Email Security Conference 2017
IAjapan 第16-17回 迷惑メール対策カンファレンス

『DMARC導入事例の紹介』

株式会社コミュニティネットワークセンター

ニコライ ボヤジエフ

2017年9月

自己紹介

名前：　ニコライ ボヤジエフ

出身：　ブルガリア《България》

在日ブルガリア人：
300人未満 ※

所属：　株式会社コミュニティネットワークセンター
技術本部　サーバグループ

担当：　メールサービス、仮想化基盤、
各種サーバシステムの運用と開発をやってます

※鳴戸部屋新親方含む

会社紹介

株式会社 コミュニティネットワークセンター
http://www.cnci.co.jp/

- **東海地方（愛知、岐阜、三重）のケーブルMSO**
- **デジタル放送サービスとインターネット接続サービスを提供 (主にB2B)**
- **数十万アカウントのメールシステムを自社で運営**
- **所在地：名古屋**

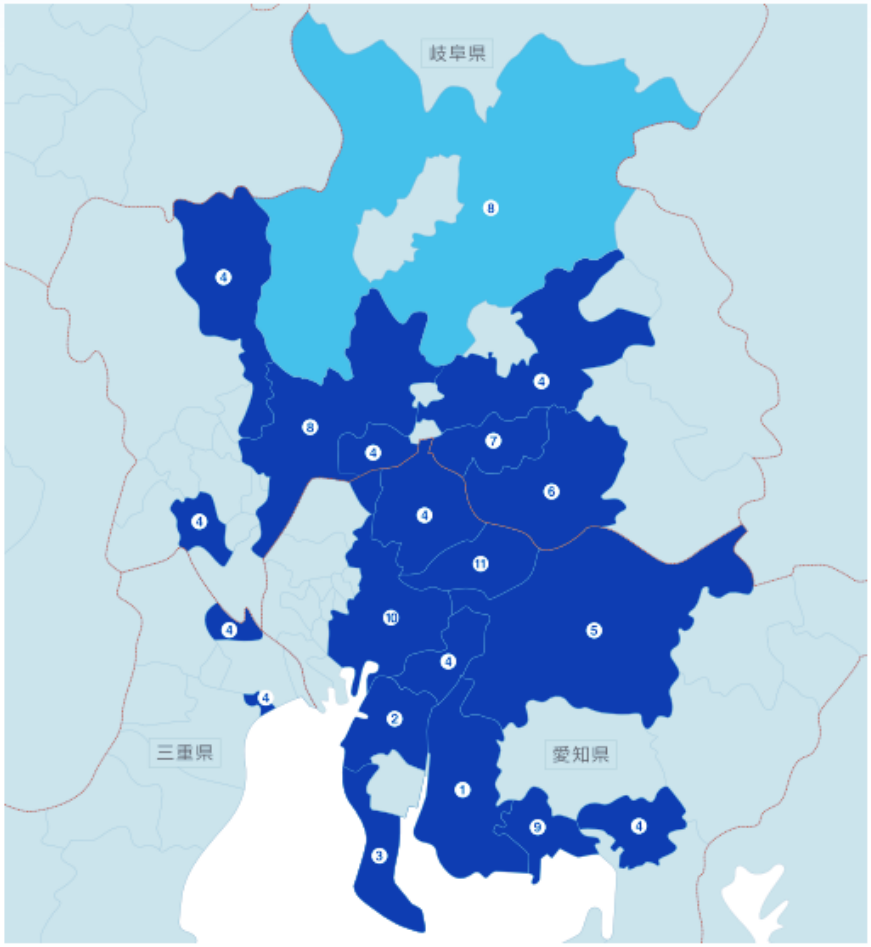
(DMARCを宣言してます)

```
$ dig _dmarc.cnci.co.jp TXT +short
"v=DMARC1¥; p=none¥; adkim=s¥; aspf=s“

$ dig _dmarc.cnci.nagoya TXT +short
"v=DMARC1¥; p=none¥; adkim=s¥; aspf=s“
```

会社紹介

株式会社 コミュニティネットワークセンター
http://www.cnci.co.jp/



【参考URL】
https://ja.wikipedia.org/wiki/コミュニティネットワークセンター

①株式会社キャッチネットワーク
②知多メディアスネットワーク株式会社
③知多半島ケーブルネットワーク株式会社
④中部ケーブルネットワーク株式会社
⑤ひまわりネットワーク株式会社
⑥おりべネットワーク株式会社
⑦株式会社ケーブルテレビ可児
⑧シーシーエヌ株式会社
⑨三河湾ネットワーク株式会社
⑩スターキャット・ケーブルネットワーク株式会社
⑪グリーンシティケーブルテレビ株式会社

他の事業者からのインフラによって
サービスを提供しているエリア

今日の話しの背景

➢ 今年、メールシステムを大幅にリニュアルしました

項目	前システム	新システム
サービスイン時期	2010年～	2017年３月～
受信プロトコル	POP	POP/IMAP
メールボックス容量	100MB	10GB
海外アクセス制限機能 ※デフォルト制限なし	なし	あり
不正アクセス対応の自動化	なし	あり
MTAのTLS対応	SMTP-out	SMTP-in (MX) SMTP-out
なりすまし対策	SPF (宣言/検証) DMARC (宣言)	**SPF (宣言/検証)** **DKIM (署名/検証)** **DMARC (宣言/検証/ポリシー適用※)** **なりすまし警告表示** **安心マーク (JIPDEC)**

今日はこの辺りの話しです

※ポリシー適用対応だが、現在未実施

DMARCの活用事例

1. 自社管理ドメインのDMARC宣言 (p=none; ruf/ruaなし) ※以前から
2. DMARC検証結果を Authentication-Results ヘッダに記載
3. なりすまし警告の判定でDMARCを活用
4. 安心マーク (JIPDEC) の判定でDMARCを活用
5. dmarc=fail 時のポリシー適用対応 ※将来的に有効化

1．DMARC宣言について

- **エンドユーザが様々な送り方をしているため、到達性に影響がでないように、エンドユーザ向けドメインにたいして p=none で宣言しています**

  ※例えば、小企業メールサーバから「差出人：ISPメールアドレス」でメール送信した場合がある

- **現時点、DMARCレポートの活用用途がないため、rua/ruf なしで宣言しています**
- **DMARC の宣言範囲 (特に、親ドメイン) を注意してます**

(DMARC宣言の例)

ドメイン	ドメイン区分	DMARCレコード	備考
starcat.ne.jp	親	なし	管理外システムでメール送信しているため、宣言しない
sa.starcat.ne.jp	サブ	v=DMARC1¥; p=none	エンドユーザ向けドメイン
sb.starcat.ne.jp	サブ	v=DMARC1¥; p=none	エンドユーザ向けドメイン
sc.starcat.ne.jp	サブ	v=DMARC1¥; p=none	エンドユーザ向けドメイン
sd.starcat.ne.jp	サブ	v=DMARC1¥; p=none	エンドユーザ向けドメイン
…	…	…	…

2．Authentication-Results ヘッダ記載について

- **DMARCの検証結果を Authentication-Results ヘッダに記載しています**
- **SPF検証結果を Received-SPF ヘッダに記載しています**

(ヘッダの例)

```
Authentication-Results: cmx03.m.cnci.ad.jp; dkim=pass header.d=gmail.com
 header.b=ixomVXch; dmarc=pass header.from=gmail.com; x-token-a=pass;
 x-token-b=pass
Received-SPF: PASS identity=mailfrom; envelope-from="example@gmail.com"
```

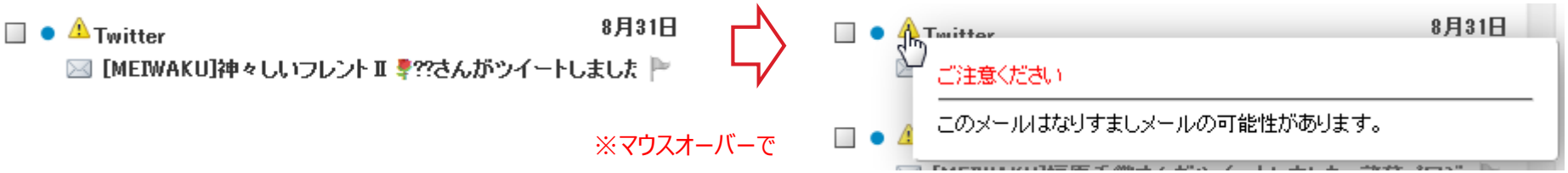
3．なりすまし警告の判定でDMARC活用

- **なりすましの可能性があるメールに対して、Webメールで「警告」を表示させています**
- **dmarc=failで警告表示できるが、ドメインリストと合致する条件を加えています**
- **「X-Senderauth-Result: fail」のカスタムヘッダも付与しています**

【なぜドメインリストと組み合わせるか？】

- p=noneでも警告表示できるようにしたかった (国内でp=rejectまだない…)
- 転送メール等の誤判定を防止したかった
- ドメインリストと組み合わせると柔軟性がある (リスト管理運用が発生しますが…)

(警告の例)



４．安心マーク (JIPDEC) の判定でDMARC活用

➢ JIPDECの「安心マーク」仕組みに対応しています。

※詳しくは、JIPDECホームページ参照：
https://robins-cbr.jipdec.or.jp/usecase/anshinmark/

＜表示条件＞

ここで
DMARC活用

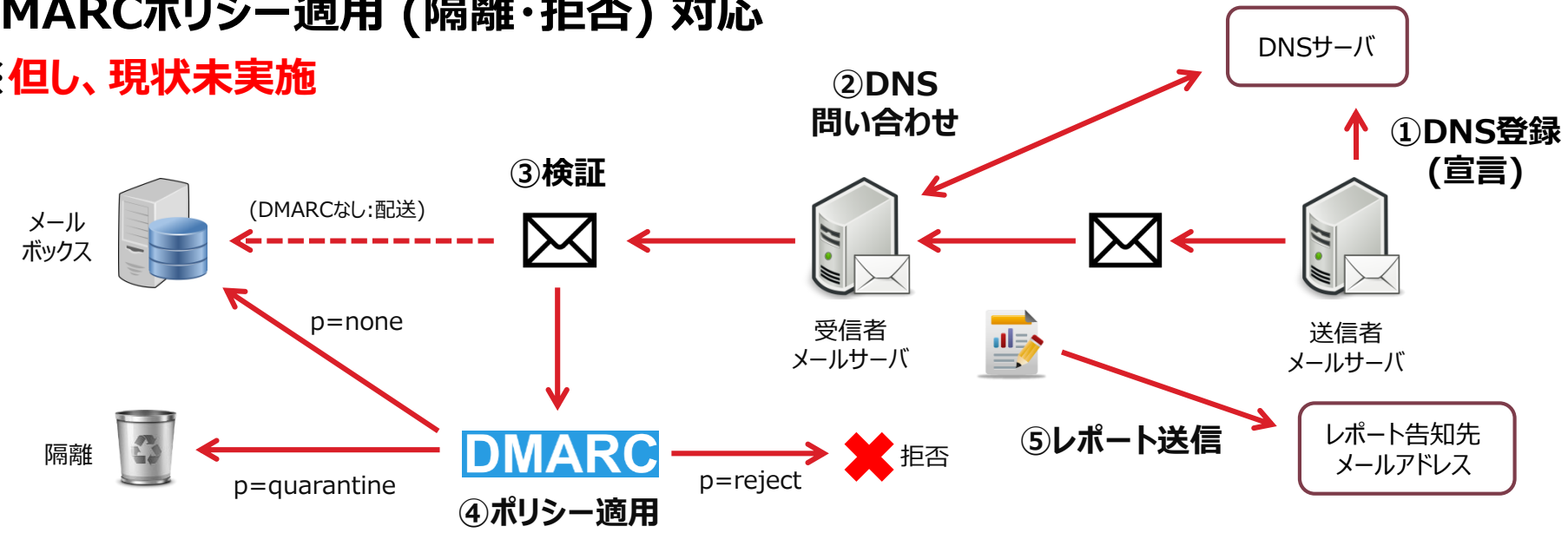
安心マーク表示条件 (OR)	内容
条件 (1)	【dmarc=pass】AND 【header.fromドメインがROBINS DBに収容されているドメインに合致】
条件 (2)	【dmarc=none】AND 【DKIM作成者署名(※)がpassしている】AND 【header.fromドメインがROBINS DBに収容されているドメインに合致】

※ DKIMのdタグドメインと作成者ドメイン(header.fromドメイン)が同じ

5．DMARCポリシー適用について

➢ DMARCポリシー適用 (隔離･拒否) 対応

※但し、現状未実施



【なぜDMARCポリシー適用してないか？】

- 法律的な解釈 (「通信の秘密」関連) が明確になっていなかった
- DMARCが知られてない、主流になっていない

➡ 将来的に、ポリシー適用がすぐ有効化できます

フィッシング対応でDMARCを活用

- **8月31日に当社ドメインを使ったフィッシングメールがエンドユーザ宛てに来ました**

あなたのWebMailをアップグレードする / Upgrade Your WebMail　2017年08月31日 午後 9:25

差出人: "Mediacat / STARCAT" <surpport@mediacat.ne.jp>

support@ではなく、
surpport@

--
Mediacat / STARCATへようこそ
あなたのメールアカウントをアップグレードする必要があります
下記のリンクをクリックし、Eメールアドレスとパスワードでログインしてアップグレードしてください

http://[redacted].de/mediacat.ne.jp/

このメッセージを読んだあとに失敗すると、アカウントは閉鎖され、すべてのメッセージと情報は失われます。

ありがとうございました
Mediacat / STARCATサポートチーム

==========

Welcome to Mediacat / STARCAT
Your Email Account must be Upgraded
Click the link below and log in with your E-Mail Address and password for upgrading

http://[redacted].de/mediacat.ne.jp/

Failure to do so after reading this message, your account will be CLOSSED and all your messages and information will be lost.

Thank you
Mediacat / STARCAT Support Team

フィッシング対応でDMARCを活用

- **ホームページで注意喚起をしました**

http://www.starcat.co.jp/announcement/20170901002342.html

- **自社ドメインでDMARC宣言したいたので、なりすまし警告表示ですぐ対応しました。**

(ヘッダ情報)

```
X-Spam-Score: 0.00
X-Spam: No
X-Country-Code: JP
Authentication-Results: cmx03.m.cnci.ad.jp; dmarc=fail
 header.from=mediacat.ne.jp; x-token-a=none; x-token-b=fail
X-Senderauth-Result: fail
Received-SPF: SOFTFAIL identity=mailfrom;
 envelope-from="surpport@mediacat.ne.jp"
```

フィッシング対応でDMARCを活用

- **Webメールで警告マークを表示**

- **自社ドメインなので、DMARC (p=none) で宣言しているが、警告表示対象リストに追加することで、dmarc=fail時に警告表示ができました**

まとめ

- システムリニューアルで最新の送信ドメイン認証技術DMARCを取り入れました
- 現状、警告表示や安心マーク表示で活用しています
- 今後、国内でも主流になっていくため、フル活用できるようにシステム対応してます
- ISPとして自社ドメインで保守的なDMARC宣言 (p=none) しているため、DMARCを使って自社ドメインが守れないと思っていましたが、フィッシング対策でDMARCを簡単に活用できて感動しました。