

私たちの失敗から学ぶ、 なりすましメール対策の挑戦記

BIGLOBE BIMI/DMARC対応編

2025年11月4日

ビッグロース株式会社

好きが、未来を変えていく。

桑原 隆造(くわはらりゅうぞう)

所属

全社横断 サービス企画部

担当業務

- ・オプションサービスの企画/運営
 - ・デバイスのセキュリティソフト
 - ・端末保証サービス
 - ・BIGLOBEメール
- など

DMARCポリシー強化を担当

松井 海友(まついみゆう)

所属

全社横断 経営企画部

担当業務

- ・会員向けマーケティング
- ・お客さま向けメール管理

BIMI推進を担当

本日参加できないため
桑原が代理発表します



加藤 理人(かとうりひと)

所属

プロダクト技術本部 アジャイル開発部

担当業務

- ・社内で「(自称)メールに詳しい人」
- ・社内で「(自称)SPFレコードの元締め」
- ・会員からのメールに関する問い合わせの調査
- ・一般財団法人インターネット協会 迷惑メール対策委員会メンバー
- ・迷惑メール対策推進協議会 技術WGメンバー

技術支援・DMARCレポート分析を担当

初めての + 高知 × (県 + 市)

BIGLOBEの会社概要

BIGLOBEは来年で通信事業40周年
光回線やMVNOなどインターネット事業を中心に拡大

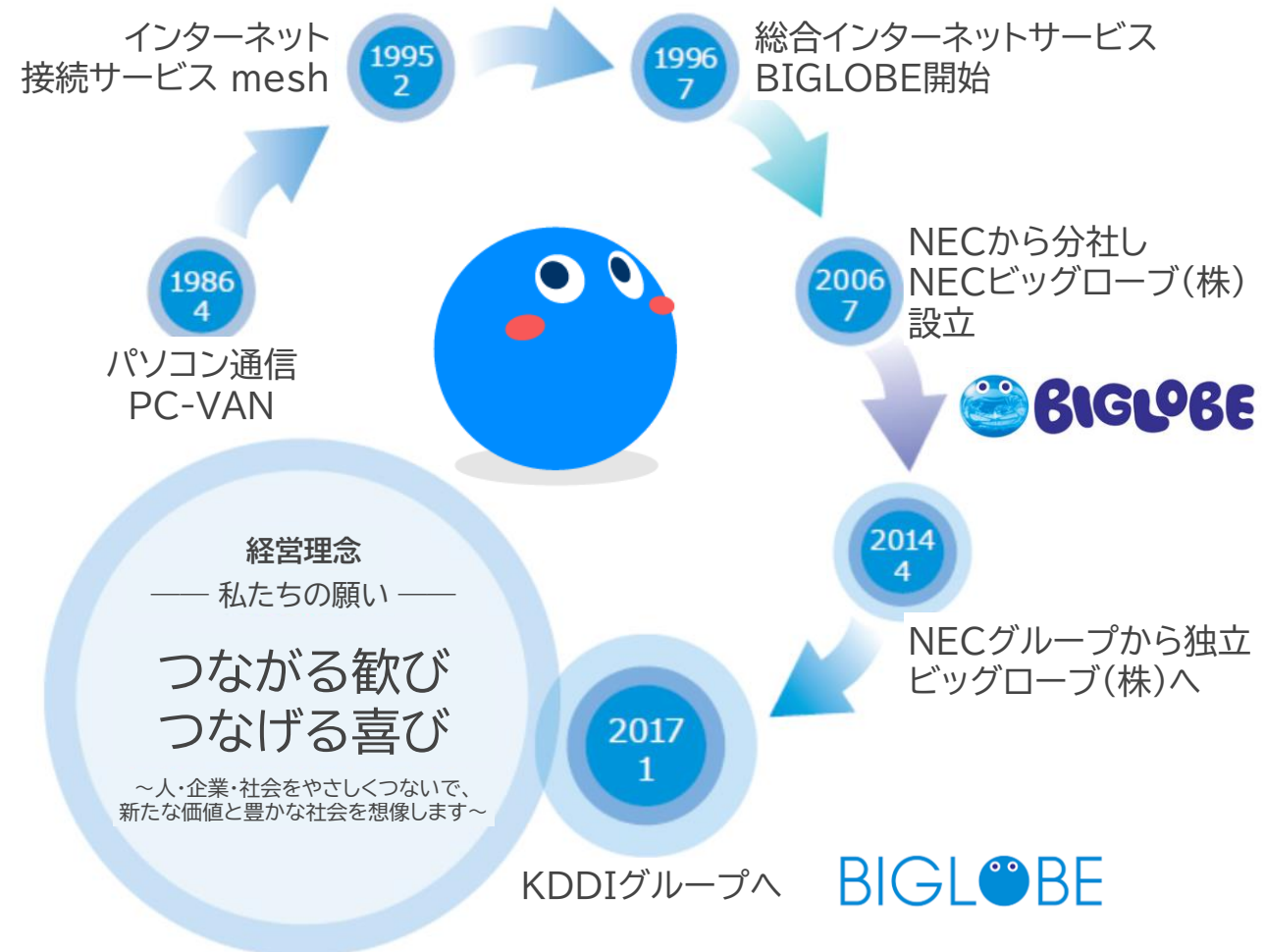
BIGLOBE光

BIGLOBE mobile

接続サービス関連の様々なサービスを提供

- ・セキュリティ
- ・機器保証
- ・メール

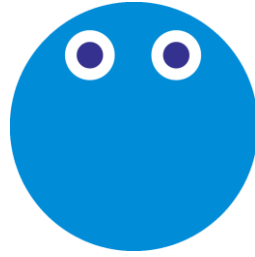
など



2025年7月16日にブランドリニューアルしました

旧ロゴ

BIGLOBE



新ロゴとスローガン

好きが、未来を変えていく。

BIGLOBE



「びっぷる」です！



1. BIMI導入に向けて

- ・思っていたよりも大変でした・・・

2. DMARC対応について

- ・DMARCポリシーを「quarantine」に設定した理由
- ・DMARCレポートの解析について

【はじめに】 BIGLOBEメールについて

BIGLOBE会員なら、BIGLOBEメールとして使えるメルアドが1つ発行

Webメール (***@***.biglobe.ne.jp)

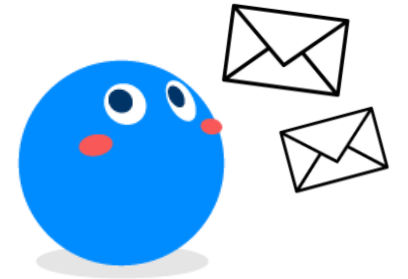
> 迷惑メールフォルダオプション

> お好みアドレス
サブドメインを自由に選択可

特定キーワード : cat、baseball、zoo などの**400種類以上** ([好きな文字列]@***.biglobe.ne.jp)

地名ワード : kouchi、tokyo、oita などの全国**300種類以上** ([好きな文字列]@***.eeyo.ne.jp)

など



1. BIMI導入に向けて

- ・思っていたよりも大変でした・・・

2. DMARC対応について

- ・DMARCポリシーを「quarantine」に設定した理由
- ・DMARCレポートの解析について

BIMI導入の背景～こんなにかかることになるとは…～

2024年11月ごろ、「1か月くらいで対応完了？」と始めたBIMI対応
実際に検討を進めたところ、3大「大変」が発覚…

BIMI導入で必要なこと

1. BIMI導入するドメインの
DMARCポリシー強化

適用したいドメインは
1個だけだから簡単！
「bcs.biglobe.ne.jp」

大変①

〇〇〇**個超**も
対応が必要！？

2. BIMIアイコンの申請



「びっぷる」アイコンは
商標登録済みだから
すぐに申請できる！

大変②

〇〇で
時間がかかりました…

3. VMCの申請
(認証マーク証明書)

Web申請だけかな？

大変③

担当者の〇〇の**提出**も
必要なの…！？

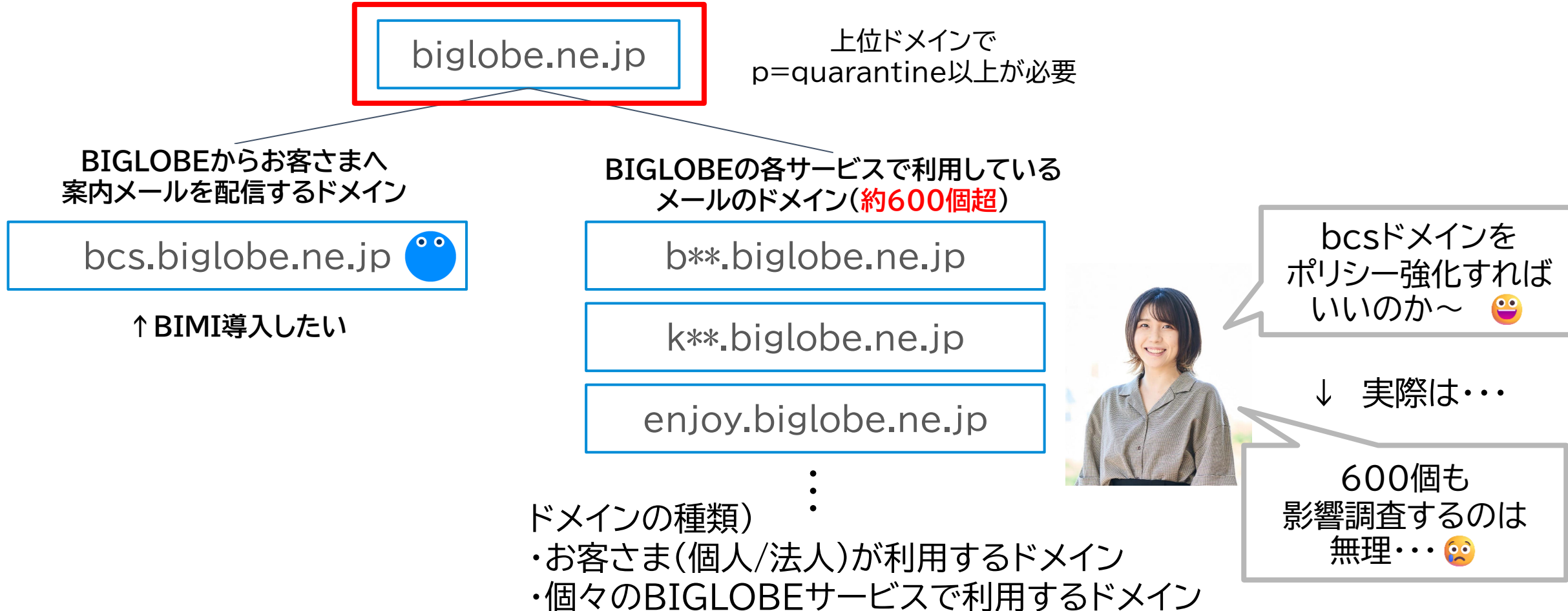
4. BIMI用のDNSレコード設定

DNSに2行追加するだけでした
・ドメイン所有者であることを証明するレコード
biglobe.ne.jp _dnsauth IN TXT "o8jhfg1bmoumvp1cs4g0x3ln2lbjav"
・BIMI表示のためのレコード (対応中)

5. DMARCレポートの解析

大変① 思っていたようにいかなかったポリシー強化

BIMI導入をしたい「bcs.biglobe.ne.jp」のみでポリシー強化が必要と思っていたが、実際には上位ドメイン「biglobe.ne.jp」でポリシー強化が必要なが判明



大変② 思ったよりも時間がかかったBIMIアイコンの申請

BIMIアイコン審査が厳格でいくつか想定外のことが...



BIMIアイコン審査の想定外

Q.

旧ロゴのデザインとほぼ一緒だから、
旧ロゴの商標をそのまま使えるのでは？



A. 

少し色味が違うだけでもNG
(並べて見なきゃわからないのに...)

旧ロゴ



Q.

すぐ商標申請したら、すぐ対応できるはず



A. 

社外に出すのは新ロゴが一般公開されて以
降になるので、一般公開までは動けない

Q.

商標登録は1カ月くらいで完了する？



A. 

最低でも数カ月かかる
通常審査で10カ月、早期審査でも2～3カ月

大変③ アイコンよりも厳密に確認される担当者の身元

当日投影限り
撮影禁止

BIMI導入に必要不可欠なVMCを取得するためには、
「組織確認」に加えて、「担当者(松井)の身元証明」も必要

私の存在を証明する
ためにWeb面談

当時の再現

ぼかし背景NGなどいろい
ろルールがありました

顔写真付き証明書の
実物確認で「後ろに手を」
と言われました

1. BIMI導入に向けて

- ・思っていたよりも大変でした・・・

2. DMARC対応について

- ・DMARCポリシーを「quarantine」に設定した理由
- ・DMARCレポートの解析について

DMARCポリシーを「quarantine」に設定した理由

理由

p=reject の影響調査は不可能と判断したため

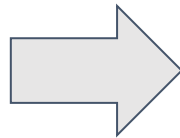
600超ドメイン

異なるサービス特性
(個人、法人、社内)

複数のメール配信システム

など

従来
none
何もしない



今回の変更
quarantine
隔離

将来的には...
reject ?
拒否

まずは「quarantine」に設定し、DMARCレポートを定期的に分析しながら
認証失敗のメールドメインを是正していく方針としました

DMARCポリシー強化で大変だったこと

- **社内への説明**
DMARCやBIMIの学習・理解からスタート
本対応がなぜ必要なのかを丁寧に説明
 - ・フィッシング詐欺対策の強化
 - ・ブランドの信頼性向上
- **ドメイン、メール配信システムへの影響調査**
長年のサービス提供によりドメイン・
メール配信システムの管理担当が不明瞭/不在
- **お客さまへの周知内容を決めること**
どういうお客さま体験になるかを重要視し、
技術的な視点も考慮しつつ、案内文を作成

「サポートページ・メール・プレスリリース」
複数手段でお客さまへ周知

対策の概要

メールの送信元が正規のBIGLOBEであるかを確認する仕組み（DMARCポリシー）を、より強固な設定に変更します。

本対策により、BIGLOBEを騙ったなりすましメール（フィッシングメールなど）が迷惑メールとして判定される可能性が高くなります。

※ご利用のメールサービスによっては、迷惑メールフォルダに自動で振り分けられるようになります。

DMARCポリシー

変更前	変更後
none（監視のみ）	quarantine（隔離）

お客さまや社内からの大きな反響は特になく、対応完了できました

DMARCレポートについて(1/5)

1. サブドメイン数「数百」の地道な調査とその壁
調査は非常に手間がかかりました

課題

攻撃対象の「数百のサブドメイン」を一つひとつ分析
DMARCレポート解析サービスに助けられました

最大の壁

なりすまし疑いメールが社外システム（クラウドサービスなど）から送信
されているケース

自社のシステムログだけでは追跡が不可能、調査が暗礁に乗り上げた

2. 社外システム送信の突破口：「お金の流れ」からのアプローチ 解決策：経理部門との連携

経理部門に協力してもらい、「お金の流れ」（サービス利用料の支払い記録など）から、その社外システムがどの部門で、何の目的で利用されているかをたどってみた

方針： **お金の流れがなければ深追いしない**

3. ヘッダ情報の壁とDMARC解析の課題

問題: 多くのメールシステムでは、なりすまし判定の鍵となる **ヘッダFromの情報がログに記録されていない** ことが多く、DMARCレポートのデータと突き合わせができないケースがある

【急募】 皆様はどうやって解析しているのでしょうか？

4. 社外システム管理者へ問い合わせ

現状: 返事を返してくれない管理者が多いです、対応に苦慮する覚悟を！

奇跡の返信：SBI証券さんは、迅速にご返信・ご協力いただけました
メール返信にてお礼を申し上げましたが、この場でもお礼申し上げます

5. たどり着いた境地：潔く「放置する勇気」

現実: 社外システム（海外サービスなど）が関係する場合、**どれだけ調べても特定できない、あるいは対応してもらえないことがあります**

結論: 「わからないものは放置する勇気」も、限られたリソースの中で調査を進めるためには必要です。放置する基準を設ければ更に良いですね

- ・ DMARCレポート解析にゴールはありません、継続することが重要
- ・ ドメインを守るために皆さんがんばろう！

1. 推進役は理解度をまず上げることが大切
2. 自社特有のタスク整理が重要
3. DMARCポリシー強化して終了ではなく、継続的な監視体制を構築
4. 「quarantineに満足することなかれ！」
DMARCレポートで問題なさそうなのでReject化へ進みます
5. 積極的なアウトプットが他社さんを助けます！

好きが、未来を変えていく。



BIGLOBE