JAPAN ANTI-ABUSE WORKING GROUP

DMARCレポートについて

TwoFive,Inc.

Naoya Takahashi

目次

1. DMARCレポートとは
2. レポートが届く仕組み
3. 主要項目の読み方
4. レポート分析の具体例
5. DMARC Fail発生時の調査
6. 活用上の注意点
7. 日常運用への活用

1. DMARCレポートとは

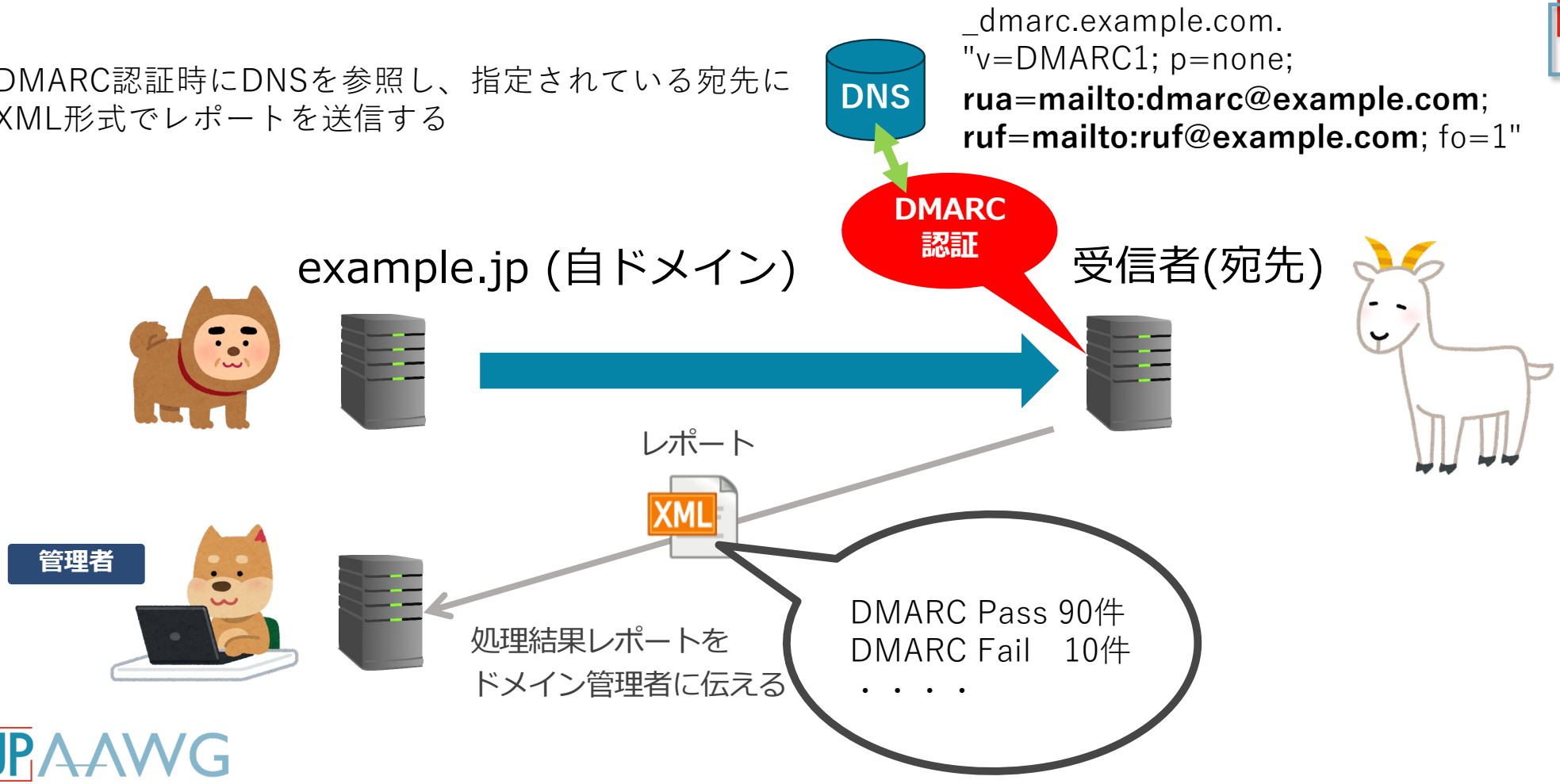
自社ドメインを名乗るメールの送信状況と認証結果を把握するためのレポート

- 主に確認できる情報
  - どのIPアドレスからメールが送信されたか
  - SPF・DKIMの認証結果はどうだったか
  - DMARC認証に成功したか、失敗したか
  - DMARCポリシーがどのように適用されたか
- 活用する目的
  - 正規のメール送信環境を把握する
  - 認証設定の不備を発見する
  - 自社ドメインを悪用したメール送信の兆候を把握する
  - DMARCポリシーの適切な運用につなげる
- RUAとRUFの2種類がある
  - RUA(集計レポート)：受信側で集計したレポート
  - RUF(失敗レポート)：1通毎の詳細が記載されたレポート



2. レポートが届く仕組み

DMARC認証時にDNSを参照し、指定されている宛先に
XML形式でレポートを送信する



2. レポートが届く仕組み

レポートのサンプル

```
▼<feedback>
 ▼<report_metadata>
    <org_name>Microsoft Corp.</org_name>
    <email>dmarcrep@microsoft.com</email>
    <report_id>86f7af79113f4a06bdc917004841f4eb@hotmail.com</report_id>
   ▼<date_range>
      <begin>1493175600</begin>
      <end>1493262000</end>
    </date_range>
  </report_metadata>
 ▼<policy_published>
    <domain>elephanet.com</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>none</p>
    <sp>none</sp>
    <pct>100</pct>
  </policy_published>
 ▼<record>
   ▼<row>
      <source_ip>121.119.191.248</source_ip>
      <count>1</count>
     ▼<policy_evaluated>
        <disposition>none</disposition>
        <dkim>fail</dkim>
        <spf>fail</spf>
      </policy_evaluated>
    </row>
```

JPAAWG

3. 主要項目の読み方

レポートに含まれる主要項目(RUA)

XML内の項目名	意味
org_name	レポートを生成した組織
date_range	集計対象期間
policy_published	レポート生成側が認識したDMARCポリシー設定
source_ip	メールの接続元IPアドレス
count	該当する条件に合致したメールの件数
policy_evaluated	DMARC評価結果と適用された処置
header_from	メールのFromドメイン
spf	SPFの認証結果
dkim	DKIMの認証結果

この他にもreason.comment等様々な項目が含まれますが、割愛します

4. レポート分析の具体例

送信元IP	件数	SPF	SPF アライメント	DKIM	DKIM アライメント	DMARC
192.0.2.10	1,000	Pass	OK	Pass	OK	Pass
192.0.2.20	200	Fail	-	Pass	OK	Pass
192.0.2.30	500	Fail	-	Fail	-	Fail
192.0.2.40	300	Pass	NG	Pass	NG	Fail



- 2.10：SPFでもDKIMでもDMARC Passしており、問題ない状況
- 2.20：SPFはFailしているがDKIMでDMARC Passしている。
  自社送信元でない場合は転送等の可能性。
- 2.30：SPF/DKIM共にFailしている為、DMARCもFailしている。
  自社送信元であれば最優先で対応する。
- 2.40：SPF,DKIM共にPassしているがアライメントが不一致でDMARC Failしている
  SaaSサービスのデフォルト設定等の可能性があり、自社契約の場合は設定を確認する。

5. DMARC Fail発見時の調査

1. 送信元の特定
   - 送信元IP、送信ドメイン、メール件数を確認する

2. 正規の送信元か確認
   - 自社設備、クラウド、メール配信サービス、委託先などを判断
   - セキュリティチェックリスト等も活用する

3. 原因を切り分ける
   - SPFの設定、DKIM署名、Fromドメインとのアライメント、転送などを確認

4. 対応と継続監視を行う
   - 正規メールなら設定を修正
   - 不正な送信が疑われる場合はセキュリティ調査を進める
   (ポリシー強化で迷惑メール扱いや届かなくすることは可能)

6. 活用上の注意点

注意点	ポイント
Fail＝攻撃とは限らない	正規メールの設定不備や転送などでも発生する
Pass＝安全とは限らない	正規に認証された攻撃メールなども存在する (攻撃者が保有しているドメインにDMARC設定している場合やDKIM Replay Attack等)
レポートにない＝送信されていない、とは限らない	• 受信側のレポート対応状況や集計範囲に依存する • レポート非対応の受信者も存在する
個別メールの内容は分からない	集計レポートはメール単位の本文や詳細なヘッダーを提供するものではない
件数だけでは判断できない	大量送信でも正規の場合があり、少量でも不正な場合がある
RUFは殆ど流通していない	個人情報が含まれる為、殆どの受信者はRUFレポートを送信しない

7. 日常運用への活用

DMARCレポートは、一度確認して終わりではなく、継続的に分析することが重要

- 定期的にレポートを確認する
- 正規の送信元IPやサービスを整理し、把握していない送信元を調査する
- DMARC Failの件数・割合・送信元の変化を監視する
- 正規メールの認証失敗を解消する
- 認証状況を踏まえ、DMARCポリシーの適用を段階的に検討する
- 業務負荷が高い場合は外部分析支援サービスを利用する



7. 日常運用への活用

DMARCレポートは、一度確認して終わりではなく、継続的に分析することが重要

- 定期的にレポートを確認する
- 正規の送信元IPやサービスを整理し、把握していない送信元を調査する
- DMARC Failの件数・割合・送信元の変化を監視する
- 正規メールの認証失敗を解消する
- 認証状況を踏まえ、DMARCポリシーの適用を段階的に検討する
- 業務負荷が高い場合は外部分析支援サービスを利用する



Thank you

