JPAAWG Japan Anti-Abuse Working Group

フィッシングメールの現状と対策（2020年前半版）
～DMARC 視点～

JPAAWG / TwoFive, Inc.

加瀬　正樹

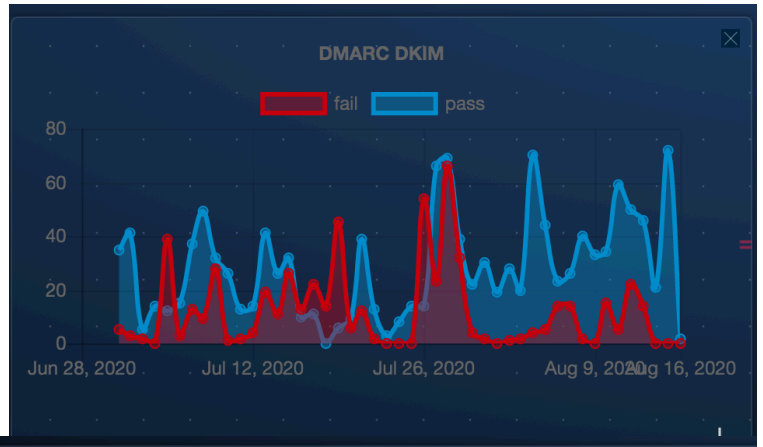
DMARC is

- DMARC は送信ドメインのなりすましを認証できる
- DMARC はなりすましたメールの取り扱いを宣言できる
- DMARC は認証結果のフィードバックを活用できる

```
Subject: Report Domain: twofive25.com Submitter: dmarc25.jp
From: DMARC/25 <report@dmarc25.jp>
To: rua@twofive25.com

--===============2253015245159906169==
Content-Type: application/gzip
MIME-Version: 1.0
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename="dmarc25.jp!twofive25.com!1597104000!1597190399!59870
2287560a097d8624baf3c535b5f.xml.gz"

H4sICGVEM18C/3NvZnRlc3QuYml6IXJvdhTWXfXf6DwAA//
. . .
8DANE7ApF/AwAA
--===============2253015245159906169==--
```



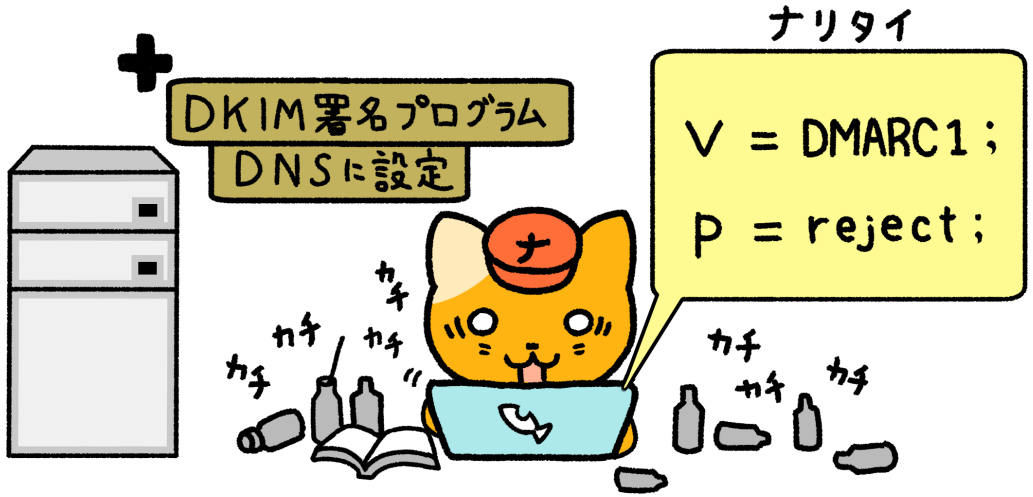
ホスト / IPアドレス	分類	国名	メール通数	DMARC DKIM Pass	DMARC SPF Pass	DKIM Pass	SPF Pass	ARC Pass
				%	%	%	%	%
mx01.twofive25.com 153.126.164.35		Japan	349	315 90.26%	349 100.00%	315 90.26%	349 100.00%	0 0.00%

DMARC is NOT

- DMARC はメールソフトの表示名を守れない（Phriendly Name）
- DMARC は類似ドメイン詐称は防げない（Homograph Domain Spoofing）
- DMARC はドメイン信頼性は見分けない（Domain Reputation）
- DMARC はアカウント不正利用は防げない（Email Account Compromise）
- DMARC はソーシャルエンジニアリング攻撃は防げない

ツール・Milter の活用

- OpenDKIM　　DKIM 署名機能、DKIM 検証機能
- OpenDMARC　　DMARC+SPF 検証、DMARCレポート機能
- YENMA　　IIJ 開発 Milter、SPF＋DKIM＋DMARC 検証機能
- RUA25　　DMARC+DKIM+SPF 検証、DMARC レポート機能



DMARC レポート供給

- 供給元の TOP2 は Google と Yahoo.com（90%以上）
- ここ1年の普及割合では、JPドメインは停滞気味

※ 2019年8月、2020年8月、TwoFive 調査

DMARC 失敗メールの取り扱い

- DMARC に失敗したメールはどのくらい隔離・拒否されるのか？

※ 2019年1月～2020年7月、TwoFive 調査

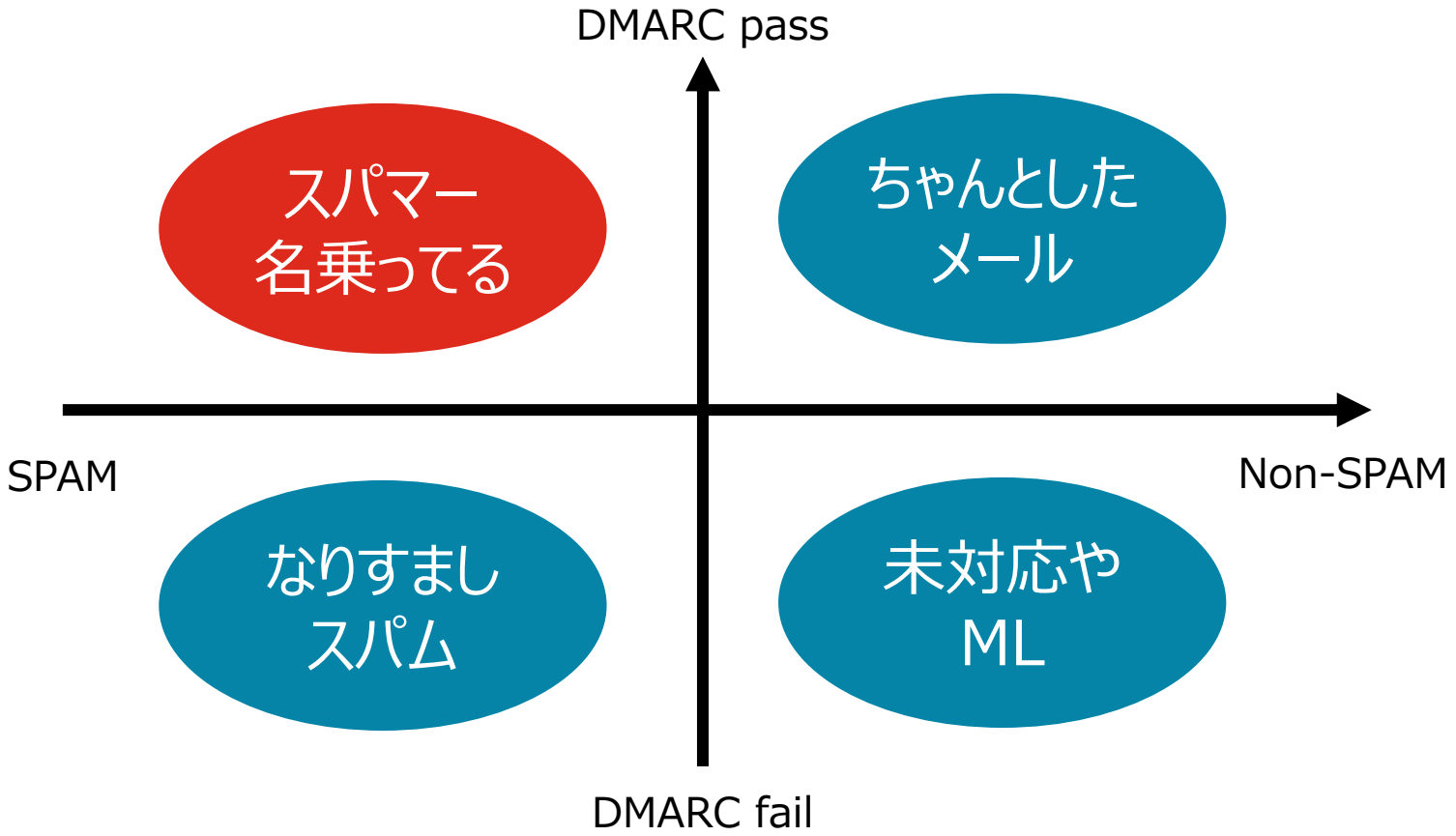
DMARC 準拠・サブドメイン詐称

- 組織ドメイン（Organizational Domain = OD）で DMARC に対応している場合、ランダム文字列のサブドメイン詐称は把握できる

※ 2020年1月、TwoFive 調査

c.f. スパム VS DMARC 関係性

- DMARC ってスパマーの方が対応してるんじゃないか？



c.f. 類似ドメイン詐称

- DMARC では保護できないさまざまな手法

※ 2020年6月～8月、TwoFive 調査

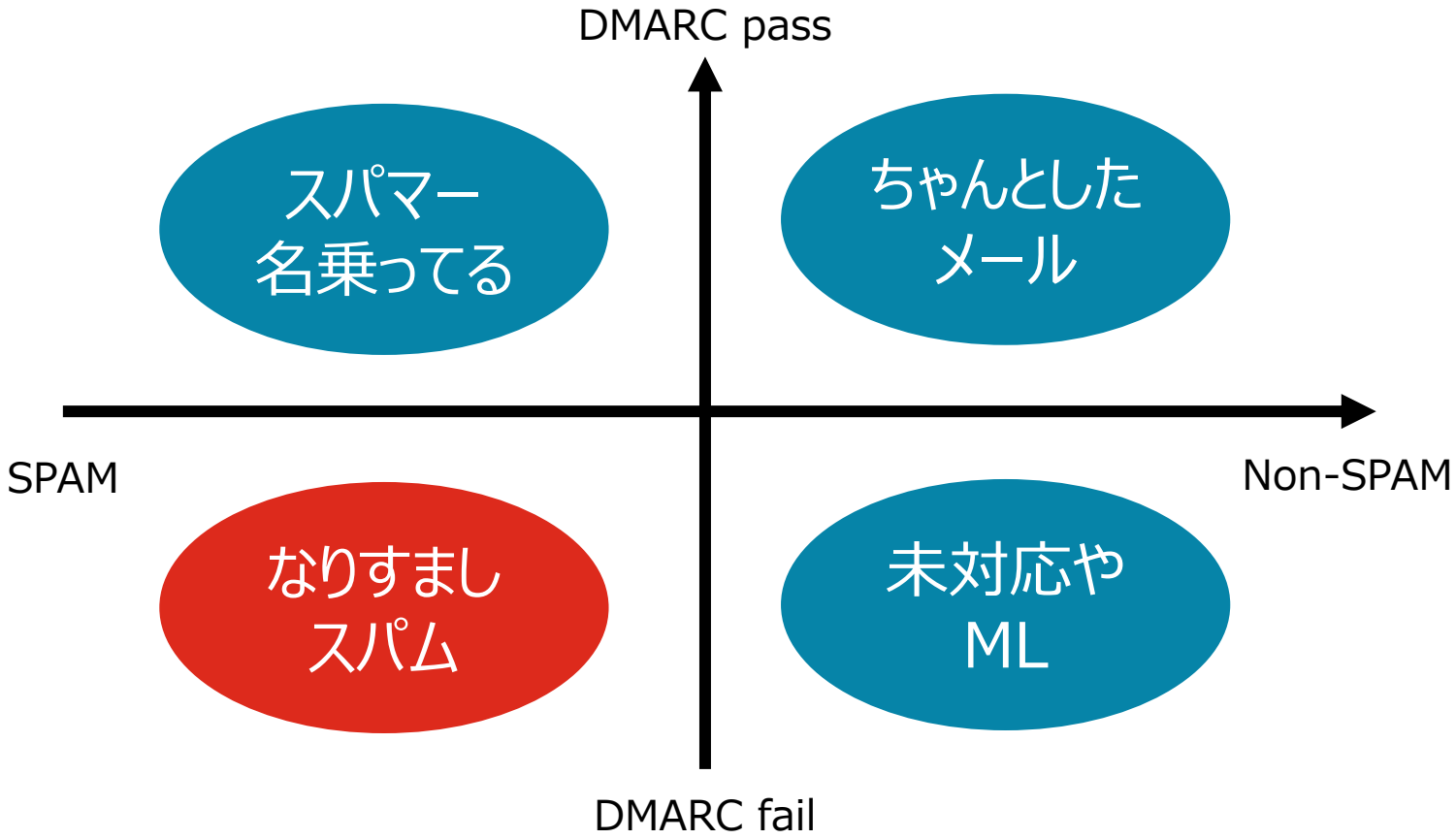
c.f. 類似ドメイン詐称

- DMARC では保護できないさまざまな手法

※ 2020年6月～8月、TwoFive 調査

c.f. スパム VS DMARC 関係性

- DMARC ってスパマーの方が対応してるんじゃないか？



c.f. 類似ドメイン詐称

- DMARC でも対策できる手法

※ 2020年6月～8月、TwoFive 調査

c.f. 類似ドメイン詐称

- DMARC でも対策できる手法

※ 2020年6月～8月、TwoFive 調査