楽天グループサービスにおける
メール送信ドメイン詐称、フィッシングメール対策

2022年11月7日

楽天グループ株式会社
執行役員
テクノロジーマネジメントディビジョン
情報セキュリティ・プライバシーガバナンス部
ジェネラルマネージャー　財津健次

Rakuten

Agenda

✓楽天グループ、楽天グループ株式会社紹介
✓楽天グループのなりすまし,偽楽天メール対策概況
✓DMARCレポートの利用
✓BIMIの実装状況と課題
✓まとめ

楽天グループ・楽天グループ株式会社

楽天グループコーポレートレポートから引用

MISSION ミッション

イノベーションを通じて、人々と社会をエンパワーメントする

楽天グループは、Eコマース、トラベル、デジタルコンテンツなどのインター ネットサービス、クレジットカードをはじめ、銀行、証券、電子マネー、スマホアプ リ決済といったフィンテックサービス、携帯キャリア事業などのモバイルサービスといった多岐にわたる分野で**70以上のサービスを提供**

▼

サービスに対応したドメイン、サブドメインから注文、発送等、各種お知らせのメールを送信

楽天グループのなりすまし,偽楽天メール対策概況

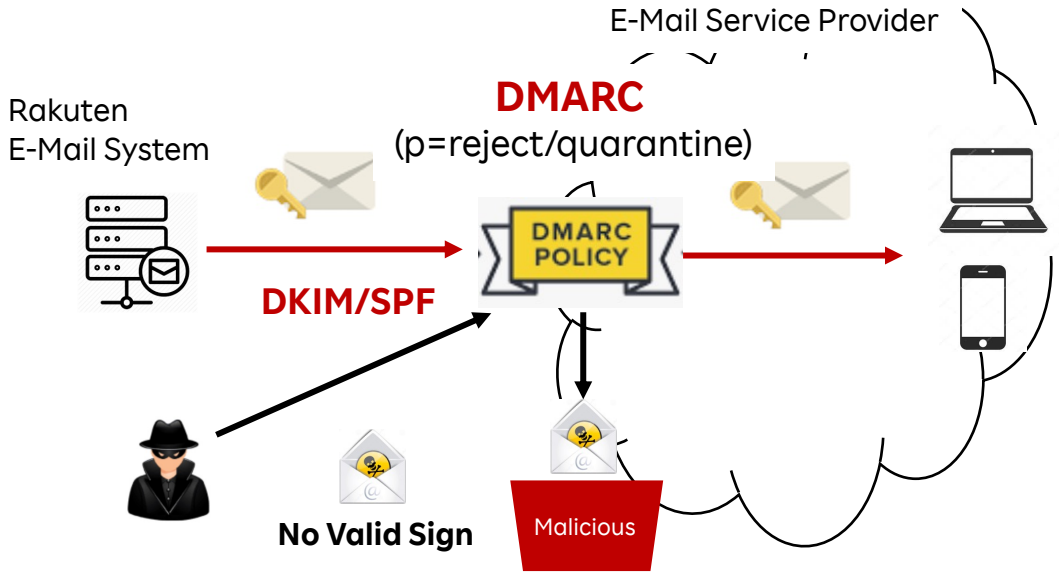
“なりすまし”、”偽”楽天メール対策の方法

① メール送信ドメイン詐称対策　= 楽天の正規ドメインを詐称して送付されるメールへの対策

② 中身がコピー、送信ドメインが似て異なる”look-alike”ドメインを利用したメールへの対策

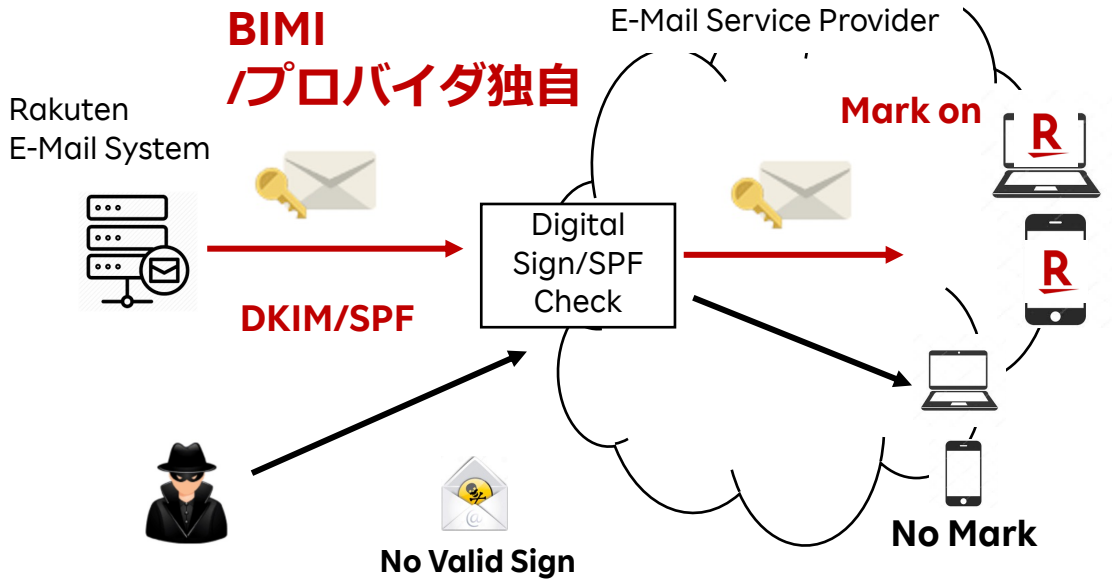
①“偽”楽天メールを受信側でフィルターする

送信側(楽天が利用するメール送信,ドメイン管理システム)にて、デジタル署名、宣言(DMARC)を行い、条件に合わないものはプロバイダ側でリジェクトないしは迷惑メールフォルダ等に移動する



②”真正”楽天メールにマークを付与する

楽天によってデジタル署名されたメールに、メールサービスプロバイダー側でマークをつけることで、利用者が本物の楽天メールを確認可能にする



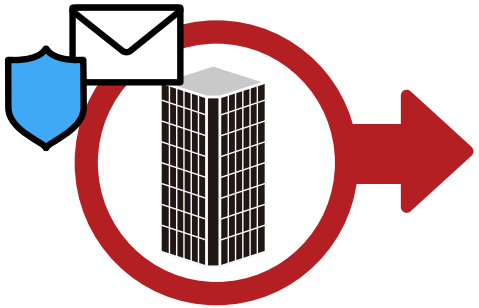
いずれの場合も、送信側（楽天サービス側)で送信ドメイン認証技術(DKIM,SPF,DMARC)の設定が必須

楽天グループおけるなりすまし、”偽メール対策実装状況

2018

楽天サービス・店舗様
を騙る偽楽天メールが
多数報告される

DKIM/DMARC

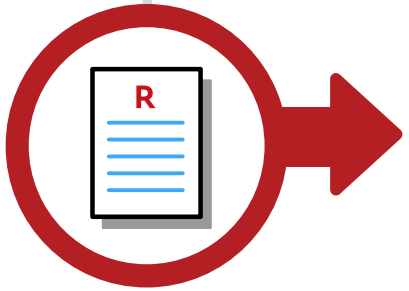


全社的に送信ドメイン認証技術
(DKIM/DMARC) 導入の推進開始

★

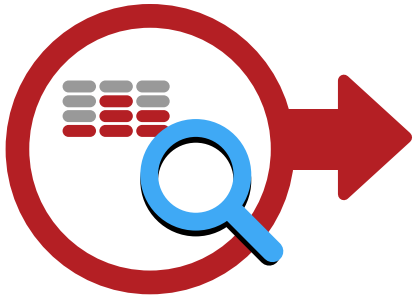
Yahoo！メール
ブランドアイコン機能に参加
2018年10月

2019



送信ドメイン認証設定
社内マニュアル制定

2020



DMARC分析ツール導入
（エクセルからの移行）

2021

★

ルートドメインへの
DMARC p=reject設定
(2021年8月)

フィッシング対策協議会報告
より楽天の名前が消える
(2021年8月分)

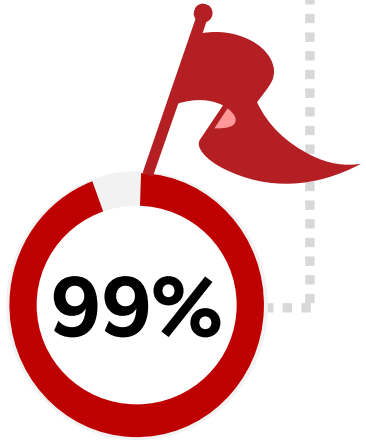
★

ドコモメール
公式アカウント機能に参加
2021年5月

BIMI実装開始
/日本国内
(2021年12月)

BIMI実装開始
/海外サービス
(2022年3月)

2022

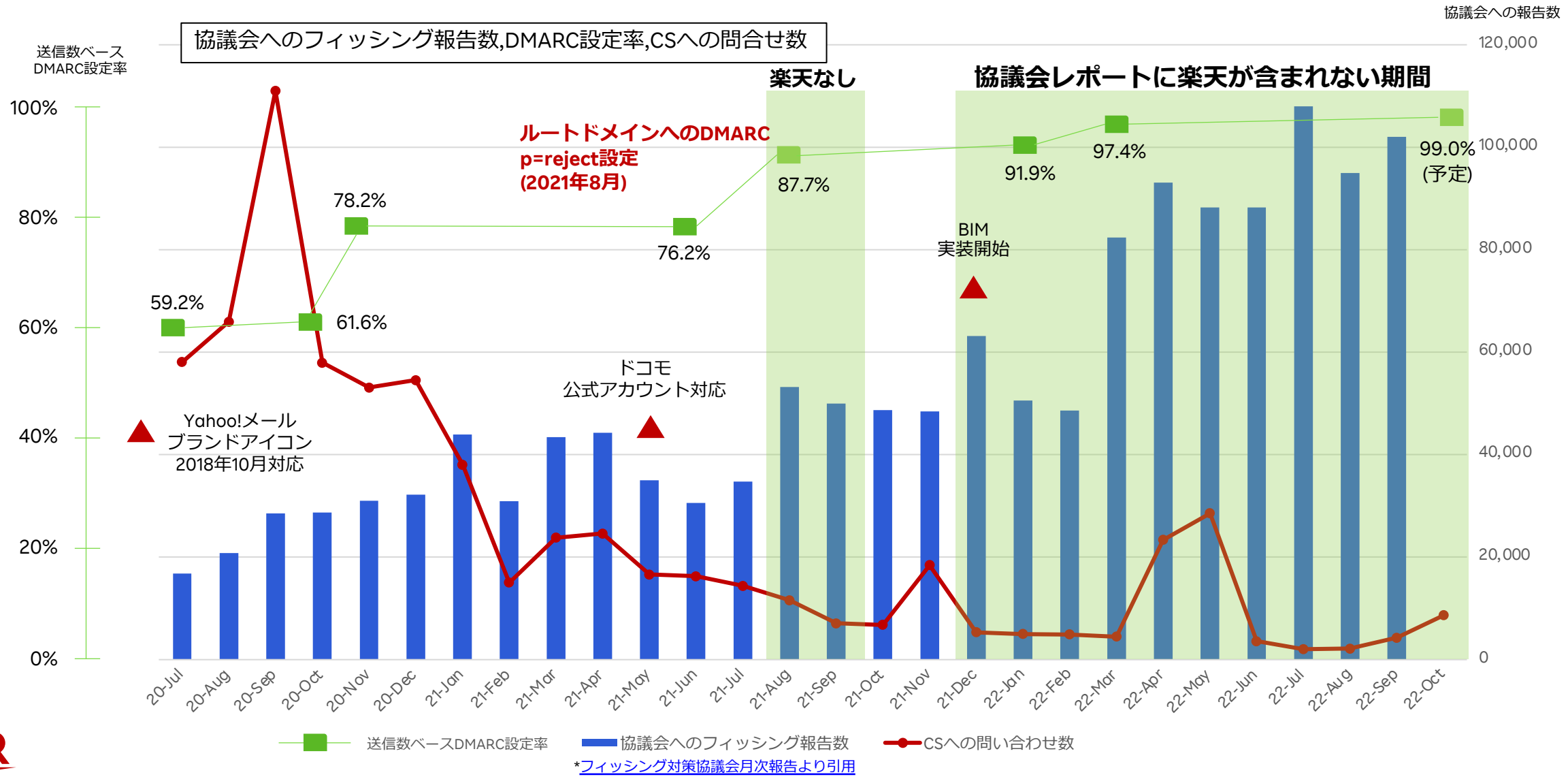


送信ドメイン認証技術
DMARC/BIMI導入率
99%を達成予定(グローバル送信数ベース

**2022年11月中旬

カスタマーサービスへの問い合わせ数の傾向と協議会への報告数の比較

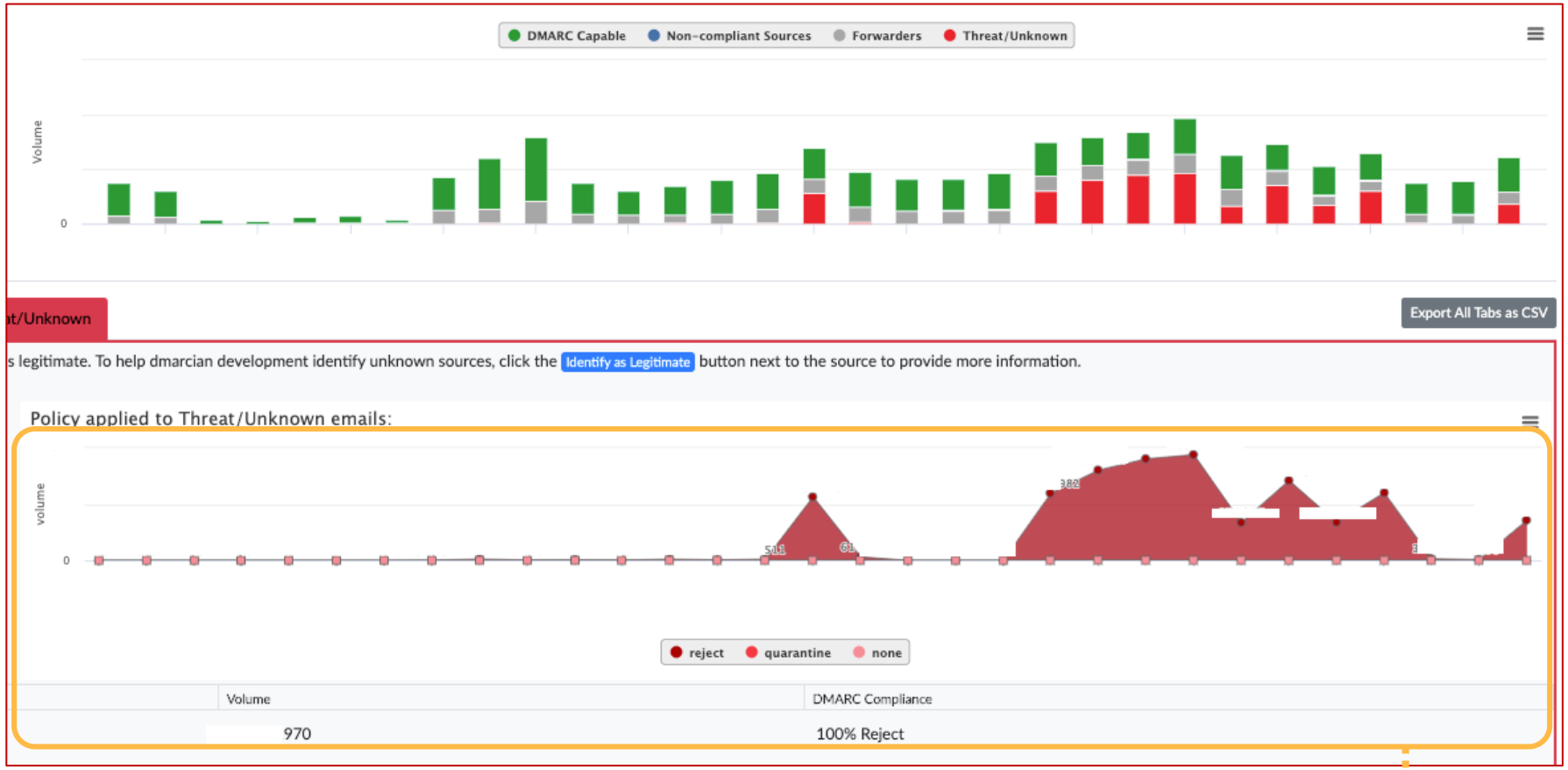
DMARC,ブランドアイコン表示が”一定レベル”のCS問い合わせ数の削減、もしくは”ターゲットブランド”になる機会の減少に寄与していると考えられる



*フィッシング対策協議会月次報告より引用

DMARCレポートの利用

DMARCレポートの徹底利用



** DMARCレポート
ツールサンプル画像

クロス
ファンクションチームの
優先順位の決定

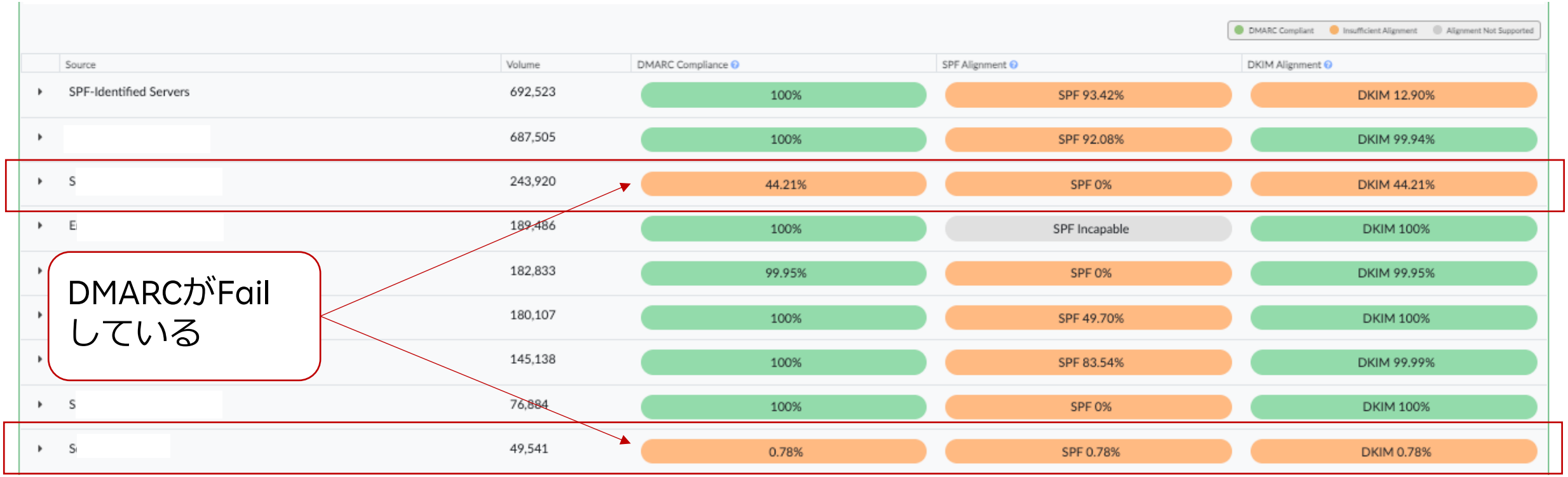
DMARCがFailしている
プラットフォームの特定、
影響状況の推測・掘り下げ

“Reject”メール数の把握
= 効果報告に有効

DMARCレポート例は講演のみ

DMARCがFailしている当該ドメイン利用プラットフォームの特定

DMARCレポートからDMARCがFailしているプラットフォームを特定し,当該プラットフォーム利用部門にDKIMの適正な設定を促す



BIMI の 実装状況と課題

BIMI (Brand Indicators for Message Identification) 利用条件概要

- ✓ DMARC(p=reject/quarantine)実装時 に利用可能となる
- ✓ VMCの購入,DNSへのBIMIレコードの設定が必要
- ✓ 表示するブランドアイコンには登録商標が必要(VMC購入時に確認される)

Email Body

Inbox View

クライアント側条件

1. Gmail クライアント
   - ✓ iOS
   - ✓ Android
2. iOS16 Apple iCloud メール
3. ブラウザ

*サムネールでのアイコン表示なし

対応メールサービス

Gmail,Yahoo.com,Apple他
*bimigroup.org参照

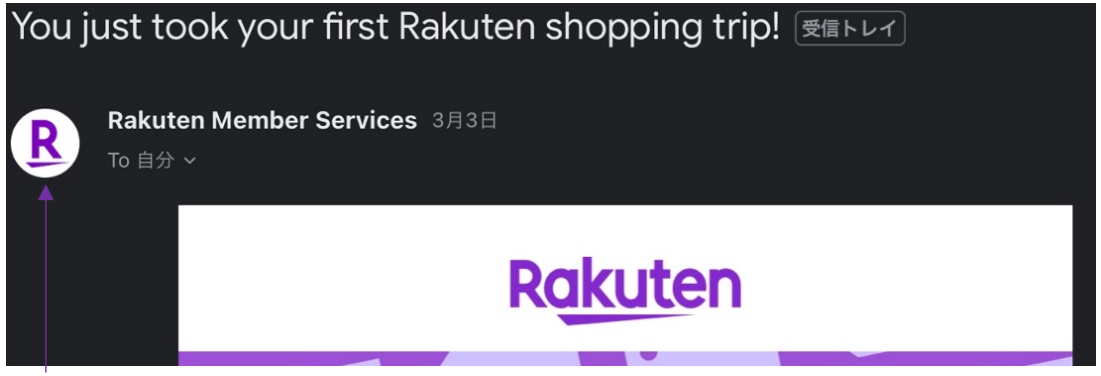
グローバル楽天サービスで主要サービスにBIMI実装済み

- ✓ 日本むけサービスは、2021年12月から実装開始
- ✓ 海外サービスは2022年3月から実装開始
- ✓ グローバル楽天サービスで90%以上の実装

** BIMI : Brand Indicators for Message Identification

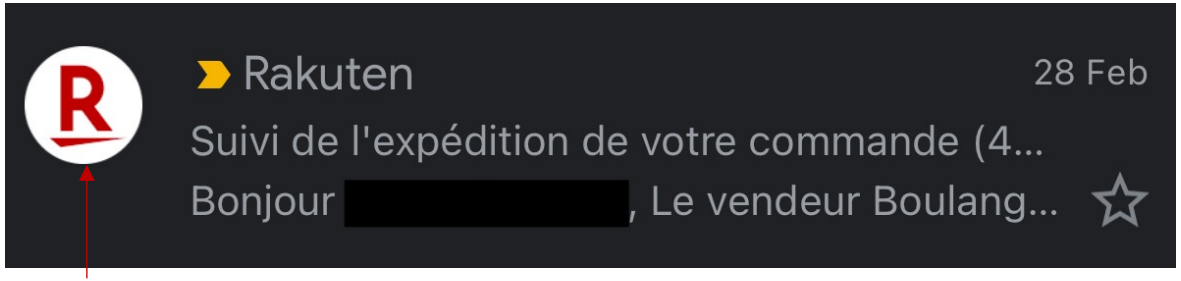
BIMI – 海外サービスでの Gmail/Yahoo.com表示対応(2022年3月対応済)

Rakuten Rewards / USA



ブランドアイコン

楽天フランス / Rakuten France

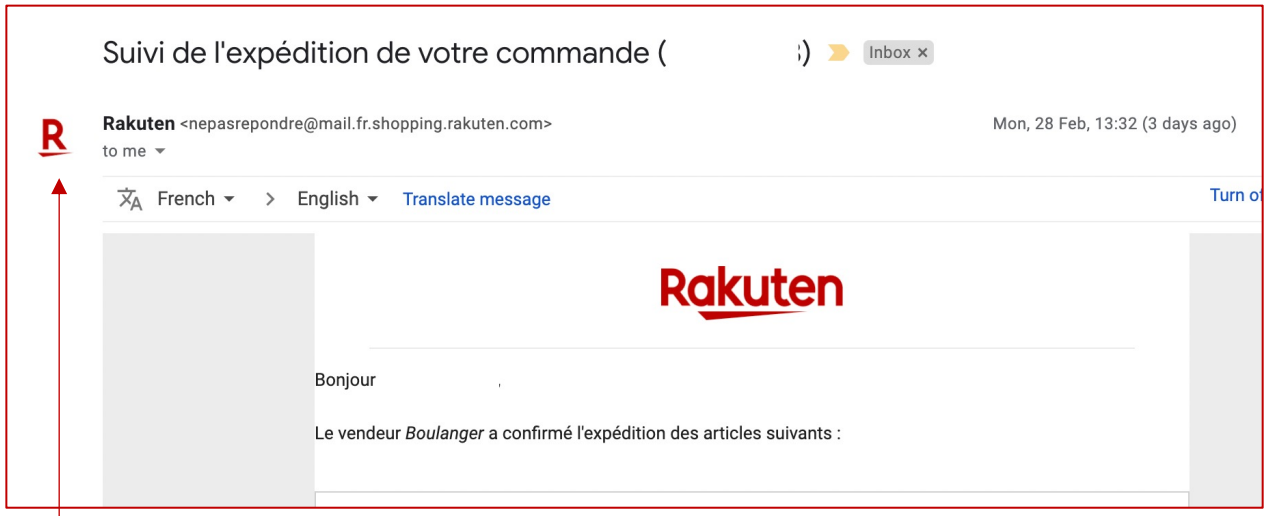


ブランドアイコン

台湾楽天市場

ブランドアイコン

楽天フランス / Rakuten France



ブランドアイコン

Apple Mail (@iclould.com) iOS 16 でのBIMI画面イメージ

ブランド
アイコン

クリック

クリック

クリック

ブランド
アイコン

***同じメールを iOS15 で表示した場合

**サムネールでのブランドアイコン表示はない

BIMI実装課題

1. 良いところ
   - ✓ Gmail,Yahoo.com,Appleが対応しているので、グローバル展開が容易

2. チャレンジ
   - ✓ VMC(Verified Mark Certificate)購入,維持の予算,人員確保が必要
   - ✓ プラットフォームで見え方が少しづつ違う
   - ✓ サービスによっては、BIMIで使いたいアイコンが商標登録されてない場合がある
   - ✓ DMARC p=reject / quarantine にまで持っていく必要がある

まとめ

まとめ

1. 2022年はDMARCをサポートするメールサービスプロバイダの増加、楽天グループでのBIMI実装と大きく進展があった

2. 2023年は課題となっている残り数パーセントのサービスへの実装も行い、楽天グループ全体のサービスの信頼性を高めたい

3. インターネットサービスをご利用のユーザ様へのよりわかりやすいお知らせを行うことで、なりすまし、偽メール対策の有効性を高める必要があると考えている


Rakuten