第17回迷惑メール対策カンファレンス

マーケティングメールやビジネスメールにおけるDMARCの活用事例

遠藤　慈明（パイプドビッツ）
小早志　康次（チーターデジタル）
加瀬　正樹（TwoFive）

講師紹介

遠藤　慈明

株式会社パイプドビッツ
社長室長

小早志　康次

チーターデジタル株式会社
Head of Deliverability

加瀬　正樹

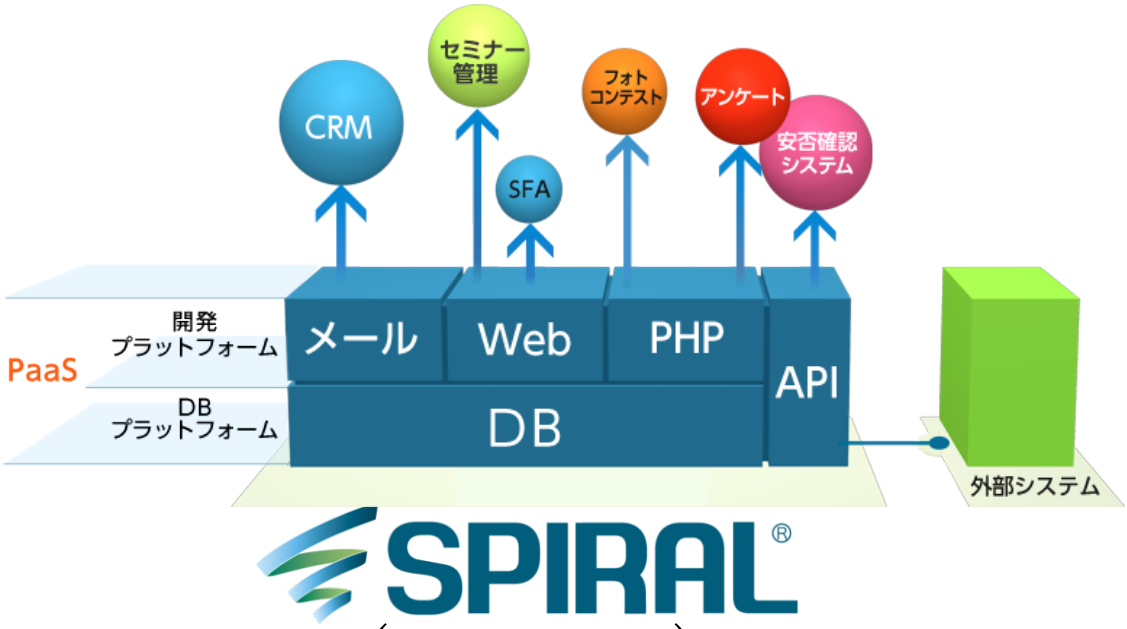
株式会社 TwoFive
開発マネージャー
一般財団法人日本情報経済社会推進協会（JIPDEC）
客員研究員

今日のファシリテータを務めさせていただきます

PIPED BITS

スパイラルブランド / クラウド事業

PaaS ～ウェブアプリケーション開発～



SPIRAL®

（ smp.ne.jp ）

グループウェア

SPIRAL PLACE®

EC

SPIRAL EC Fashion meets IT

- 10,000AC以上
  金融,官公庁多い
- スピード開発
- データ管理が得意
- 高速メール配信

株式会社パイプドビッツ（パイプドHDグループ）

CHEETAH DIGITAL

エイケア・システムズ
（メール配信システム日本No1）

ALTOVISION
アルトビジョン
（メールマーケティングコンサル日本No1）

M&A

エクスペリアン
experian

- マーケティングサービス
- 信用情報サービス
- 意思決定分析サービス
- コンシューマーサービス

独立

CHEETAH DIGITAL

日本法人は元エイケアシステムズ、元アルトビジョン、そしてエクスペリアンのマーケティングサービス事業部を母体として、チームを再編成。
1999年より日本国内で培ってきたデジタルコミュニケーションに関する人財と知見はそのままに、より強力マーケティングテクノロジーを日本市場で展開。

マーケティングツールの提供

- マーケティングオートメーション（CCMP）
- メール配信システム（MailPublisher）

導入・運用支援

- 要件定義
- 環境構築
- システム構築
- データ連携

プロフェッショナルサービス

- マーケティング戦略立案
- シナリオ立案
- クリエイティブ制作
- コンテンツ配信代行

アジェンダ

- DMARC の復習とレポート状況
- DMARC 対応した企業の事例紹介
- 企業が DMARC に対応するには？
- 会場からの質疑

DMARC 復習とレポート状況

詳しくは他セッションで

DMARC とは

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

＋

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排除できます

主な DMARC 対応ドメイン（DNS 設定している）

国内 ISP でも DMARC レコードを設定しているドメインは多く見つかる

```
$ dig +short _dmarc.so-net.ne.jp txt
"v=DMARC1¥; p=none"
$ dig +short _dmarc.biglobe.ne.jp txt
"v=DMARC1¥; p=none"
$ dig +short _dmarc.nifty.com txt
"v=DMARC1¥; p=none¥; rua=mailto:dmarc-rua-com@nifty.com"
$ dig +short _dmarc.iij.ad.jp txt
"v=DMARC1¥; p=none¥; adkim=s¥; aspf=s¥; rua=mailto:dmarc-rua@iij.ad.jp¥; ruf=mailto:dmarc-
ruf@iij.ad.jp"
$ dig +short _dmarc.dti.ne.jp txt
"v=DMARC1¥; p=none”
$ dig +short _dmarc.yahoo.ne.jp txt
"v=DMARC1¥; p=quarantine¥; rf=afrf¥; rua=mailto:ymail_dmarc_report@yahoo.ne.jp¥;
ruf=mailto:ymail_dmarc_report@yahoo.ne.jp”
$ dig +short _dmarc.docomo.ne.jp txt
"v=DMARC1¥; p=none"
$ dig +short _dmarc.ezweb.ne.jp txt
"v=DMARC1¥; p=none"
$ dig +short _dmarc.softbank.ne.jp txt
"v=DMARC1¥; p=none"
$ dig +short _dmarc.mufg.jp txt
"v=DMARC1¥; p=none¥; fo=1¥; rua=mailto:bank-of-tokyo-mitsubishi@rua.agari.com¥;
ruf=mailto:bank-of-tokyo-mitsubishi@ruf.agari.com"
```

主な DMARC 対応ドメイン（ポリシーを適用している）

海外ドメインを中心に DMARC ポリシーを適用している ISP は見つかる

当日限り

あるドメインの特定1日分の disposition が reject であるレポートを集計（加瀬調べ）

主な DMARC 対応ドメイン（レポートを送付している）

当日限り

あるドメインの特定1日分のレポートを集計（TwoFive調べ）

主な DMARC 対応ドメイン（レポートを送付している）

当日限り

あるドメインの特定1日分のレポートを集計（TwoFive調べ）

海外における DMARC 事情

How HMRC's use of DMARC Helped it stop 300,000 phishing emails
http://www.information-age.com/how-hmrcs-use-of-dmarc-helped-it-stop-300000-phishing-emails-123467934/

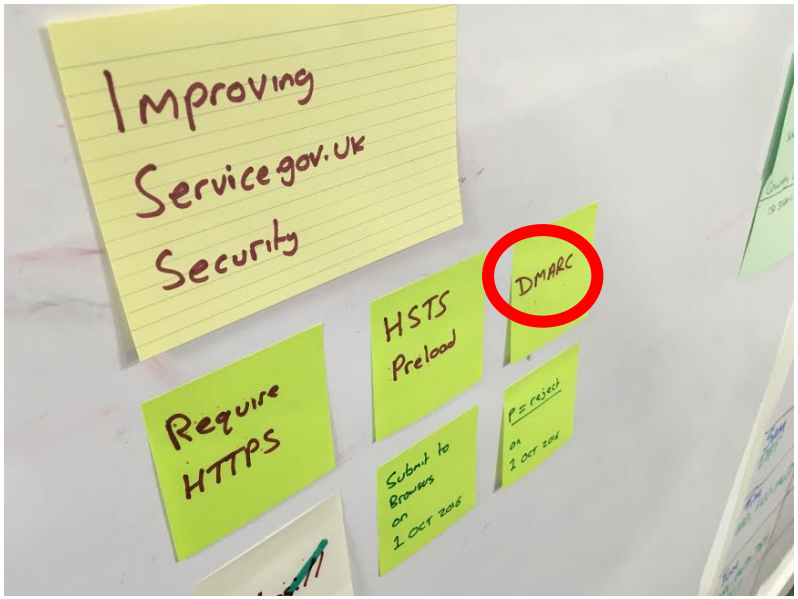
HMRC のサイバーセキュリティ責任者は、DMARC 実装に取り組み、チームは膨大な予算を3億ドル削減した

"It's notable that UK firms with a large customer base of consumers are most likely to adopt DMARC."
https://www.infosecurity-magazine.com/news/fortune-500-and-ftse-100-firms/

大きな顧客を持つ英国の企業が DMARC を対応する可能性が高いのは注目すべきである

海外における DMARC 事情

Updating our security guidelines for digital services



英国の電子サービス向けガイドラインに **DMARC** の記述

“p=reject
少なくとも p=none で上書きすべき”

https://gdstechnology.blog.gov.uk/2016/06/28/updating-our-security-guidelines-for-digital-services/

DMARC 対応に向けた環境

Who Is Using DMARC?

- ADP (adp.com)
- Aetna (aetna.com)
- Air BnB (airbnb.com)
- American Express (americanexpress.com, aexp.com)
- American Greetings (americangreetings.com) [1] [2]
- Apple Music (applemusic.com)
- Box (box.com)
- *British Airways (britishairways.com)*
- Chase Bank (chase.com, jpmchase.com) [1] [2]
- Citibank (citibank.com)
- DHL (dhl.com)
- Evernote (evernote.com)
- Facebook (facebook.com) [1]
- FedEx (fedex.com)
- *The Gap (gap.com)*
- GroupOn (groupon.com)
- Instagram (instagram.com)
- LinkedIn (linkedin.com) [1] [2]
- *Old Navy (oldnavy.com)*
- PayPal (paypal.com) [1] [2] [3]
- Pinterest (pinterest.com)
- Publishers Clearinghouse (pch.com)
- Rolling Stone (mail.rollingstone.com)
- Squarespace (squarespace.com)
- Twitter (twitter.com)
- United Parcel Service (ups.com)
- US Federal Trade Commission (ftc.gov)
- US Senate (senate.gov)
- US Postal Service (usps.gov)
- USAA (usaa.com)
- Wachovia Bank (wachovia.com)
- *Wells Fargo (wellsfargo.com)*
- WhatsApp (whatsapp.com)

Deployment Tools

DNS Record Lookup and Parsing

- Agari: DKIM, DMARC, and SPF lookup tools (scroll down, below webinar link)
- dmarcian.com: DMARC Inspector (retrieve and check DMARC record for a domain)
- dmarcian.com SPF Surveyor (recursively retrieve and expand SPF records)
- dmarcanalyzer.com Validate SPF Record (recursively retrieve and expand SPF records)
- Online Trust Alliance: Query Tool for DMARC Records
- Proofpoint: DMARC Record Check
- Proofpoint: SPF Record Check
- Scott Kitterman's SPF Record Test Tool
- ValiMail: DMARC and SPF Record Check

Message Validation

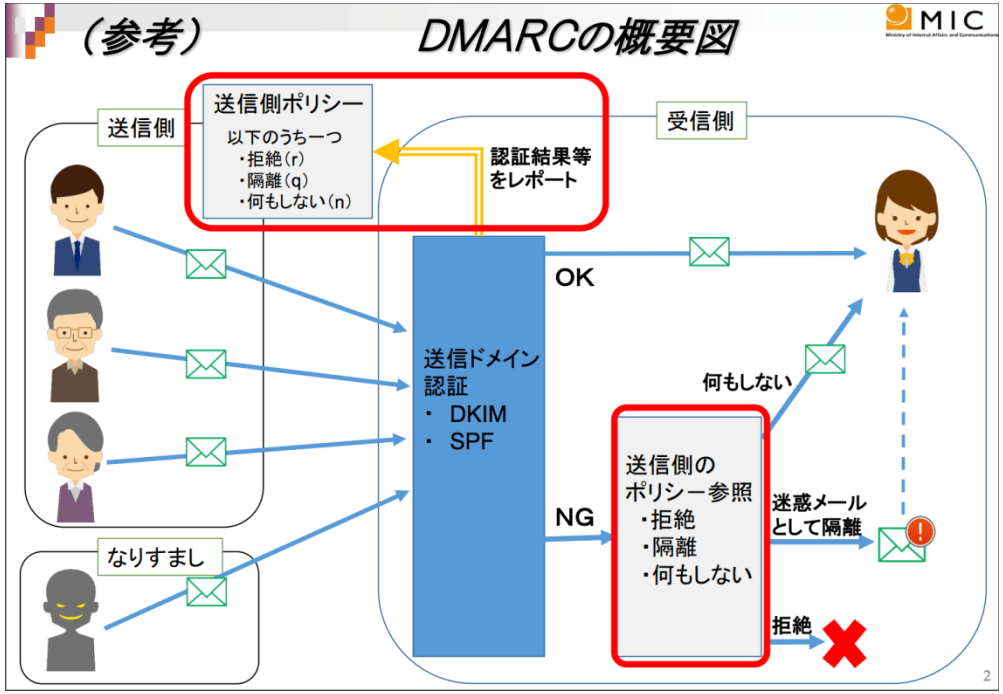
Send a message to the following services, where it will be evaluated according to several authentication systems. For message reflectors, send an email message from the domain you wish to check, and a report will be sent back.

- Message reflector: autoreply@dmarctest.org at dmarctest.org – DMARC reports sent every 5 minutes
- Message reflector: check-auth@verifier.port25.com by Port25 (instructions – DK, DKIM, Sender-ID, SPF)
- Message reflector: checkmyauth@auth.returnpath.net by Return Path (DK, DKIM, DMARC, Sender-ID, SPF)
- Message reflector: mailtest@unlocktheinbox.com by Unlock The Inbox (DK, DKIM, DMARC, Sender-ID, SPF)
- DMARC, DKIM and SPF Test System at NIST
- The Validator (of DKIM, DMARC and SPF – registration required) by Message Systems

https://dmarc.org/who-is-using-dmarc/
https://dmarc.org/resources/deployment-tools/#Record_Lookup

DMARC 対応に向けた環境

今年の7月に総務省による DMARC 導入に関する法的な留意点、**拒絶(r)**の実施方法が公表



なりすましメール対策として DMARC の普及・活用を目的として、迷惑メール対策推進協議会の議論を経て、公表

DMARC等の送信ドメイン認証技術の導入に関する法的整理

引用: http://www.soumu.go.jp/main_content/000495390.pdf

DMARC 対応した企業の事例紹介

小早志さんからご紹介

メール配信代行事業者の状況

Envelope-FromとHeader-Fromが別のドメイン

エラーメールをメール配信代行事業者がハンドリングすることにより、お客様が健全なメール配信を行うため

Envelope-From (RFC5321.From)

- メール配信代行事業者が管理するドメイン
  - SPIRAL : smp.ne.jp
  - Mail Publisher : bma.mpse.jp など

Header-From (RFC5322.From)

- 顧客企業/サービスが管理するドメイン

Cheetah Digitalの取り組み

1.顧客企業/サービスが管理するドメインへの対応

- DMARCポリシーは、rejectを推奨
  - なりすまし対策
  - ISP送信ガイド遵守
- 実際に設定されているポリシーはnoneが100%

2.メール配信代行事業者が管理するドメインの対応

- DMARCポリシーはrejectを設定
  - Header-Fromでは未使用（≒パークドメイン）
  - なりすまし対策
- 他のドメインも対応を計画中

1.顧客企業/サービスが管理するドメインへの対応

1. きっかけ

- 顧客からのDMARC公表方法の相談を受ける
- ポリシーをrejectにすることを目標とする

2. DMARCを公表

- ポリシーはnoneで公表

3. Aggregate Reportを分析

- 複数種のメール配信システム/Envelope-Fromを利用している

2.メール配信代行事業者が管理するドメインの対応

1. ドメイン利用用途の確認
2. ポリシーはnoneでDMARCを公表
3. Aggregate Reportの分析
4. ポリシーをquarantine（pct=100）に変更
5.ポリシーをreject（pct=100）に変更

企業が DMARC に対応するには？

3名で議論をしていきます

会場からの質疑

ありがとうございました