最新フィッシング動向とDMARC運用のポイント

TwoFive　加瀬　正樹

なりすましメール対策 DMARC

- メールドメインの DNS の TXT レコード（_dmarc.example.com）に以下のような宣言をする

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

なりすましメール対策 DMARC

- メールドメインの DNS の TXT レコード（_dmarc.example.com）に以下のような宣言をする
- 差出人を偽装されたメールはポリシーに従った処理を指示できる

なりすましメール対策 DMARC

- メールドメインの DNS の TXT レコード（_dmarc.example.com）に以下のような宣言をする
- 差出人を偽装されたメールはポリシーに従った処理を指示できる
- 認証結果をメール受信側からレポート受信先へフィードバックがある

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

日本の企業ドメインでも
DMARC 対応は確実に増えている！

国内 EC サイトトップ30の DMARC ポリシー

- なりすましメールとして狙われやすいのは B2C サービス
- 2022年EC売上トップ30社のうち、19社（63.3 %）が DMARC 導入済み
- p=none のメールドメインは 73.7 %

https://netshop.impress.co.jp/node/10185
https://note.com/twofive/n/neb66d4122496

でも・・・

DMARC ポリシーが p=none

のままでいいのだろうか？

DMARC レポートを分析して

メール環境を改善して

ポリシーを変更するまでが大事

DMARC レポートとはどんなデータか？

- 1日分の認証結果
- あくまで統計情報
  - 個人特定する情報は含まず
  - メール本文は含まず
- XML 形式
  - DMARC 評価結果と処理結果
  - DKIM 認証結果とその詳細
  - SPF 認証結果とその詳細

```
<?xml version="1.0" encoding="utf-8"?>
<feedback>
  <report_metadata>
    <org_name>[redacted]</org_name>
    <email>reporting@dmarc25.jp</email>
    <extra_contact_info>https://[redacted]</extra_contact_info>
    <report_id>554dfa26d3acb90d45da90dc21ce7bd8</report_id>
    <date_range>
      <begin>1671580800</begin>
      <end>1671667199</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>twofive25.com</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>quarantine</p>
    <sp>quarantine</sp>
    <pct>100</pct>
  </policy_published>
  <record>
    <row>
      <source_ip>[redacted].234.226</source_ip>
      <count>1</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>pass</dkim>
        <spf>pass</spf>
```

DMARC レポートのどこに注目したらいいか？

- DMARC pass 率
  - 企業のコーポレートドメインの場合は、ARC pass も含めた方がよい
- DKIM pass 率
- 送信元（source_ip）のうち、自社管理サーバでの DMARC pass 率
  - できるならば、SPF でも DKIM でも pass が理想的
- 送信元（source_ip）のうち、SaaS サーバでの DMARC pass 率
  - 基本的には DKIM pass しか期待できない

- スパム発信元は除外
- メール転送専用サーバは除外

どのタイミングで DMARC ポリシーを変更？

- コントロールできる範囲で改善できたあとにポリシー変更
- 一定期間 DMARC pass 率が安定して高い水準を維持してから
  - サブドメイン・組織ドメインの関係性
  - B2B なのか B2C なのか

- 新規ドメインの場合は、取得した直後に p=reject にする
- すでに攻撃や被害確認されている場合は、ポリシー変更後に FP 分析

ポリシーを変更したらメールが届かなくなる？

- 大手クラウドメール（Google, MS365, etc）では救済されがち
- 大手メーリングリスト（Mailman, Groups.io, etc）では救済されがち
- DKIM 対応によってメール転送・再配信も救済されがち
  - メールの添付ファイルの加工を含むメールゲートウェイは注意が必要

- 国内ISPは認証のみ（ヘッダーに結果記載のみ）の場合が多い
- メールの到達性で重要なのは最初の宛先
- DMARC レポートを継続的に分析して、False Positive を潰す
- p=quarantine から p=reject へ段階的に変更していく

その他

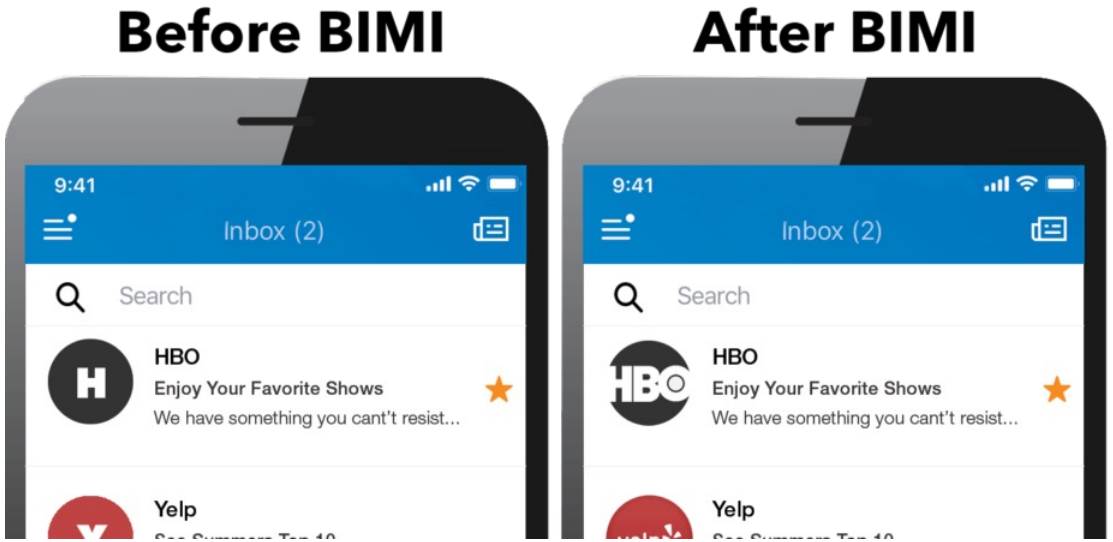
- ビジネス SaaS を選定するときには、DKIM 対応可能かどうか
- DNS ホスティングを選定するときには、DMARC / DKIM 対応可能かどうか
- **ブランドアイコンBIMI対応ドメインも増えている**

アイコン表示 BIMI（ビミ）

- DMARC ポリシーは p=quarantine 以上
  - 組織ドメインでも p=reject あるいは (p=quarantine かつ pct=100)
  - sp=none の場合は対象外

- アイコン画像は SVG フォーマット
  - スクリプトを含まない画像（ SVG Tiny PS ）

- VMC (Verified Mark Certificate) の発行
  - アイコン画像を証明するため
  - 商標登録チェックもある
  - Gmail や iPhone 標準アプリで表示させるためには必要



参考: https://bimigroup.org/

- アイコン画像、VMC証明書の場所をBIMIレコードで宣言

BIMI（ビミ） – 設定方法

- DNS の TXT レコード（default._bimi.example.jp）で宣言をする

v=BIMI1; l=https://example.jp/xxx.svg; a=https://example.jp/xxx.pem

バージョン

アイコンの URL

l=タグは
HTTPS サーバに配置

VMC の URL

a=タグは
HTTPS サーバに配置

BIMI（ビミ） – 設定方法

- DNS の TXT レコード（default._bimi.example.jp）で宣言をする
- タグによって必要なデータの場所を指定する

v=BIMI1; l=https://example.jp/xxx.svg; a=https://example.jp/xxx.pem

バージョン

アイコンの URL

l=タグは
HTTPS サーバに配置

VMC の URL

a=タグは
HTTPS サーバに配置

BIMI（ビミ） – 設定方法

- DNS の TXT レコード（default._bimi.example.jp）で宣言をする
- タグによって必要なデータの場所を指定する
- ロゴを出し分けるためにセレクターを指定可能（デフォルトは “default”）

v=BIMI1; l=https://example.jp/xxx.svg; a=https://example.jp/xxx.pem

バージョン

アイコンの URL

l=タグは
HTTPS サーバに配置

VMC の URL

a=タグは
HTTPS サーバに配置

ありがとうございました

フィッシングメール対策は TwoFive におまかせください

https://www.twofive25.com/

sales@twofive25.jp