,910

（主要な要因：SPF・DKIMを実装している場合）

SPF Pass& Not Aligned ：メールの転送によるSPF失敗、かつ転送者のSPFが成功
SPF Fail ：メールの転送による認証失敗
DKIM Pass& Not Aligned ：メール転送時の件名の書き換え等によるDKIM失敗、
かつ転送者のDKIMが成功
メール送信代行業者のDKIMが成功
DKIM Fail ：メール転送時の件名の書き換え等によるDKIM失敗

DMARC Compass -Unauthorized

事例： SPF Pass& Not Aligned　転送メールサーバ

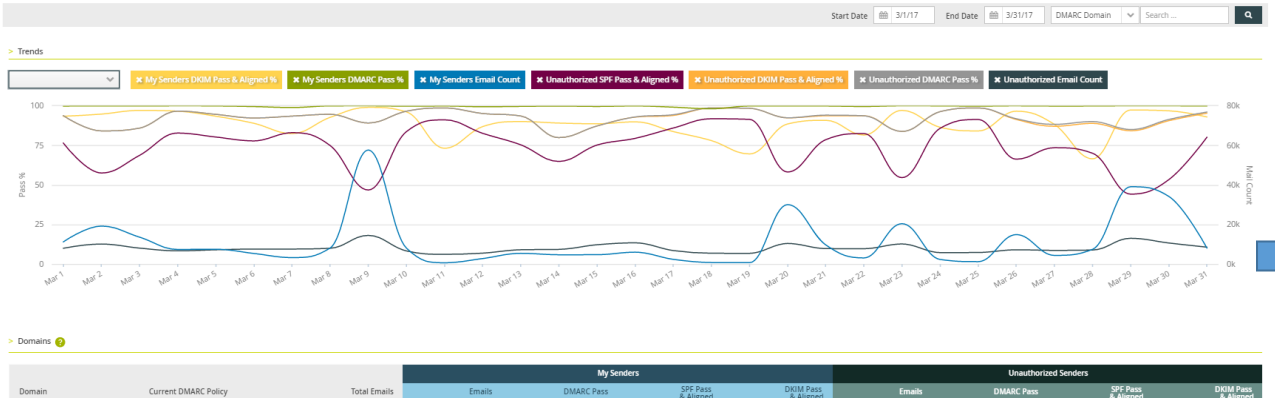
Sender	Domain	RDNS
):400e:c05::*	co.jp	mail-pg0-x22a.google.com ...
):4003:c0f::*	co.jp	mail-ot0-x235.google.com ...
):4003:c06::*	co.jp	mail-oi0-x229.google.com ...
):400c:c05::*	co.jp	mail-vk0-x22f.google.com ...
20.*	co.jp	mail-qk0-f172.google.com ...

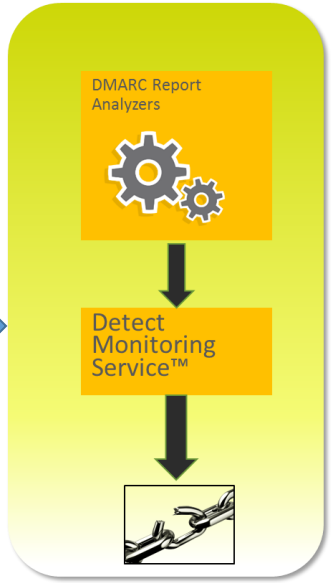
Googleのサーバで転送されていると
推測でき、安全なメールと識別

DMARC Compass –フィッシング検知

DMSとの連携により、迅速閉塞

DMARC Compassで受信したRUFレポートを解析し、メール本文に書かれたURLをスキャンします。





Thank you!

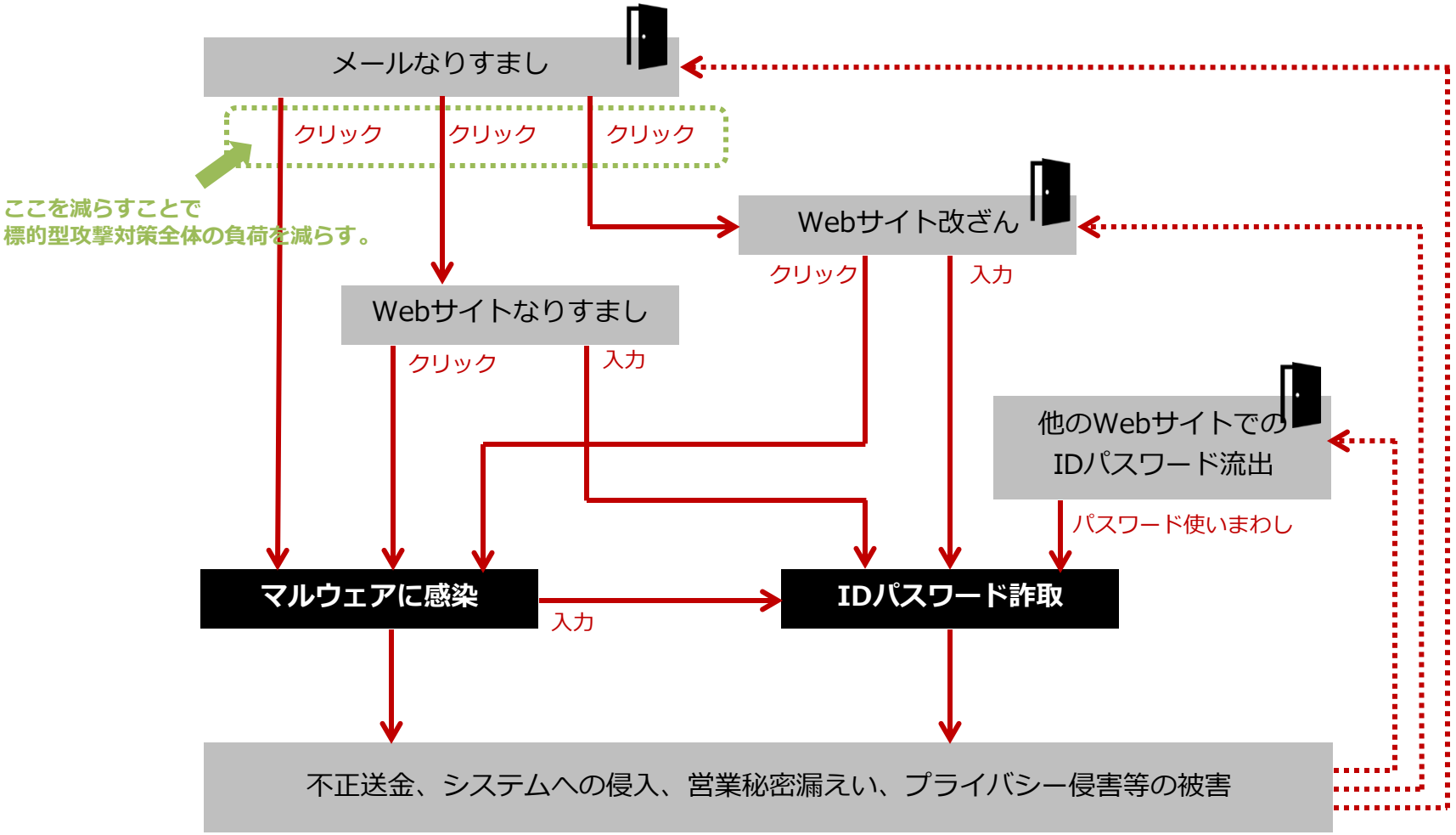
日本事業開発マネージャ
畠山　昌録　mhatakeyama@easysol.net

EASYSOLUTIONS®
TOTAL FRAUD PROTECTION

www.easysol.net

実際にDMARCレポート受信してみました

標的型攻撃対策における、なりすましメール対策の重要性



メールなりすまし対策としてすべきこと

- 正しいメールを正しいと判断できるようにする。
  - ・電子署名付きメール（**S/MIME**）を使う。
  - ・送信ドメイン認証（**DKIM**）に対応し、

  「**安心マーク**」によるDKIMの可視化をする。

S/MIME
エスマいぬ

DKIM
ディーキいぬ

- 正しくないメールを正しくないと判断できるようにする。
  - ・**DMARC**に対応する。
    p=reject
    （なりすましメールは受信しないで下さいという設定）

自社でのDMARC利用

- DMARC普及と同時に、DMARCレポート提供サービスの普及も必要と考え、レポート提供サービスも受けることにした。

- DNSサーバのレコードに以下の一行を追加。

Bind9_dmarc.jipdec.or.jp 3600 IN TXT
"v=DMARC1¥;p=none¥;pct=100¥;fo=1¥;ri=86400¥;
rua=mailto:jipdec_rua@xx.easysol.net¥;
ruf=mailto:jipdec_ruf@xx.easysol.net"
GUIHost: _dmarcTXT Value:
v=DMARC1;p=none;pct=100;fo=1;ri=86400;
rua=mailto:jipdec_rua@xx.easysol.net;
ruf=mailto:jipdec_ruf@xx.easysol.net

ruaレポート：「集計レポート」DMARC認証に失敗したメールの統計的データ
rufレポート：「認証失敗レポート」それぞれの失敗に関する詳細情報

毎週のサマリレポート

10/3～10/9間のjipdec.or.jp発信メールのDMARCレポートの統計情報サマリ

The following summary statistics were compiled from the period starting on 2016-10-03 and ending on 2016-10-09 .

DMARC統計レポート

DMARC Aggregate Reporting
* Emails detected across all domains: 6664
* DMARC aligned emails: 2822 (42.35%)
* SPF aligned emails: 2643 (39.66%)
* DKIM aligned emails: 179 (2.69%)

統計レポート対象の受信メール総数

DMARC認証にpassしているメール数とその比率

SPF認証にpassしているメール数とその比率

DKIM認証にpassしているメール数とその比率

DMARCエラーレポート

DMARC Failure Reporting
* DMARC RUF reports received: 0
* Emails not DMARC aligned: 3842 (57.65%)
* Emails not SPF aligned: 4021 (60.34%)
* Emails not DKIM aligned: 6485 (97.31%)

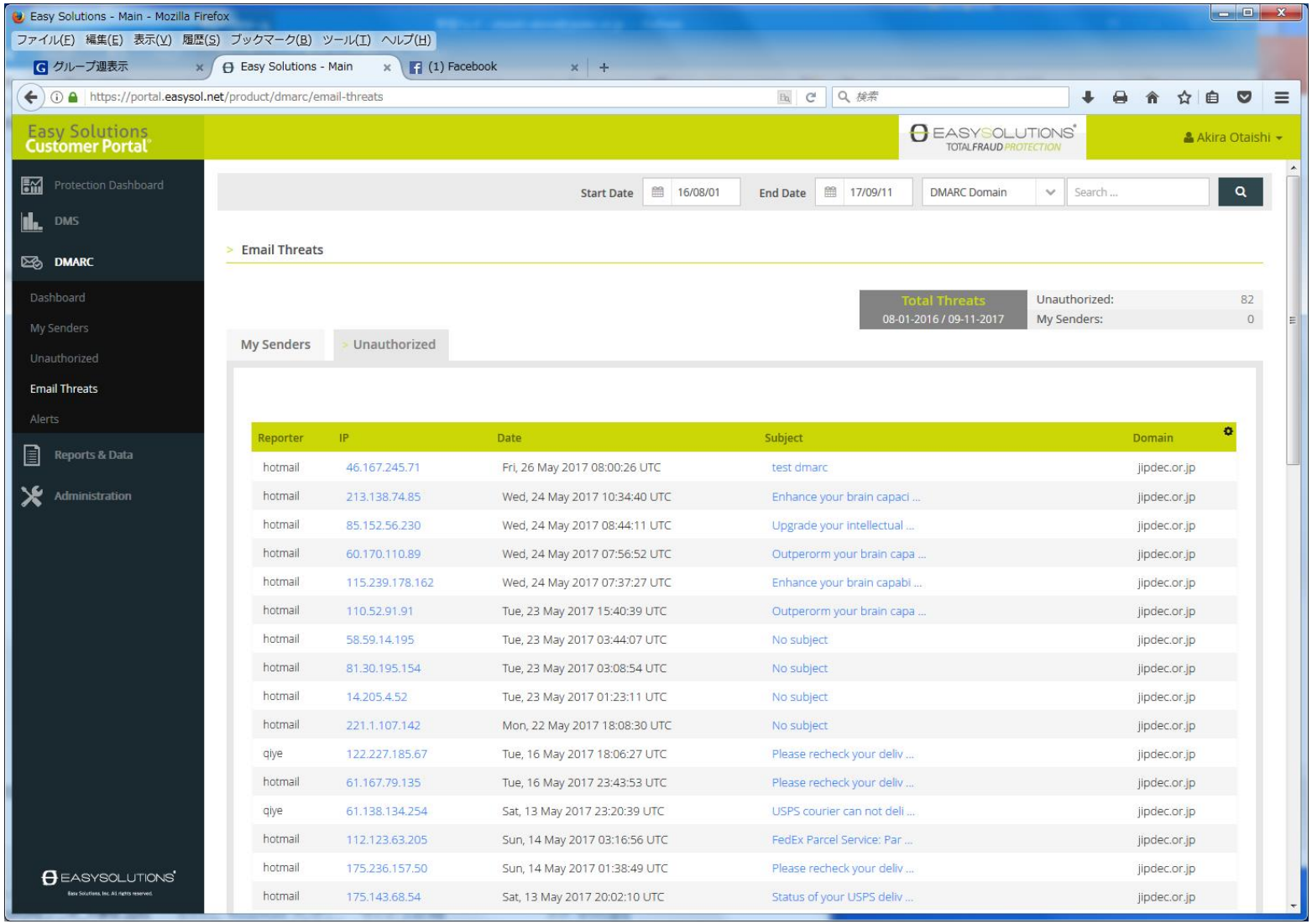
受信したrufレポート総数

DMARC認証にfailしているメール数とその比率

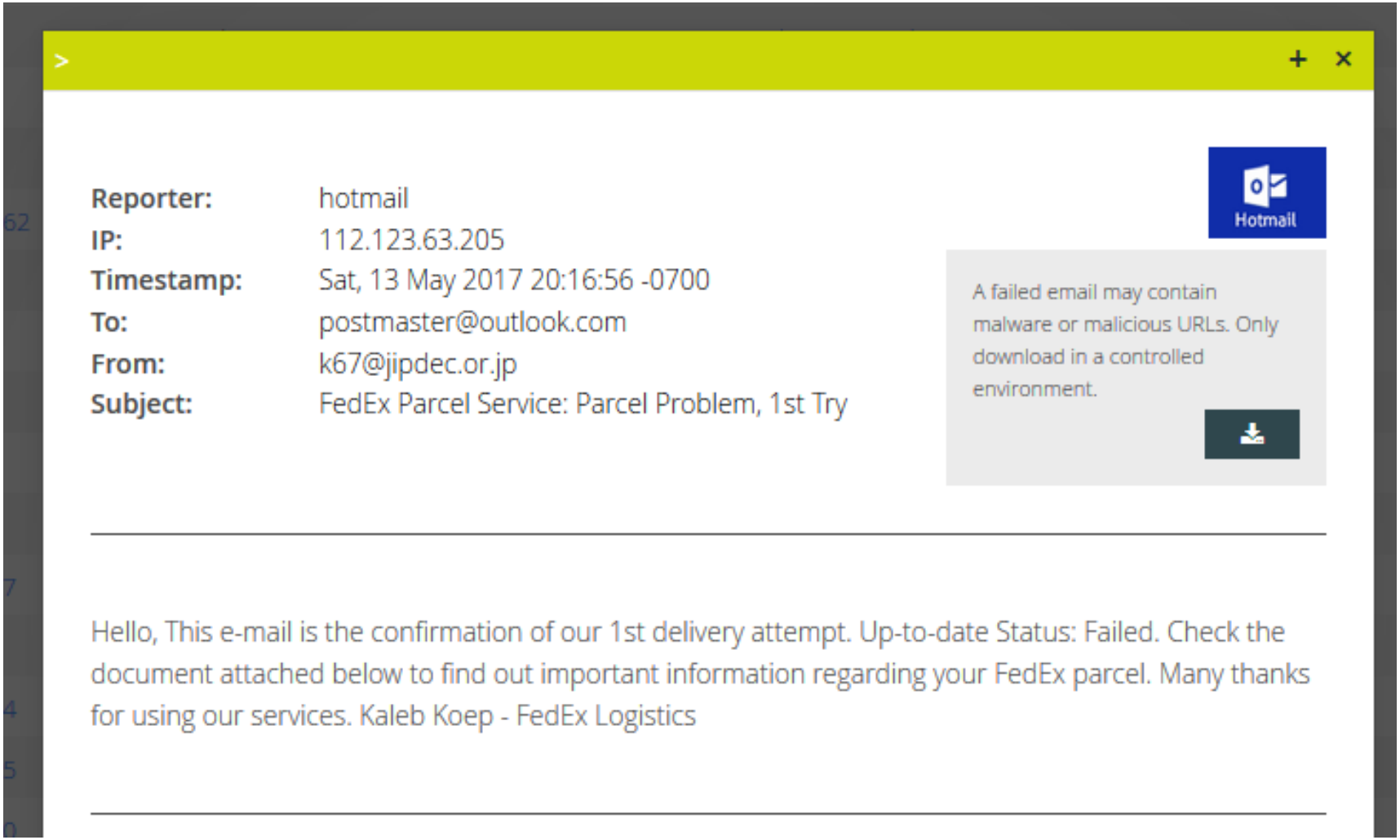
SPF認証にfailしているメール数とその比率

DKIM認証にfailしているメール数とその比率

Email Threatsをチェック



なりすましメールの例（その１）



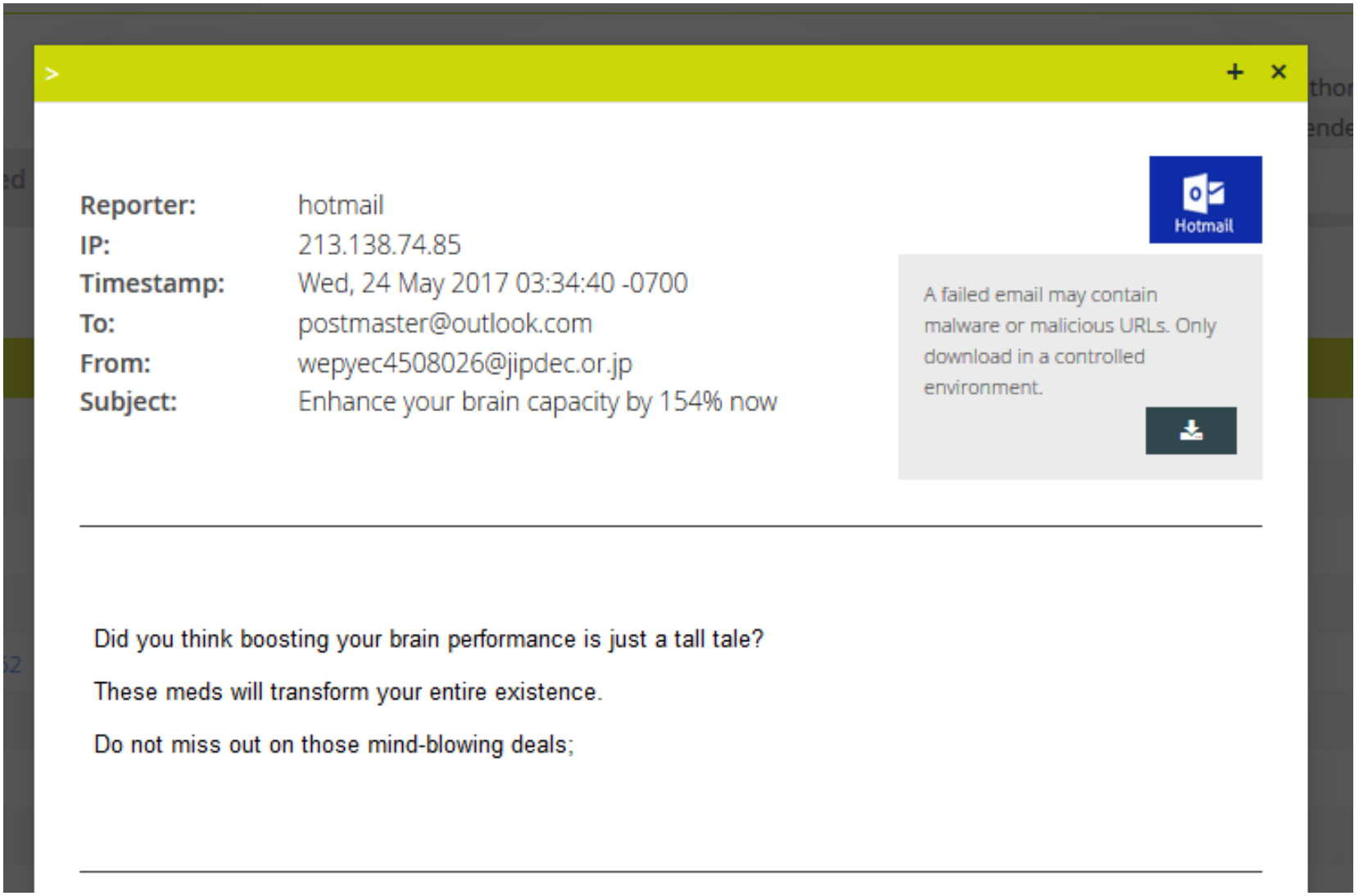
Reporter: hotmail
IP: 112.123.63.205
Timestamp: Sat, 13 May 2017 20:16:56 -0700
To: postmaster@outlook.com
From: k67@jipdec.or.jp
Subject: FedEx Parcel Service: Parcel Problem, 1st Try

Hotmail

A failed email may contain malware or malicious URLs. Only download in a controlled environment.

Hello, This e-mail is the confirmation of our 1st delivery attempt. Up-to-date Status: Failed. Check the document attached below to find out important information regarding your FedEx parcel. Many thanks for using our services. Kaleb Koep - FedEx Logistics

なりすましメールの例（その２）



Reporter: hotmail
IP: 213.138.74.85
Timestamp: Wed, 24 May 2017 03:34:40 -0700
To: postmaster@outlook.com
From: wepyec4508026@jipdec.or.jp
Subject: Enhance your brain capacity by 154% now

Hotmail

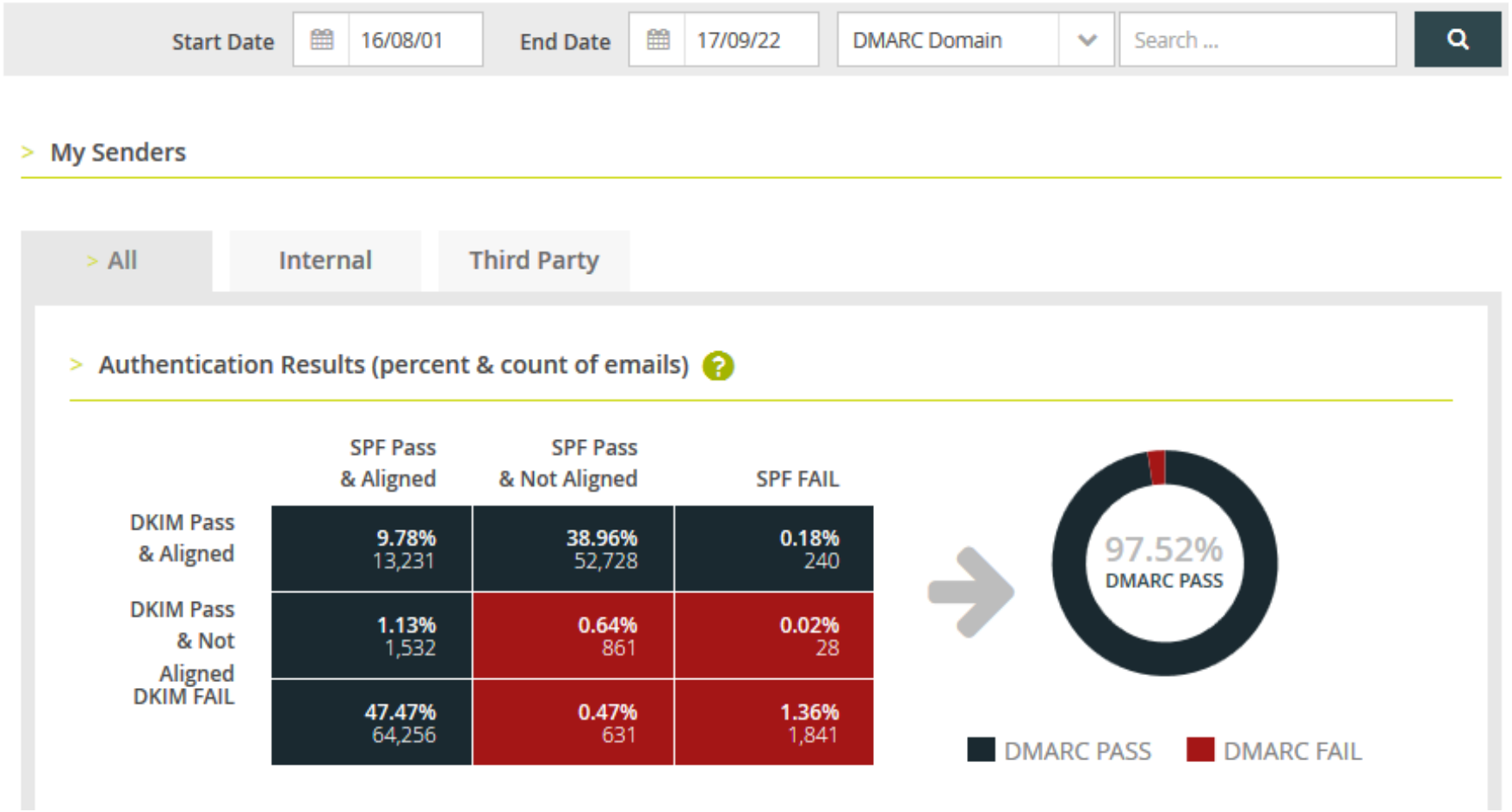
A failed email may contain malware or malicious URLs. Only download in a controlled environment.

Did you think boosting your brain performance is just a tall tale?

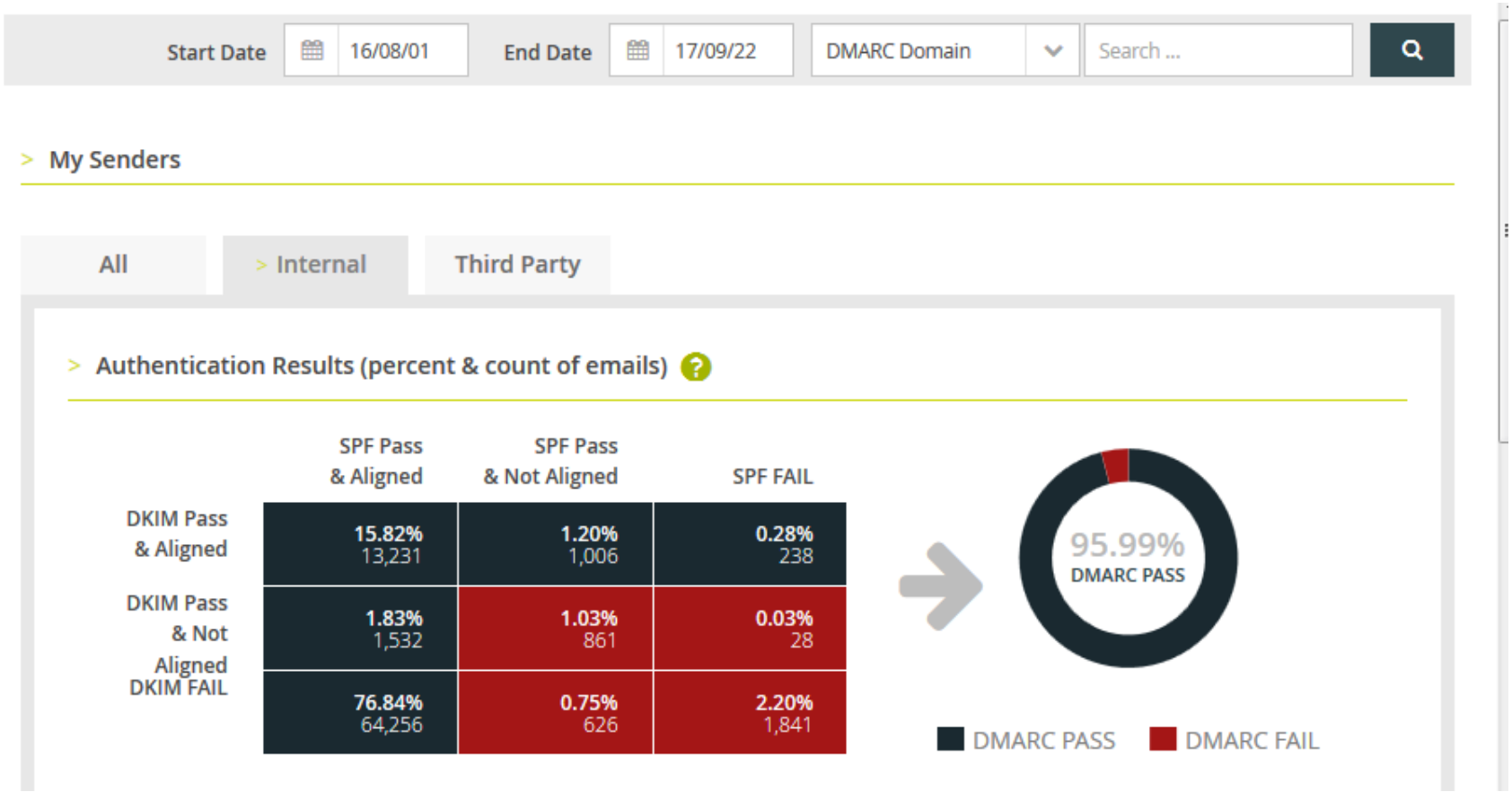
These meds will transform your entire existence.

Do not miss out on those mind-blowing deals;

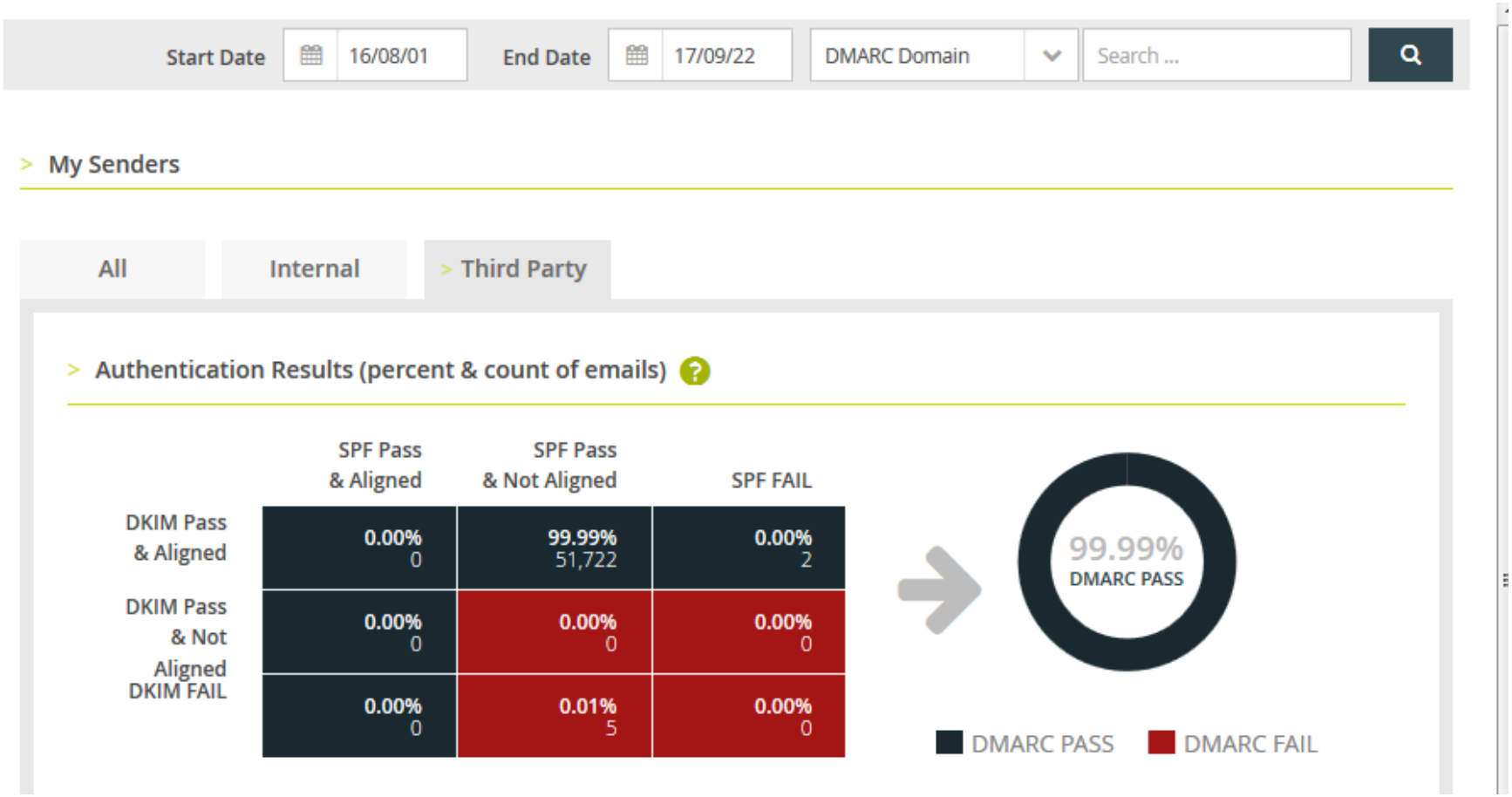
My Senderに登録した送信サーバの認証状況



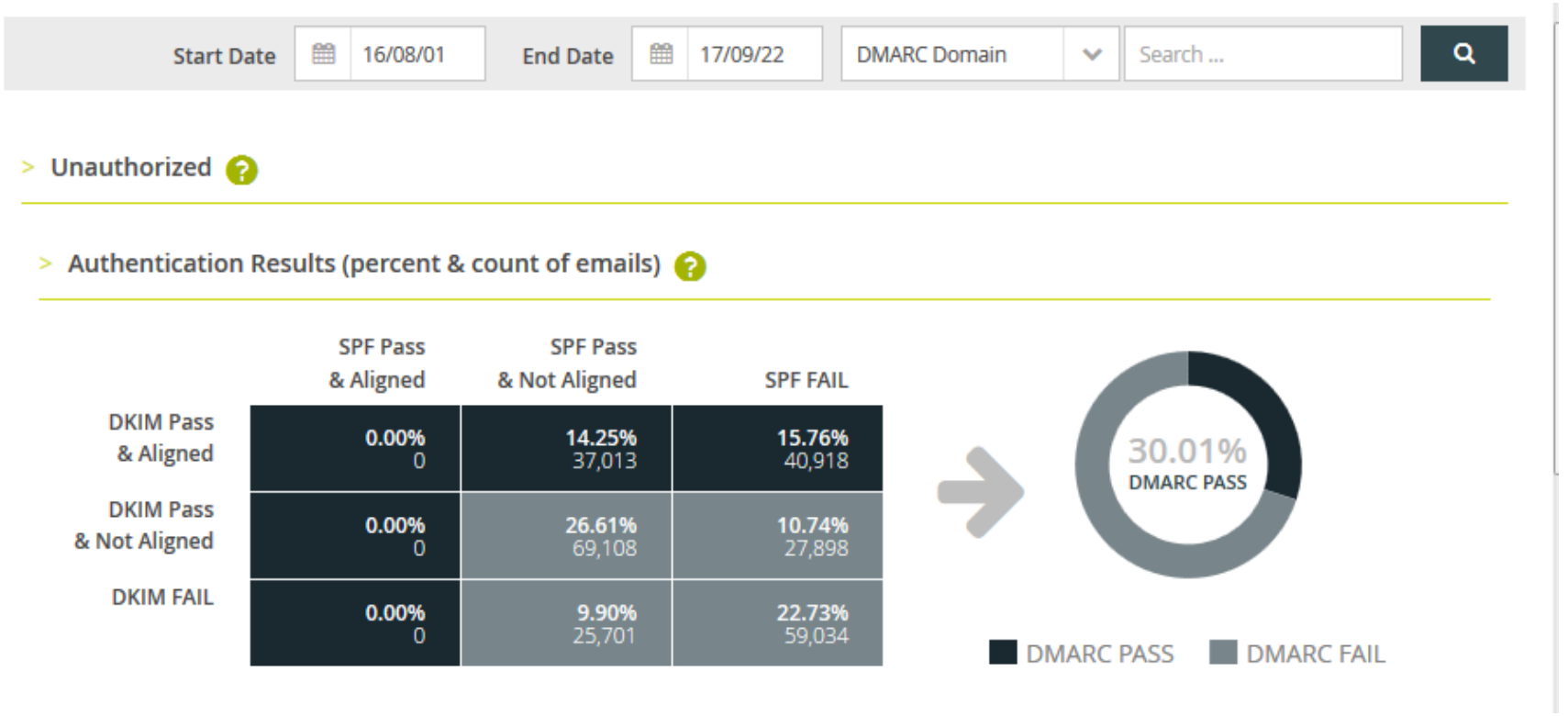
My Senderに登録した送信サーバの認証状況（Internal）



My Senderに登録した送信サーバの認証状況（Third Party）



登録していない送信サーバの認証状況



今後取り組みたいこと

- 運用ノウハウを蓄積し、情報発信、情報共有を進めたい。
- できるだけ早く、p=reject　を書きたい。