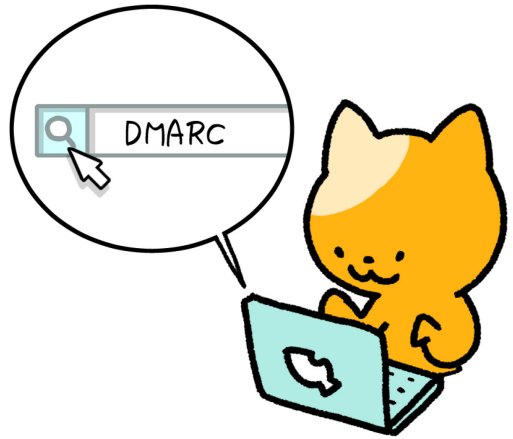
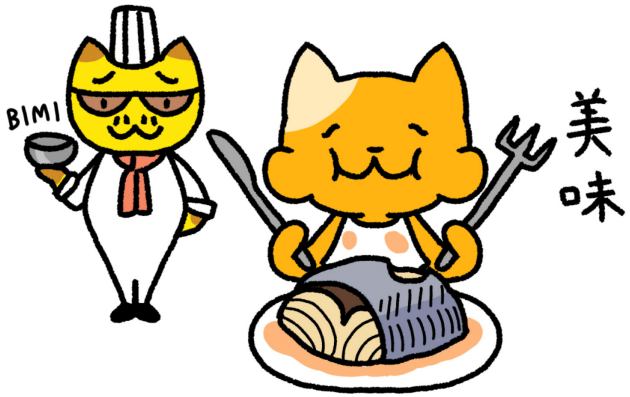
2024年のメール運用とDMARC

株式会社TwoFive
加瀬　正樹

本日のコンテンツ

- 10分でわかる送信ドメイン認証
- ドメイン管理者の DMARC 対応方法
- サーバ運用者の DMARC 対応方法
- DMARC レポートとその運用





古賀さんの資料より

- メール運用管理者の誰もが気にした方がいいのは、SPF と DKIM と DMARC
  - **ドメイン管理者** = DNS ゾーンを管理するエンジニア
  - **サーバ運用者** = 送信サーバや受信サーバを運用するエンジニア

メール運用管理者に求められる対応 早見表

		SPF か DKIM 対応	逆引き記載	spam rate <0.3%	転送は ARC 署名	DMARC 対応	TLS 通信対応	RFC 5322 準拠	@gmail .com 騙るな	List-Unsubscribe
1	個人でメール設備を運用	✅	✅	✅	✅	✅	✅	✅	✅	
2	企業でオンプレ設備を保有	✅	✅	✅	🌟	✅	✅	✅	✅	
3	クラウドサービス利用	🌟		✅		🌟		✅	✅	
4	オンプレ設備でメール送信	✅	✅	✅		✅	✅	✅	✅	✅
5	非 IT 部門で SaaS 利用	✅		✅		✅			✅	✅

10 分でわかる
送信ドメイン認証 3 種類

送信ドメイン認証

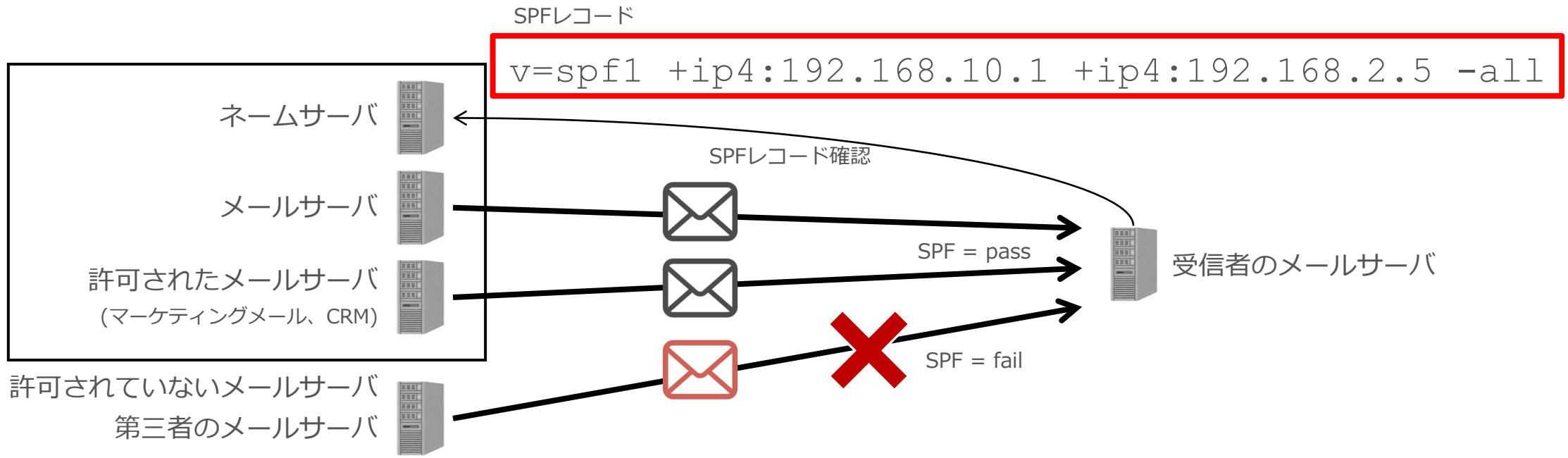
- ドメイン単位で送信者が名乗っている情報(メールドメイン)が正しいか確認する技術

SPF	規格	DKIM
RFC 7208	ドキュメント	RFC 6376 (STD 76)
IPアドレスで判定	認証方法	電子署名で判定
エンベロープ From ドメイン	保護する対象	署名ドメイン
DNS に設定を記述	対応の難しさ	サーバーに実装
Authentication-Results ヘッダー	確認方法	Authentication-Results ヘッダー
転送に弱い ヘッダー From 詐称が可能	問題点	メーリングリストに弱い ヘッダー From 詐称が可能

SPF (Sender Policy Framework)

- ドメイン名所有者が許可したメールサーバ(IPアドレス)から送信されているか、受信者が確認する技術

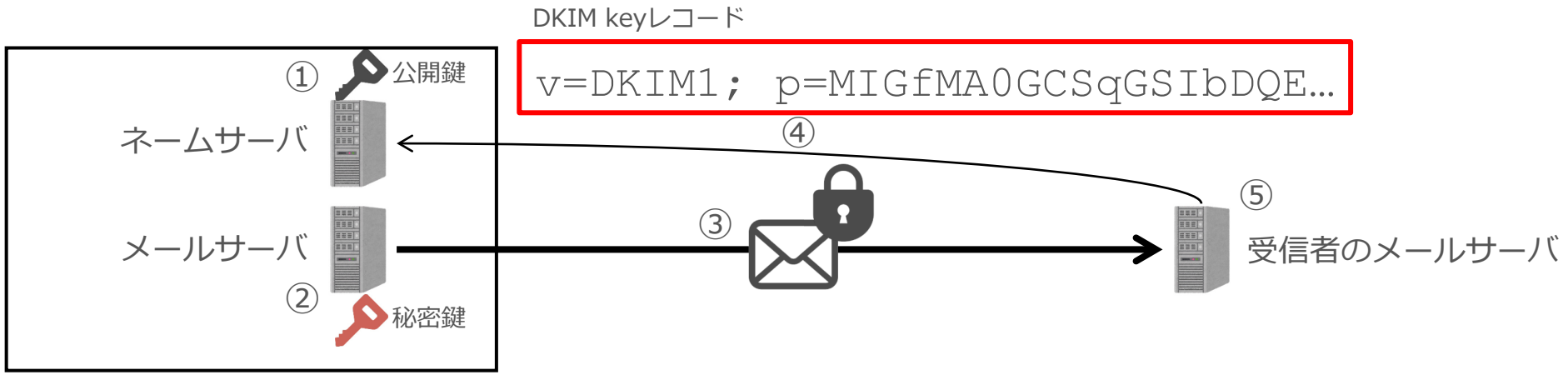
対象のドメイン名	エンベロープ From のドメイン
送信者(ドメイン管理者)	許可した IP アドレスのリスト(SPFレコード)をネームサーバ(DNS)へ登録する。
受信者	SPF レコードを取得し、メールの送信元 IP アドレスがリストに含まれているか確認する。



DKIM (DomainKeys Identified Mail)

- 送信元メールサーバがメールデータを利用して電子署名を行い、受信者が検証する技術
  - 電子署名検証: 内容が改ざんされていないか
  - 公開鍵の授受: ドメイン名所有者が正しいか

対象のドメイン名	署名ドメイン
送信者(ドメイン管理者)	① 電子署名に使用する公開鍵情報をネームサーバに登録する。
送信者	② メールデータから秘密鍵を使って電子署名を作成しメールに付加する。 ③ 電子署名付きメールを送信する。
受信者	④ 送信者のドメイン名(署名ドメイン名)のネームサーバから公開鍵を取得する。 ⑤ 公開鍵を使って電子署名を検証する。



(再掲) 送信ドメイン認証

- ドメイン単位で送信者が名乗っている情報(メールドメイン)が正しいか確認する技術
- SPF も DKIM もメールクライアントで表示するヘッダーFromドメインが詐称可能

SPF	規格	DKIM
RFC 7208	ドキュメント	RFC 6376 (STD 76)
IPアドレスで判定	認証方法	電子署名で判定
エンベロープ From ドメイン	保護する対象	署名ドメイン
DNS に設定を記述	対応の難しさ	サーバーに実装
Authentication-Results ヘッダー	確認方法	Authentication-Results ヘッダー
転送に弱い ヘッダー From 詐称が可能	問題点	メーリングリストに弱い ヘッダー From 詐称が可能

DMARC - 2つの機能

認証

IPアドレス(SPF)や
電子署名(DKIM)を使って
なりすましメールか
どうかを認証する技術

分析

サーバに届いたメールの
認証結果を
ドメインの管理者に
集計レポートする技術

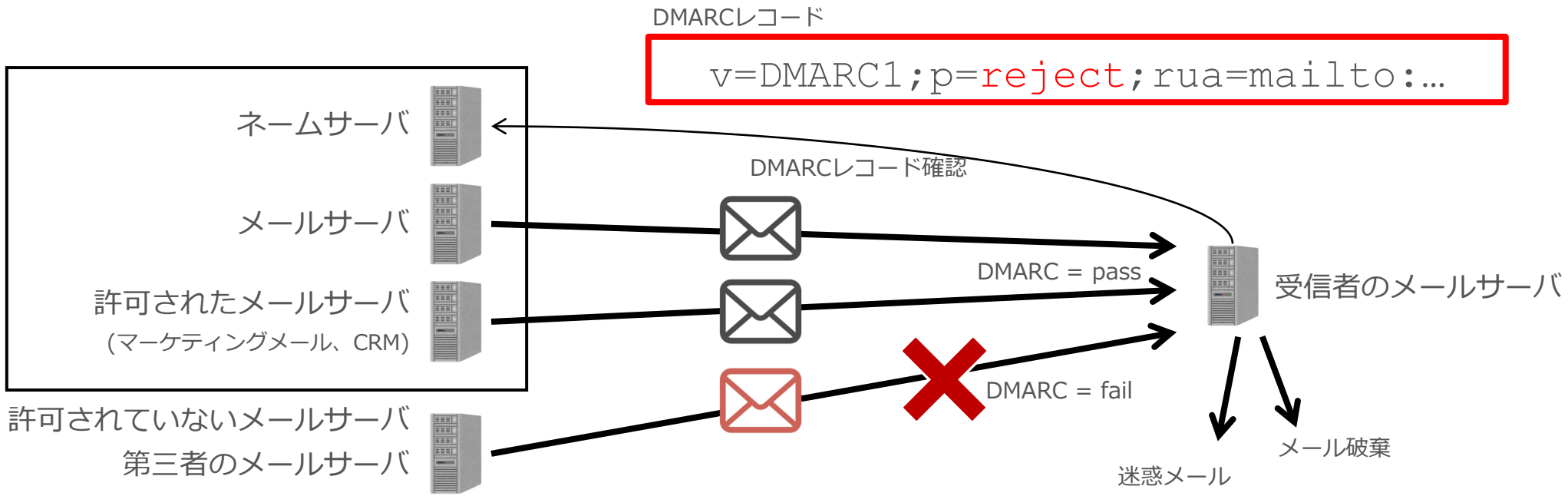
認証＋集計レポートによって
正しいメールを届けて
なりすましメールを削除できます

- 2016年政府サービス義務化
- 2017年政府ドメイン義務化
- 2018年7月
  サイバーセキュリティ2018記載
- 2020年6月
  フィッシングレポート2020記載
- 2023年10月
  メール送信ガイドラインアップデート
- 2024年11月 日経225銘柄
  DMARC 導入企業は 92.0 %

DMARC - 認証（ポリシー機能）

- ポリシー機能によるメール取り扱い指定
  - 認証結果が失敗した場合、受信者にどのように処理してほしいか宣言する

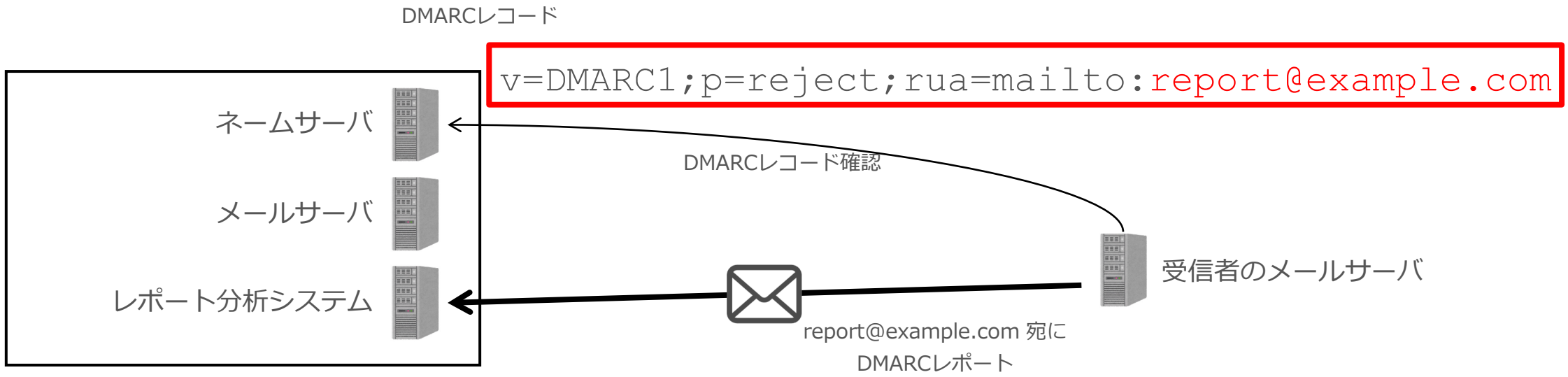
none (何もしない)	受信箱に入れる
quarantine (隔離する)	迷惑メールなんて意する、迷惑メールフォルダーへ入れる
reject (受信拒否する)	送信者へエラーを返す、受信して破棄する



DMARC - 分析（レポート機能）

- ポリシー機能によるメール取り扱い指定
  - 認証結果が失敗した場合、受信者にどのように処理してほしいか宣言する

- レポート機能によるフィードバック
  - DMARC/SPF/DKIM認証結果、送信元情報
  - どのように処理したか
  - その他(認証失敗したメールのヘッダーなど)



DMARC - 認証（その他動作仕様）

- ポリシー機能によるメール取り扱い指定
  - 認証結果が失敗した場合、受信者にどのように処理してほしいか宣言する

- レポート機能によるフィードバック
  - DMARC/SPF/DKIM認証結果、送信元情報
  - どのように処理したか
  - その他(認証失敗したメールのヘッダーなど)

- SPF、DKIM いずれかで認証 Pass（かつイン・アライメント）

- ヘッダー Fromを保護できる

(参考) DMARC の認証の考え方

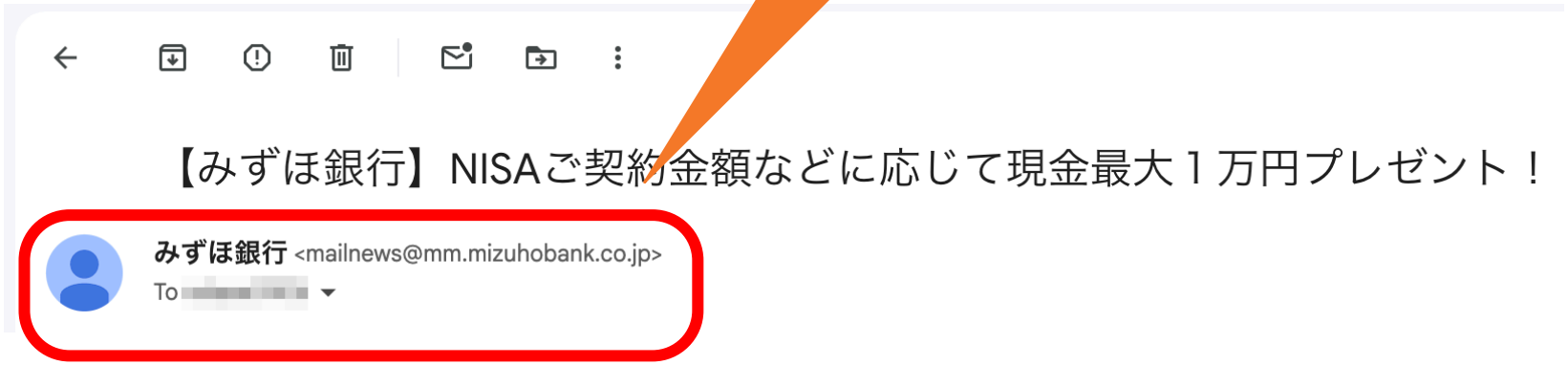
(SPF が Pass または DKIM が Pass) かつ "イン・アライメント"

- イン・アライメントとは “ドメイン名が一致している”
- SPF が Pass している場合は・・・
  - ヘッダー From ドメイン = エンベロープ From ドメイン
- DKIM が Pass している場合は・・・
  - ヘッダー From ドメイン = DKIM 署名ドメイン(DKIM-Signatureのd=タグ)
- アライメントモード
  - strict : ドメイン完全一致
  - relaxed : 組織ドメイン(Organizational Domain)一致
    （mail.example.co.jp の 組織ドメイン(OD) => example.co.jp）

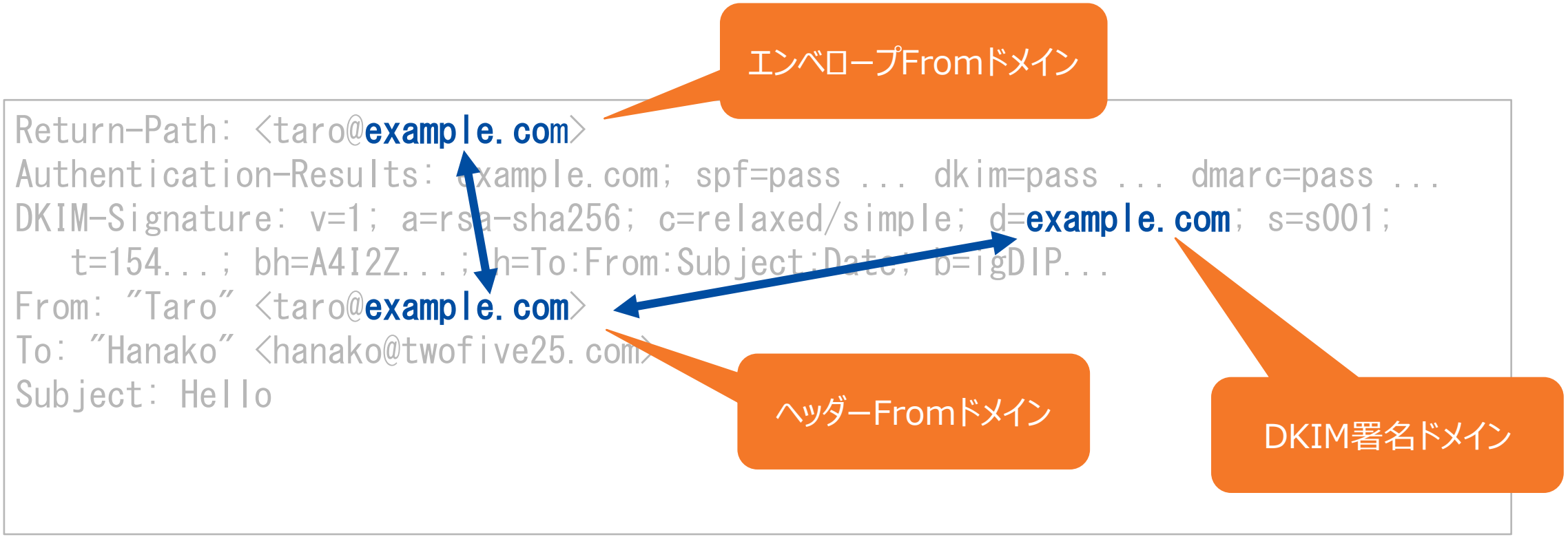
(参考) DMARC の認証の考え方

```
Return-Path: <taro@example.com>
Authentication-Results: example.com; spf=pass ... dkim=pass ... dmarc=pass ...
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=example.com; s=s001;
   t=154...; bh=A4I2Z...; h=To:From:Subject:Date; b=igDIP...
From: "Taro" <taro@example.com>
To: "Hanako" <hanako@twofive25.com>
Subject: Hello
```

ヘッダーFromドメイン



(参考) DMARC の認証の考え方



- SPF が Pass している場合は・・・
  - ヘッダー From ドメイン = エンベロープ From ドメイン
- DKIM が Pass している場合は・・・
  - ヘッダー From ドメイン = DKIM 署名ドメイン(DKIM-Signatureのd=タグ)

ドメイン管理者の DMARC 対応方法

ドメイン管理者はどのように DMARC 対応するか

- SPF と同じようにDNS の TXT レコード（_dmarc.example.com）に以下のような宣言
- 親ドメインに設定することで、配下のサブドメイン全てに適用が可能
- 必要に応じて、サブドメインごとに設定が可能

v=DMARC1; p=none; rua=mailto:rua@example.com

バージョン

必須

ポリシー

none: そのまま受信
quarantine: 隔離
reject: 拒否

レポート受信先

任意だが設定すべき

ドメイン管理者はどのように DMARC 対応するか

- パラメーターは以下の通り

v=DMARC1; p=none; rua=mailto:rua@example.com

タグ	目的	記述例	記述必須	省略時
v	プロトコルバージョン	v=DMARC1	○	-
p	ポリシー (none, quarantine, reject)	p=none	○	-
sp	サブドメインのポリシー (none, quarantine, reject)	sp=quarantine	-	p=と同じ
pct	ポリシー適用する割合 (0-100)	pct=20	-	pct=100
rua	集計レポート送信先	rua=mailto:rua@example.com	-	なし
ruf	失敗レポート送信先	ruf=mailto:ruf@example.com	-	なし
aspf	SPFアライメントモード (r, s)	aspf=r	-	r
adkim	DKIMアライメントモード (r, s)	adkim=s	-	r

DMARC レコードの例（InternetWeek）

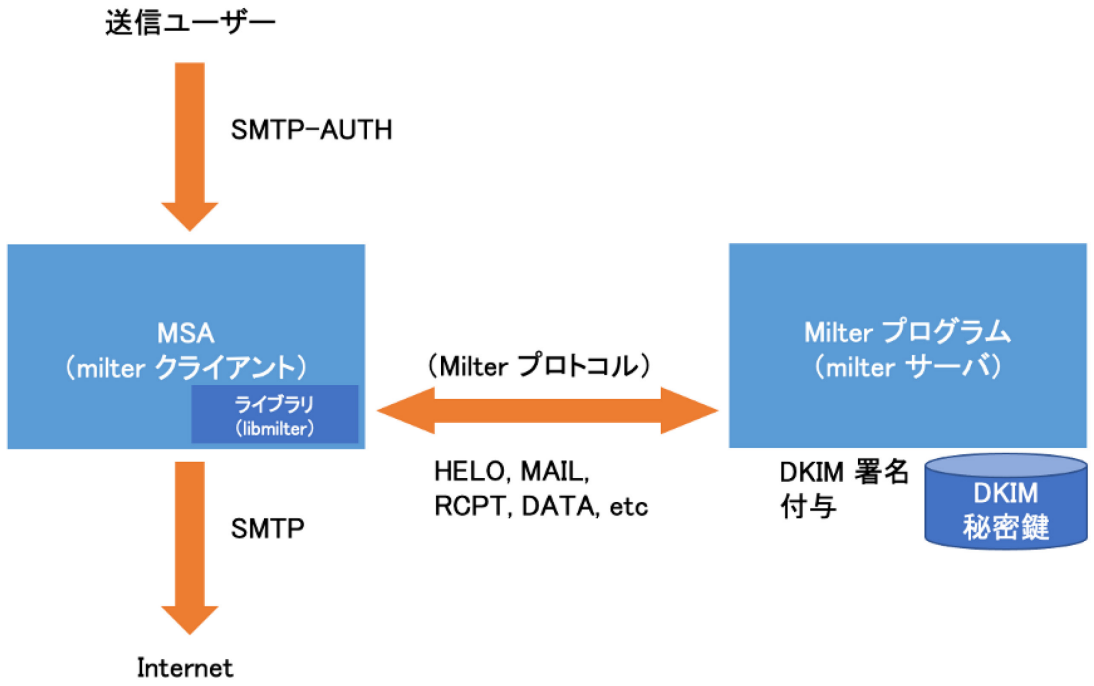
```
dig +short _dmarc.internetweek.jp txt
"v=DMARC1; p=reject; sp=reject; adkim=s; aspf=s; rua=mailto:dmarc@nic.ad.jp;"
```

タグ	目的	記述内容	記述必須
v	**プロトコルバージョン**	**v=DMARC1**	○
p	**ポリシー (none, quarantine, reject)**	**p=reject**	○
sp	**サブドメインのポリシー (none, quarantine, reject)**	**sp=reject**	-
pct	ポリシー適用する割合 (0-100)		-
rua	**集計レポート送信先**	**rua=mailto:dmarc@nic.ad.jp**	-
ruf	失敗レポート送信先		-
aspf	**SPFアライメントモード (r, s)**	**aspf=s**	-
adkim	**DKIMアライメントモード (r, s)**	**adkim=s**	-

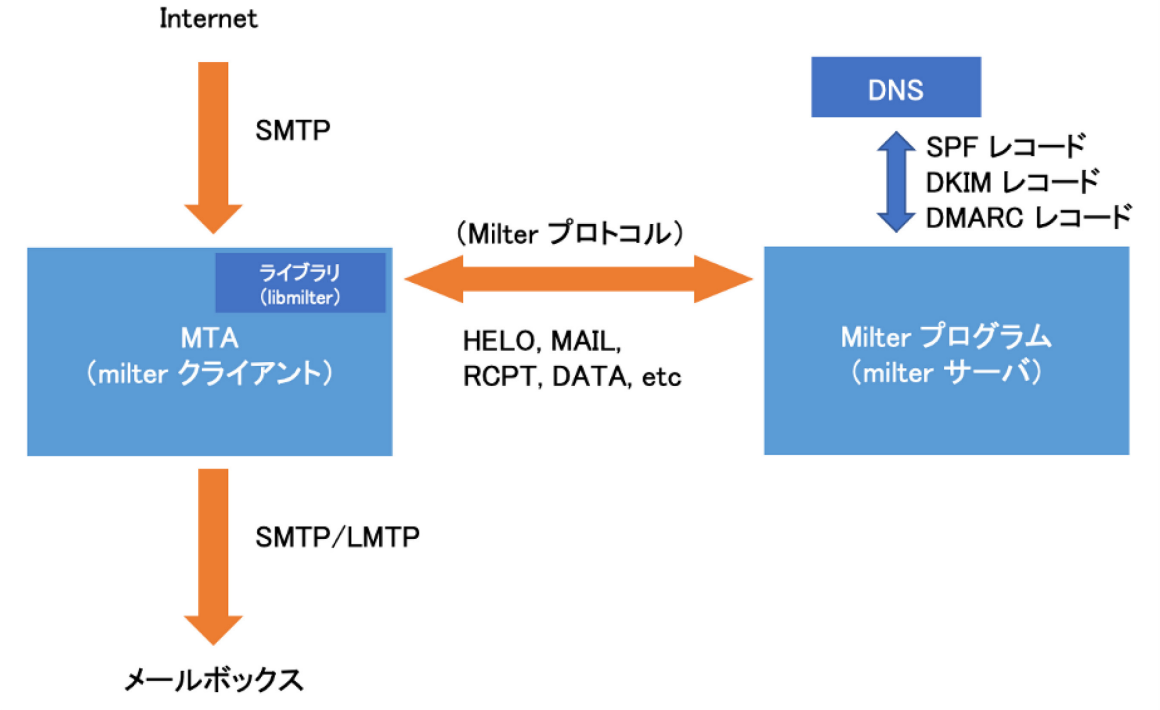
サーバ運用者の DMARC 対応方法

Milterプログラム

- Milter = mail + filter
- Sendmail が開発した libmilter ライブラリを利用して、MTA の外側のアプリケーションで処理を実行、その結果を MTA 側で活用するためのインターフェース。



＜送信時のMilterの流れ＞



＜受信時のMilterの流れ＞

Milterプログラム

- Milter = mail + filter
- 受信側として利用する場合は、以下のような候補から選択する。
  - （OpenDMARC+OpenDKIM, Fastmail, Rspamd）

	OpenDMARC	OpenDKIM	Fastmail Authentication milter	Rspamd
開発元/Author	The Trusted Domain Project	The Trusted Domain Project	Fastmail Pty. Ltd.	Vsevolod Stakhov
開発言語	C 言語	C 言語	Perl	C 言語 + Lua
SPF 認証機能	○	―	○	○
DKIM 認証機能	―	○	○	○
DMARC 認証機能	○	―	○	○
DKIM 署名機能	―	○	○	○
その他機能	DMARC レポート送付	―	ARC, BIMI 認証など	DMARC レポート送付

※ 2024年11月調査

送信サーバ対応 (OpenDKIM の場合)

※ 環境に適用する際にはご自身で確認をした上で適用ください

- インストール

```
$ sudo dnf install opendkim
```

- 鍵ペアの生成(対象ドメインとセレクター名を指定して生成)

```
$ opendkim-genkey -D /etc/opendkim/internetweek.jp -b 2048 -d internetweek.jp -s selector25
```

- 公開鍵の DNS レコード登録

```
$ cat selector25.txt
default._domainkey      IN    TXT  ( "v=DKIM1; k=rsa; "
        "p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBg・・・
b8WdNQo1CkHTpiwOtCQV6JKfBeYAw+d66Slt+6UbETyeY52mZRnYFJ/5iD0PX2Pna1GAHyrIQdOXoZZLfEBf6nWUo
+W/ZarZKK6qx2wk+rtbswIDAQAB" )  ; ----- DKIM key selector25 for internetweek.jp
```

- 秘密鍵の所有権の変更

```
$ sudo chown -R opendkim:opendkim /etc/opendkim/internetweek.jp
```

送信サーバ対応 (OpenDKIM の場合)

※ 環境に適用する際にはご自身で確認をした上で適用ください

- OpenDKIM の定義変更(キーテーブルとサイニングテーブルを指定)

```
$ sudo vi /etc/opendkim.conf
・・・
Mode    s
・・・
KeyTable        /etc/opendkim/KeyTable
・・・
SigningTable    refile:/etc/opendkim/SigningTable
・・・
```

- キーテーブルの変更(署名に利用する秘密鍵を指定)

```
$ sudo vi /etc/opendkim/KeyTable
・・・
selector25._domainkey.example.com
internetweek.jp:selector25:/etc/opendkim/internetweek.jp/selector25.private
・・・
```

送信サーバ対応 (OpenDKIM の場合)

※ 環境に適用する際にはご自身で確認をした上で適用ください

- サイニングテーブルの変更(署名するヘッダーFromドメインを指定)

```
$ sudo vi /etc/opendkim/SigningTable
・・・
*@internetweek.jp selector25._domainkey.internetweek.jp
```

- Postfix の定義変更(ポート 8891 を利用する場合)

```
/etc/postfix/main.cf:
・・・
milter_protocol=6
smtpd_milters = inet:localhost:8891
milter_default_action = tempfail
```

- OpenDKIM の起動

```
$ sudo systemctl start opendkim
$ sudo systemctl enable opendkim
```

- Postfix リロード

```
$ sudo systemctl reload postfix
```

受信サーバ対応 (OpenDKIM+OpenDMARC の場合)

※ 環境に適用する際にはご自身で確認をした上で適用ください

- インストール

```
$ sudo dnf install opendkim
$ sudo dnf install opendmarc
```

- OpenDKIM の定義変更(認証モードの設定)

```
$ sudo vi /etc/opendkim.conf
・・・
Mode    v
・・・
```

- OpenDMARC の定義変更(識別子とSPF認証の設定)

```
$ sudo vi /etc/opendmarc.conf
・・・
AuthservID      internetweek.jp
・・・
SPFIgnoreResults true
・・・
SPFSelfValidate true
・・・
```

受信サーバ対応 (OpenDKIM+OpenDMARC の場合)

※ 環境に適用する際にはご自身で確認をした上で適用ください

- Postfix の定義変更(OpenDKIM はポート 8891、OpenDMARC は 8893 を利用する場合)

```
/etc/postfix/main.cf:
・・・
milter_protocol=6
smtpd_milters = inet:localhost:8891, inet:localhost:8893
milter_default_action = accept
```

- OpenDKIM と OpenDMARC の起動

```
$ sudo systemctl start opendkim
$ sudo systemctl enable opendkim
$ sudo systemctl start opendmarc
$ sudo systemctl enable opendmarc
```

- Postfix リロード

```
$ sudo systemctl reload postfix
```

DMARC レポートとその運用

集計レポート v.s. 失敗レポート

- DMARCの重要な機能として、DMARC レポートがある
  - 集計レポート(Aggregate Report)
  - 失敗レポート(Forensic Report)

	集計レポート（Aggregate Report）	失敗レポート（Forensic Report）
レポートの受け取り方	DMARCレコード rua= タグで指定	DMARCレコード ruf= タグで指定
レポートの頻度	通常は1日1回ないし数回	都度
データ形式	添付ファイル（XML形式）	添付ファイル（ ARF形式など）
データ流通量	多い	少ない
主な提供元サービス	Google, Microsoft, NTTドコモ, KDDI, etc	—
注意点	活用するためには分析ツールが必要 集計された統計情報のみ	メッセージ自体を扱うため流通は皆無 FP 検体が期待できない

(再掲) ドメイン管理者はどのように DMARC 対応するか

- パラメーターは以下の通り

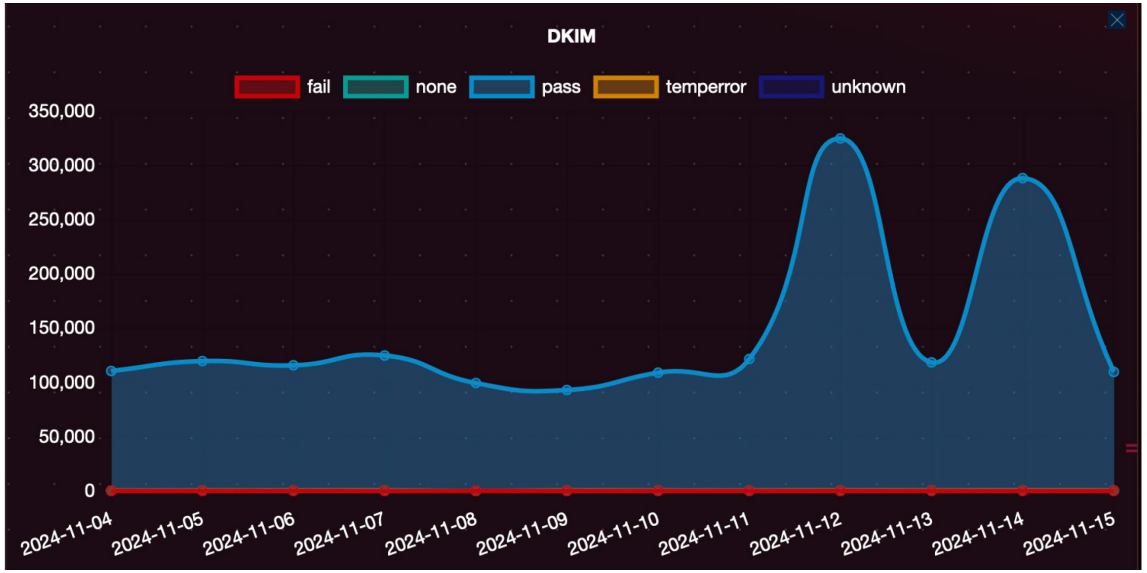
v=DMARC1; p=none; rua=mailto:rua@example.com

タグ	目的	記述例	記述必須	省略時
v	プロトコルバージョン	v=DMARC1	○	-
p	ポリシー (none, quarantine, reject)	p=none	○	-
sp	サブドメインのポリシー (none, quarantine, reject)	sp=quarantine	-	p=と同じ
pct	ポリシー適用する割合 (0-100)	pct=20	-	pct=100
rua	集計レポート送信先	rua=mailto:rua@example.com	-	なし
ruf	失敗レポート送信先	ruf=mailto:ruf@example.com	-	なし
aspf	SPFアライメントモード (r, s)	aspf=r	-	r
adkim	DKIMアライメントモード (r, s)	adkim=s	-	r

DMARC 集計レポートは XML 形式データ

- 添付ファイルとして XML 形式データ(またはその圧縮データ)が提供される

```
<?xml version="1.0" encoding="UTF-8"?>
<feedback>
  <version>1.0</version>
  <report_metadata>
・・・
</report_metadata>
・・・
<record>
    <row>
      <source_ip>210.130.202.146</source_ip>
      <count>1</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>pass</dkim>
        <spf>fail</spf>
・・・
</policy_evaluated>
    </row>
    <identifiers>
・・・
    </identifiers>
    <auth_results>
       <dkim>
         <domain>twofive25.com</domain>
         <selector>tf0002</selector>
         <result>pass</result>
         <human_result>2048-bit key</human_result>
       </dkim>
・・・
```



レポーター	メール通数	none	quarantine	reject
		%	%	%
google.com	487,141	484,310	2,689	142
		99.42%	0.55%	0.03%
AMAZON-SES	150,133	149,650	0	483
		99.68%	0.00%	0.32%
Enterprise Outlook	106,658	104,899	1	1,758
		98.35%	0.00%	1.65%

DMARC 失敗レポートは ARF 形式データ

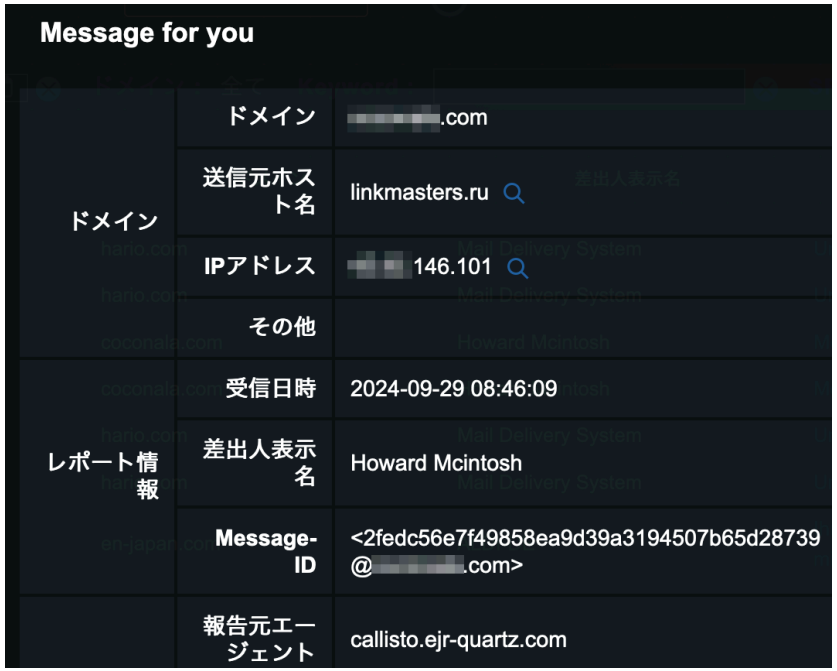
- 添付ファイルとして ARF 形式データが提供される

```
--_----Mdxr3dvV1hhNcqqqZCkZ7Q===_1F/C7-08347-7D651936
Content-Type: message/feedback-report; name=report

Feedback-Type: auth-failure
User-Agent: Lua/1.0
Version: 1.0
Original-Mail-From: XXXXXXXXXXX@dmarc25.jp
Original-Rcpt-To: XXXXXXX@example.com
Arrival-Date: Wed, 07 Dec 2022 22:15:35 -0500
Message-ID: <da835ffa-ffca-47ce-af31-e9dcc5a444d9@XXXXXXXXX>
Authentication-Results: dmarc=fail (p=quarantine, dis=quarantine) header.from=dmarc25.jp
Source-IP: XX.XX.XX.XX
Delivery-Result: smg-policy-action
Auth-Failure: dmarc
Reported-Domain: dmarc25.jp

--_----Mdxr3dvV1hhNcqqqZCkZ7Q===_1F/C7-08347-7D651936
Content-Type: message/rfc822
Content-Disposition: inline

Received: from XXXXXXXXXXXXX.com (XXXXXXXXXXX.com [XX.XX.XX.XX])
            by XXXXXXXXX.com (ABCDE Messaging Gateway) with SMTP id OF.C7.08347.4D6519
36; Wed,  7 Dec 2022 22:15:34 -0500 (-05)
. . .
```



ドメイン管理者の一般的な DMARC 運用サイクル

DMARCレコードを p=none で宣言

不正なメールは排除されない

DMARCレポートを分析

レポートに含まれる以下の内容を確認

- メールの送信元情報
- メールのDMARC認証結果
- メールの処理結果（受信/隔離/破棄）

送信メールのDMARC対応

自社が送信している全てのメールで
DMARCの認証が成功するよう設定

- SPF/DKIMの設定
- ドメインの見直し（必要なら）

p=quarantine/reject に変更

不正なメールが排除される

ドメイン管理者の DMARC 運用のポイント

- **DNS 設定後にツールで必ず確認する**
- **組織ドメイン (Organizational Domain) で必ず設定する**
  - サブドメインについても DMARC が有効となる
  - 把握していないサブドメインについても可視化できる
- **特定用途のドメインは p=reject でスタートする**
  - メールで利用していないドメインでは p=reject で設定する
  - 運用開始しやすい新規ドメインでは p=reject で設定する
- **集計レポート (Aggregate Report) を収集して分析する**
  - 送信元グループ別(クラウドサービス、自組織など)で区別して分析する
  - よく知られた転送サーバやホスティングサーバは優先度を下げて分析する
  - IPレピュテーションの低いサーバは優先度を下げて分析する
- **DKIM 認証への対応を優先する**
  - すでに SPF レコードに設定された送信元サーバは、DKIM 必須で対応すべき

サーバ運用者の DMARC 運用のポイント

- **セキュリティゲートウェイサービスを利用する場合は DKIM と DMARC を有効化する**
  - DKIM 署名対応
  - DMARC 認証
  - DMARC ポリシーに従った処理
  - 集計レポートのフィードバック
- **集計レポート(Aggregate Report)のフィードバックは可能であれば対応する**
  - OpenDMARC では opendmarc-import と opendmarc-report で対応できる
  - メールサーバへの同居の場合はキャパシティプランニングをする必要がある
- **失敗レポート(Forensic Report)のフィードバックは注意する**
  - 失敗レポートの通数による影響を考える
  - 失敗レポートの取り扱いに十分な注意が必要となる
- **集計レポート送信では DKIM 署名対応する**
  - DMARC ポリシーは p=reject

本日のまとめ

- 10分でわかる送信ドメイン認証
- ドメイン管理者の DMARC 対応方法
- サーバ運用者の DMARC 対応方法
- DMARC レポートとその運用