C13
メールセキュリティ2026キャッチアップ

スピーカー

- 古賀 勇(株式会社インターネットイニシアティブ)
- 加瀬 正樹(株式会社TwoFive)

本日のアジェンダ

- メール基礎キャッチアップ – DMARC　加瀬: 20分
- メール運用キャッチアップ – 証明書管理　古賀: 20分
- おまけ

- Open mic　二人: 10分

メール基礎キャッチアップ
- DMARC

典型的なメールのなりすまし方法

SMTP プロトコルでは 3 つの送信者情報をやりとりしている

社員 A
taro@example.jp

取引先 B

EHLO example.jp

メールサーバ
（IP アドレス）

MAIL FROM:<taro@example.jp>

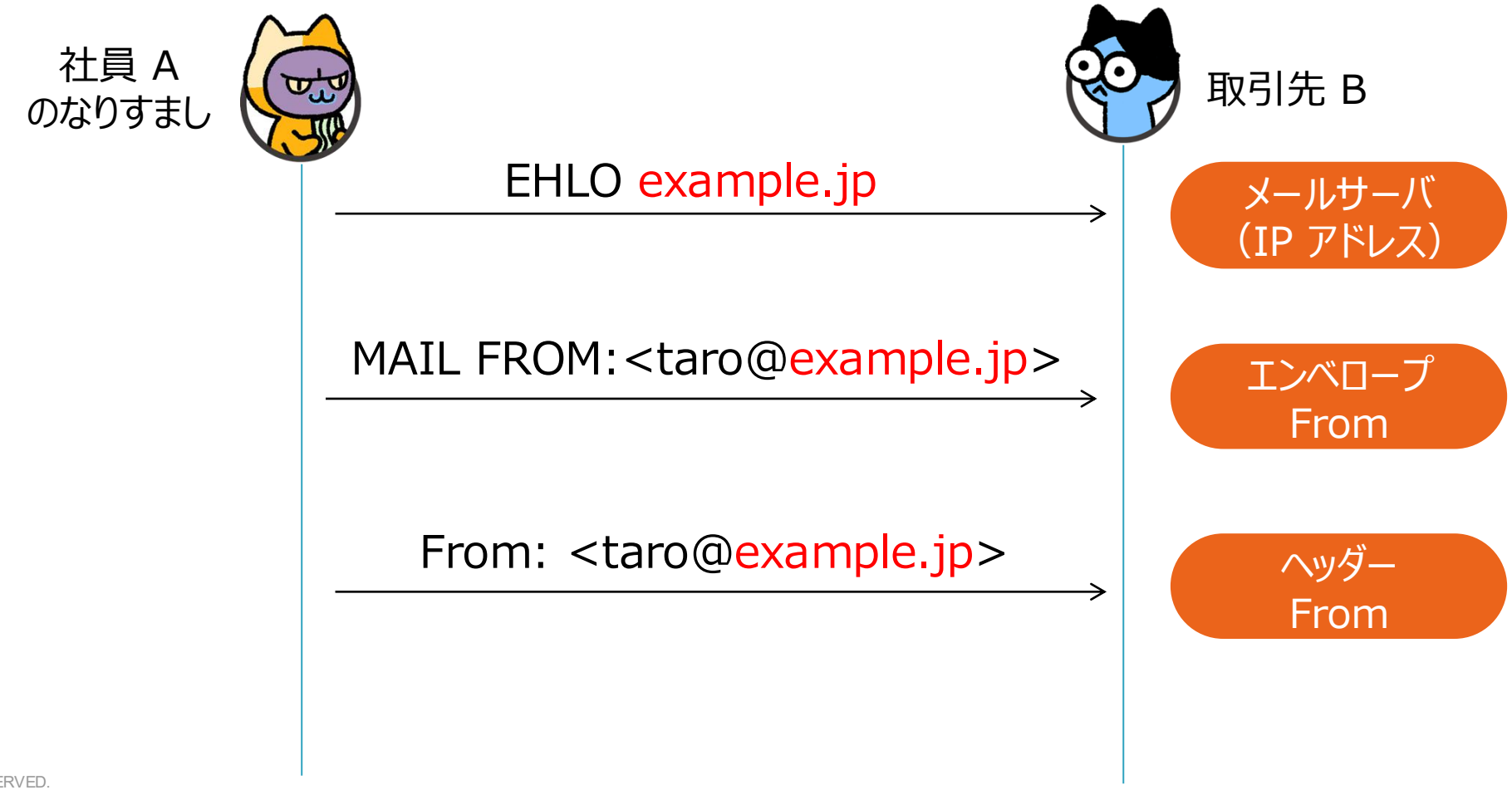
エンベロープ
From

From: <taro@example.jp>

ヘッダー
From

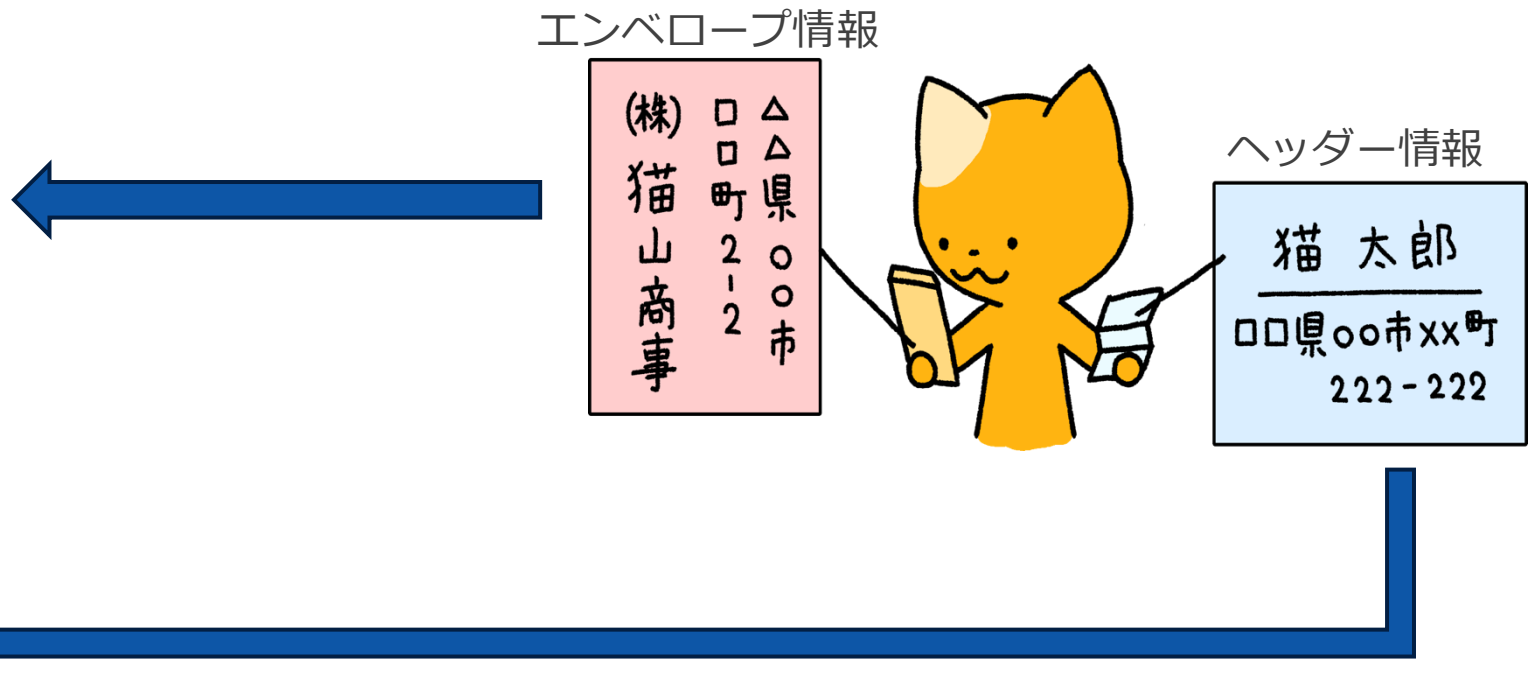
典型的なメールのなりすまし方法

しかし、攻撃者は SMTP プロトコルでニセ情報を使うことが簡単にできてしまう



2つのFrom (ヘッダー vs エンベロープ)

S: 220 foo.com Simple Mail Transfer Service Ready
C: EHLO bar.com
S: 250-foo.com greets bar.com
S: 250-8BITMIME
S: 250-SIZE
S: 250-DSN
S: 250 HELP
C: MAIL FROM:<Smith@bar.com>
S: 250 OK
C: RCPT TO:<Jones@foo.com>
S: 250 OK
C: RCPT TO:<Green@foo.com>
S: 550 No such user here
C: RCPT TO:<Brown@foo.com>
S: 250 OK
C: DATA
S: 354 Start mail input; end with <CRLF>.<CRLF>
C: From: :<Smith@bar.com>
C: Blah blah blah...
C: ...etc. etc. etc.
C: .
S: 250 OK
C: QUIT
S: 221 foo.com Service closing transmission channel



https://tools.ietf.org/html/rfc5321#section-10 一部改

送信ドメイン認証技術

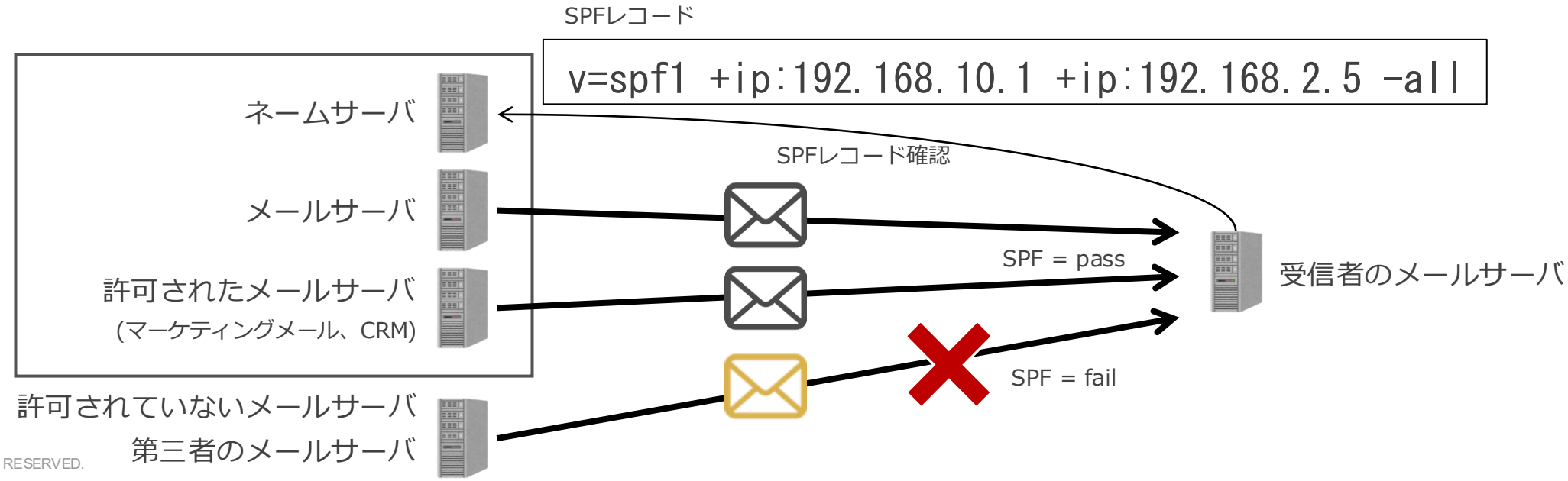
ドメイン単位で送信者が名乗っている情報(メールドメイン)が正しいか確認する技術

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	送信者のエンベロープ From のドメイン
送信者(ドメイン所有者)	許可した IP アドレスリスト(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。

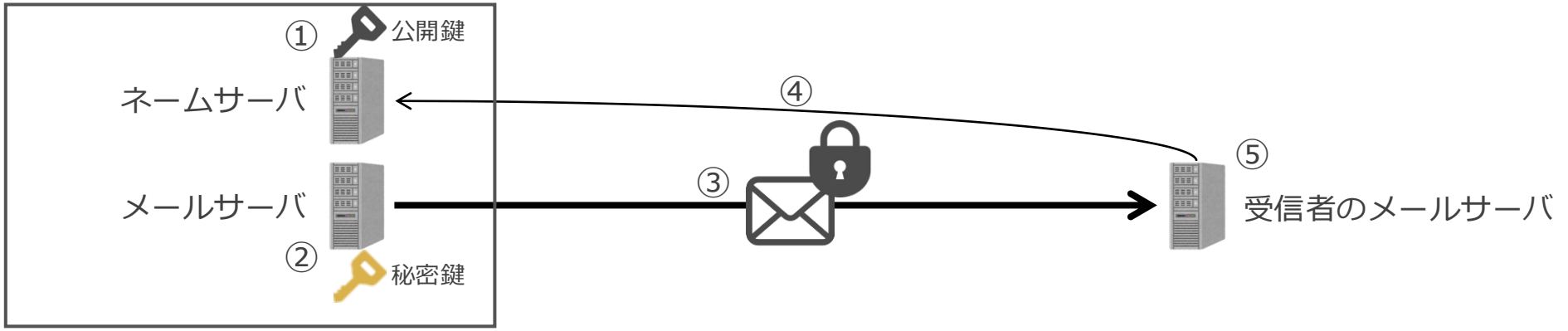


DKIM (DomainKeys Identified Mail)

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: ドメイン所有者が正しいか**

送信者(ドメイン所有者)	① 電子署名に使用する公開鍵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メールに電子署名を付加する。 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(署名ドメイン)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。



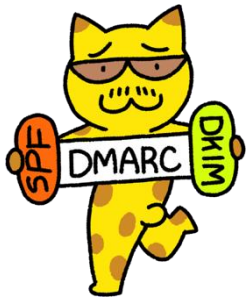
DMARC: 2つの機能

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

2012年
電子メール関連企業・組織により
DMARC.org 設立

2016年
2016年政府サービス義務化

2017年
2017年政府ドメイン義務化

2020年
2023年2月 経産省/総務省/警察庁
カード会社などへ DMARC 導入要請

2024年
2024年2月 Google/Yahoo.com
DMARC をメール送信ガイドラインに追加

2025年
2025年1月 国内大手メールサービス
DMARC 必須化

2026年
DMARC RFC 改訂 (9989,9990,9991)

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)
    - 受信箱へ入れる
  - quarantine (隔離する)
    - 迷惑メール判定する、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

DMARC - 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
- SPF、DKIM いずれかで認証 Pass
- ヘッダー Fromを保護できる

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）に上記のような宣言をする
- 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

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

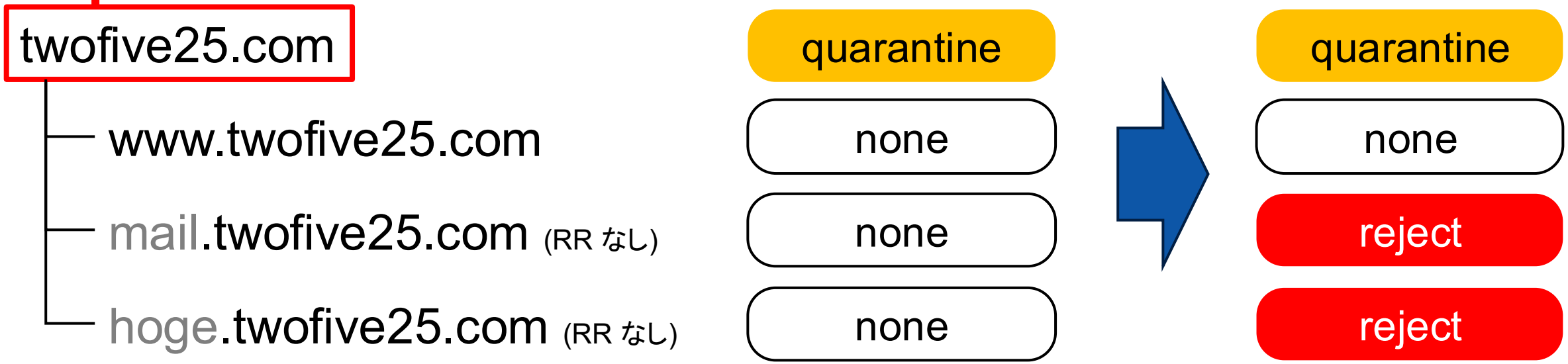
v=DMARC1; p=none; rua=mailto:rua@example.com

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
np	存在しないサブドメインのポリシー (none, quarantine, reject)		-	sp=,p=と同じ
pct	ポリシー適用する割合 (0-100)	pct=20	廃止	pct=100
t	テストモードかどうか	t=y	-	t=n
psd	Public Suffix Domain であるかどうか (y, n, u)	psd=y	-	psd=u
rua	集計レポート送信先	rua=mailto:rua@example.jp	-	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	-	aspf=r
adkim	DKIMアライメントモード (r, s)	adkim=s	-	adkim=r
fo	失敗レポートのオプション (0, 1, d, s)	fo=1	-	0
rf	失敗レポートの形式 (現状 afrf のみ)	rf=afrf	-	afrf
ri	集約レポートの送信間隔(秒)	ri=14400	廃止	86400

[キャッチアップ] DMARC レコードの np=タグ

ドメイン名が存在しない（NXDOMAIN）の場合の取り扱いを指示するタグ。
意図しないサブドメインを詐称した場合に np= で指定したポリシーとなる。

v=DMARC1; p=quarantine; sp=none; np=reject;



[キャッチアップ] DMARC レコードの np=タグ

ドメイン名が存在しない（NXDOMAIN）の場合の取り扱いを指示するタグ。
意図しないサブドメインを詐称した場合に np= で指定したポリシーとなる。
今後は、PSD(Public Suffix Domain)での運用が想定される。

v=DMARC1; p=reject; sp=none; np=reject;

[キャッチアップ] DMARC レコードの t=タグ（pct=タグの代替）

ポリシー適用割合を示していた pct= の代替としてテストモードを t= で指示するタグ。
Enforcement する前のテスト用として利用が想定され、pct= を 100 以外で指定しているドメインはあらかじめ t=y を追加するなどの注意が必要。

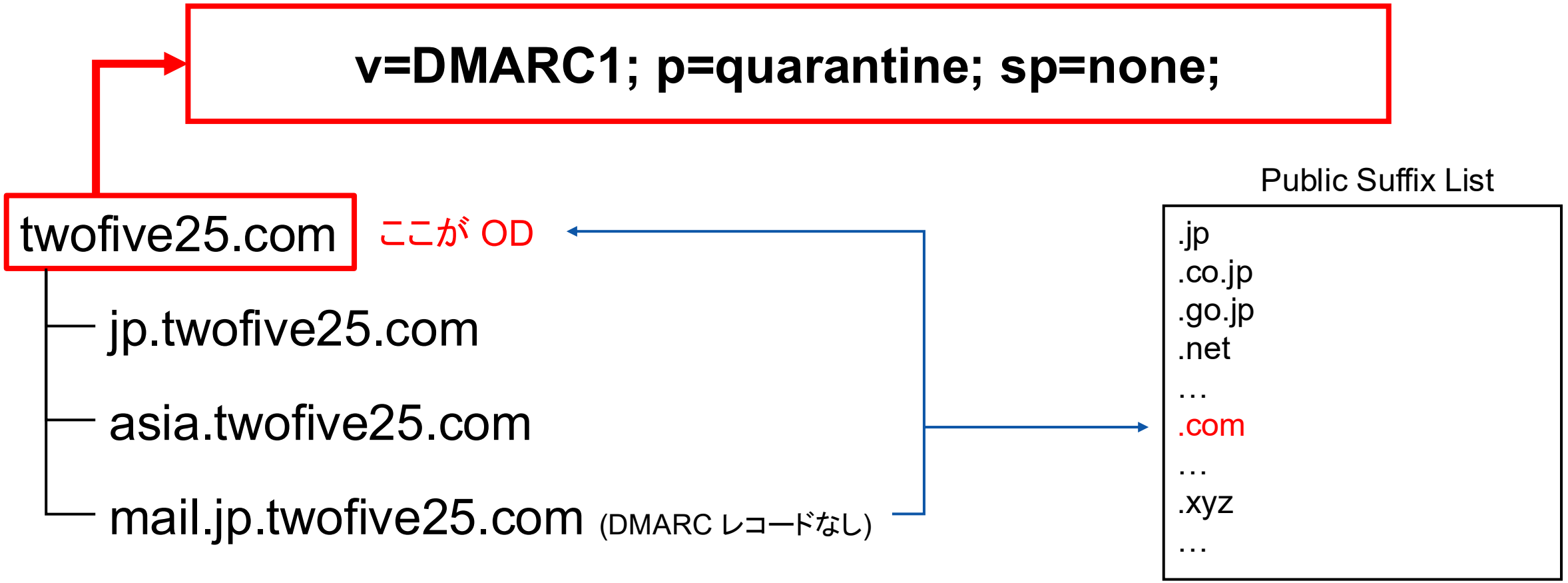
v=DMARC1; p=reject; pct=50;

新しい規格に従えば・・・

v=DMARC1; p=reject;

[キャッチアップ] DMARC レコードの psd=タグ

どのドメインが組織ドメイン(Organizational Domain) であるかを、従来の
Public Suffix List に頼らずに探索・決定するためのタグ。
特に、PSD やサブドメインが複数組織で利用されている場合の利用が想定される。



[キャッチアップ] DMARC レコードの psd=タグ

どのドメインが組織ドメイン(Organizational Domain) であるかを、従来の
Public Suffix List に頼らずに探索・決定するためのタグ。
特に、PSD やサブドメインが複数組織で利用されている場合の利用が想定される。

v=DMARC1; p=quarantine; sp=none; psd=n;

- twofive25.com　ここが OD
  - jp.twofive25.com
  - asia.twofive25.com
  - mail.jp.twofive25.com (DMARC レコードなし)

Public Suffix List

.jp
.co.jp
.go.jp
.net
…
.com
…
.xyz
…

[キャッチアップ] DMARC レコードの psd=タグ

どのドメインが組織ドメイン(Organizational Domain) であるかを、従来の
Public Suffix List に頼らずに探索・決定するためのタグ。
特に、PSD やサブドメインが複数組織で利用されている場合の利用が想定される。

v=DMARC1; p=quarantine; sp=none; psd=y;

twofive25.com ここが PSD
- jp.twofive25.com ここが OD
- asia.twofive25.com ここが OD
- mail.jp.twofive25.com (DMARC レコードなし)

Public Suffix List

.jp
.co.jp
.go.jp
.net
…
.com
…
.xyz
…

[キャッチアップ] DMARC ポリシー切り替えアプローチ

これまでの DMARC 運用の経験を踏まえたポリシー切り替えのアプローチが追記。
特に銀行や金融機関などの通知メールなどは reject が適している。
一般ドメインは DMARC レポートの運用を踏まえて quarantine や reject を選択。

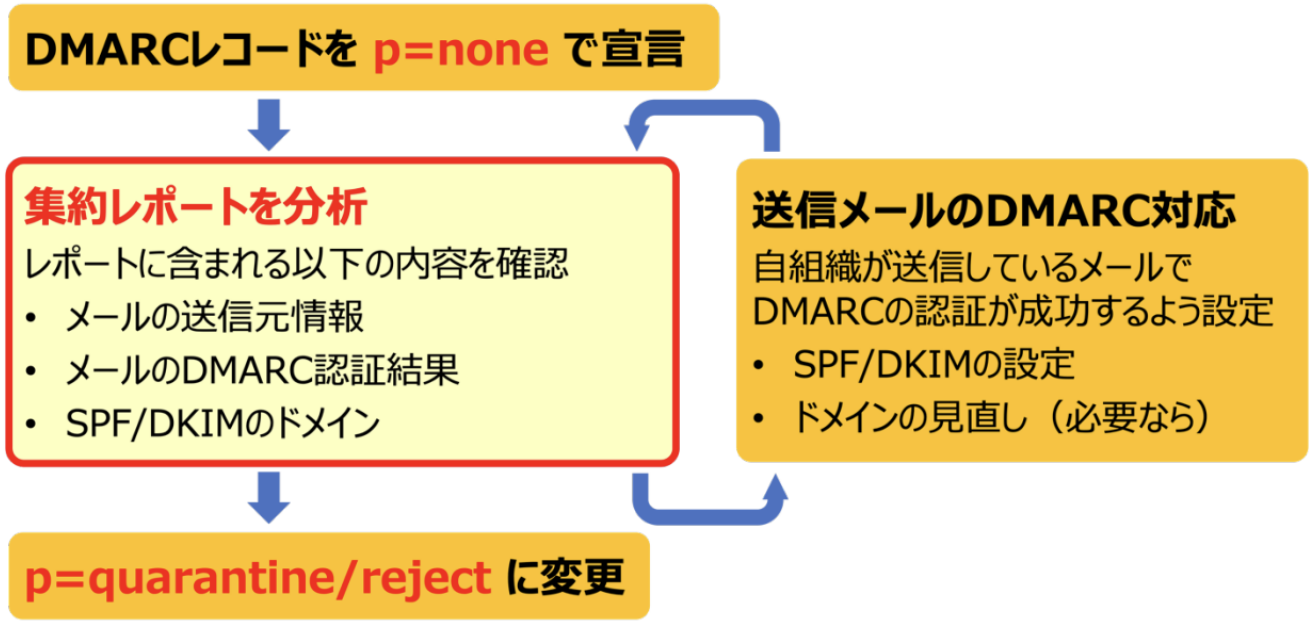


図 5.1 改善サイクルイメージ

- 間接メールフローの把握とリスク管理
- ポリシー切り替えの指標と基準
- ポリシー切り戻し判断基準の準備

DMARCポリシー変更のためのガイドブック V1.0
https://www.dekyo.or.jp/soudan/data/anti_spam/dmarc_guidebook.pdf

メール運用キャッチアップ
- 証明書管理