JP AAWG Japan Anti-Abuse Working Group

JANOG54 Meeting in NARA

Gメールショック！
メールインフラを安心・安全に変える(た)、
にわとりたまご問題の結論とは。

時間配分（４５分）

・北崎 恵凡　５分
　ソフトバンク株式会社、JPAAWG運営委員
・熊沢 明生　８分
　ソフトバンク株式会社
・中島 直規　８分
　KDDI株式会社
・正見 健一朗　８分
　株式会社NTTドコモ
・質疑応答/パネルディスカッション　１０分

Gメールショックとは

・2023年10月にアナウンスされたGoogleと米国Yahoo!メールで実施する**迷惑メール対策強化**

・主な要点

- 送信ドメイン認証 (SPF、DKIM、DMARC) の設定が必要
- 一日5,000通のメールを送信するメール送信者はより厳しい送信ドメイン認証の設定が求められる
- 一斉メール送信する場合は、購読解除機能の実装が必要
- 受信ユーザーが求めないメールは送信しないこと (Complaints rate 0.3%未満)

・影響度の大きさから実施時期を延期

- 送信ドメイン認証の適用 (2024年2月→4月)
- 迷惑メール率による受信拒否 (2024年6月～開始)

JPAAWG

Googleは段階的に規制を実施

	Step1 2024年 2月	Step2 2024年 4月	Step3 2024年 6月
Gmail	一部へ**テンポラリーエラー**を応答	一定の割合で**リジェクト**応答	ガイドラインを満たしていない**ドメインへリジェクト応答**

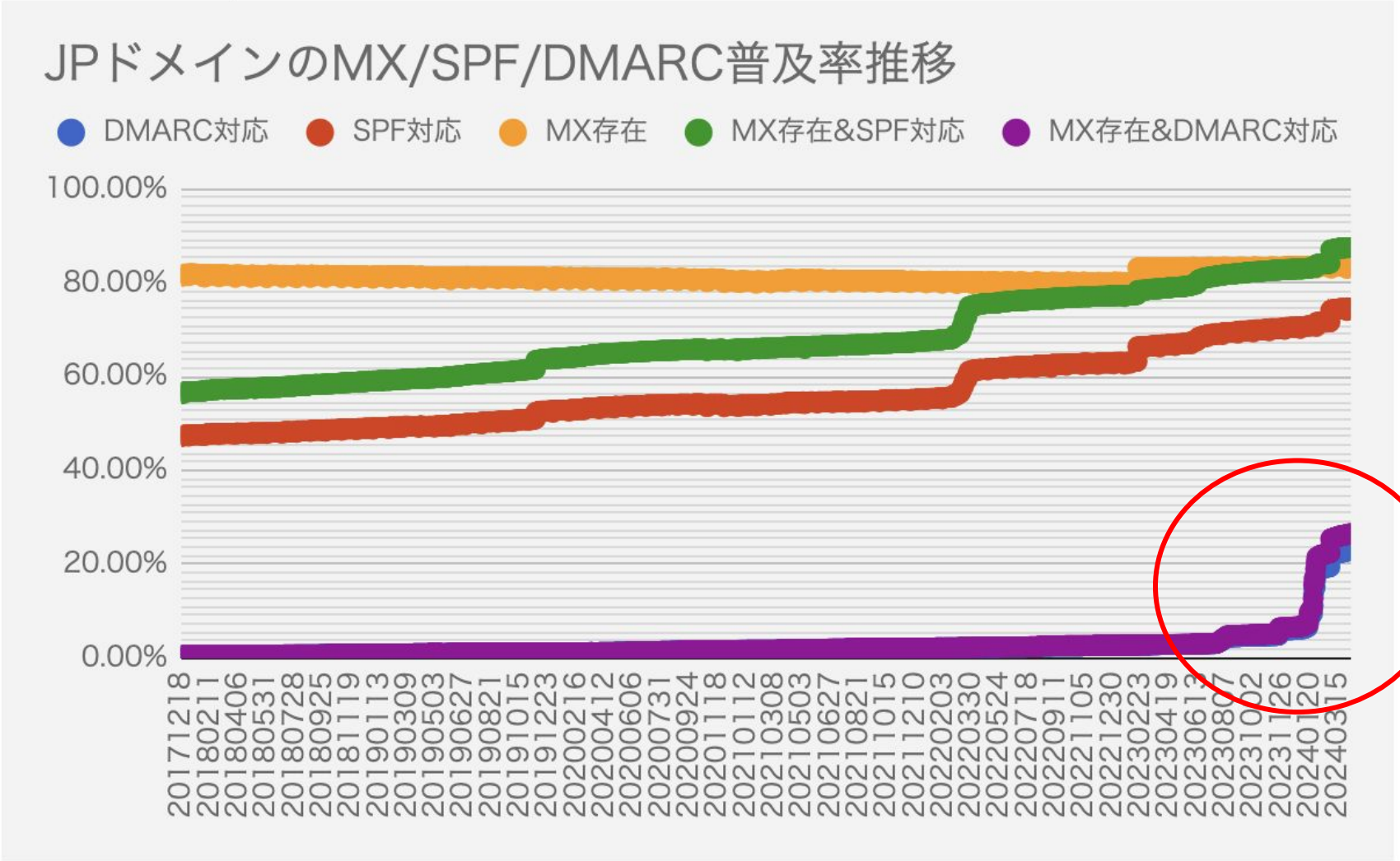
	Step1 2024年 2月
Yahoo!(米国)	現時点で掲載無し

対応が遅れているケース

一般情報（口頭のみ）

2024.4.1 どうなったか (Before & After)

DMARC adoption statistics of JP domains



2024.6.1 どうなったか (Before & After)

各社の状況（口頭のみ）

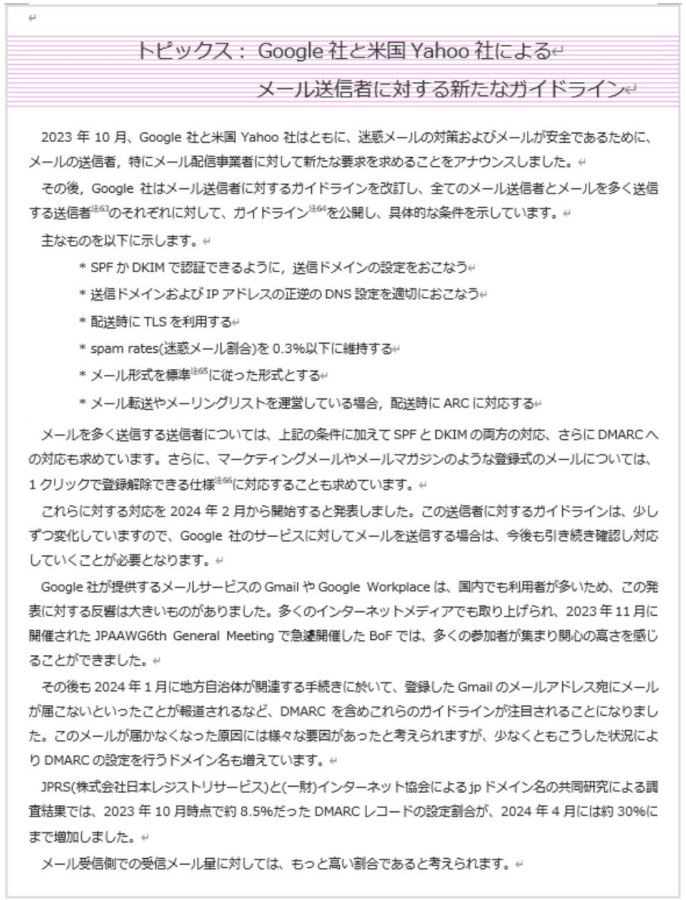
いまのところ大きな影響なし？

本質的な課題
(この先、求められていること)

・メール本文の検閲 (通信の秘密との関係性整理)
・フィルタリング (包括同意でもオプトアウトによる無力化対策)
・ドキュメント、ガイドライン、技術標準の改定

・黒船来航は良かった？悪かった？
・迷惑メールを減らす (送らせない)

建設的なアプローチ①
迷惑メール白書2022-2024 （８月公開予定）



トピックス： Google 社と米国 Yahoo 社による
メール送信者に対する新たなガイドライン

2023 年 10 月、Google 社と米国 Yahoo 社はともに、迷惑メールの対策およびメールが安全であるために、メールの送信者，特にメール配信事業者に対して新たな要求を求めることをアナウンスしました。

その後，Google 社はメール送信者に対するガイドラインを改訂し、全てのメール送信者とメールを多く送信する送信者[注63]のそれぞれに対して、ガイドライン[注64]を公開し、具体的な条件を示しています。

主なものを以下に示します。

* SPF か DKIM で認証できるように，送信ドメインの設定をおこなう
* 送信ドメインおよび IP アドレスの正逆の DNS 設定を適切におこなう
* 配送時に TLS を利用する
* spam rates(迷惑メール割合)を 0.3%以下に維持する
* メール形式を標準[注65]に従った形式とする
* メール転送やメーリングリストを運営している場合，配送時に ARC に対応する

メールを多く送信する送信者については、上記の条件に加えて SPF と DKIM の両方の対応、さらに DMARC への対応も求めています。さらに、マーケティングメールやメールマガジンのような登録式のメールについては、1 クリックで登録解除できる仕様[注66]に対応することも求めています。

これらに対する対応を 2024 年 2 月から開始すると発表しました。この送信者に対するガイドラインは、少しずつ変化していますので、Google 社のサービスに対してメールを送信する場合は、今後も引き続き確認し対応していくことが必要となります。

Google 社が提供するメールサービスの Gmail や Google Workplace は、国内でも利用者が多いため、この発表に対する反響は大きいものがありました。多くのインターネットメディアでも取り上げられ、2023 年 11 月に開催された JPAAWG6th General Meeting で急遽開催した BoF では、多くの参加者が集まり関心の高さを感じることができました。

その後も 2024 年 1 月に地方自治体が関連する手続きに於いて、登録した Gmail のメールアドレス宛にメールが届こないといったことが報道されるなど、DMARC を含めこれらのガイドラインが注目されることになりました。このメールが届かなくなった原因には様々な要因があったと考えられますが、少なくともこうした状況により DMARC の設定を行うドメイン名も増えています。

JPRS(株式会社日本レジストリサービス)と(一財)インターネット協会による jp ドメイン名の共同研究による調査結果では、2023 年 10 月時点で約 8.5%だった DMARC レコードの設定割合が、2024 年 4 月には約 30%にまで増加しました。

メール受信側での受信メール量に対しては、もっと高い割合であると考えられます。

トピックス：BIMI (ブランドロゴの表示)

メール受信側では、送信ドメイン認証技術によって認証した結果をメールヘッダーに記載することになっています。しかしながらメール利用者が用いるメールクライアントの多くは、これら認証結果を含むヘッダーや結果自体を標準で表示することはほとんどありませんし、参照した場合でも直感的にわかりやすい形式とは言い難い部分があります。そのため送信ドメイン認証技術が普及した場合でも、メール受信者がなりすましメールであるか、正規のメールであるかを判断することは簡単ではありませんでした。

そこで、日本では幾つかのメールサービス事業者が独自に送信ドメイン認証技術を用いて、受信メールクライアント上でイメージ表示する機能を提供し、視覚的にメール送信者を判断しやすくする仕組みを提供しています。グローバルでは、2021 年に Brand Indicator（いわゆるブランドロゴ）を表示させるための仕様が、IETF(Internet Engineering Task Force)に提出され、現在議論が進んでいます。

これが BIMI [注67] (Brand Indicators for Message Identification)です。

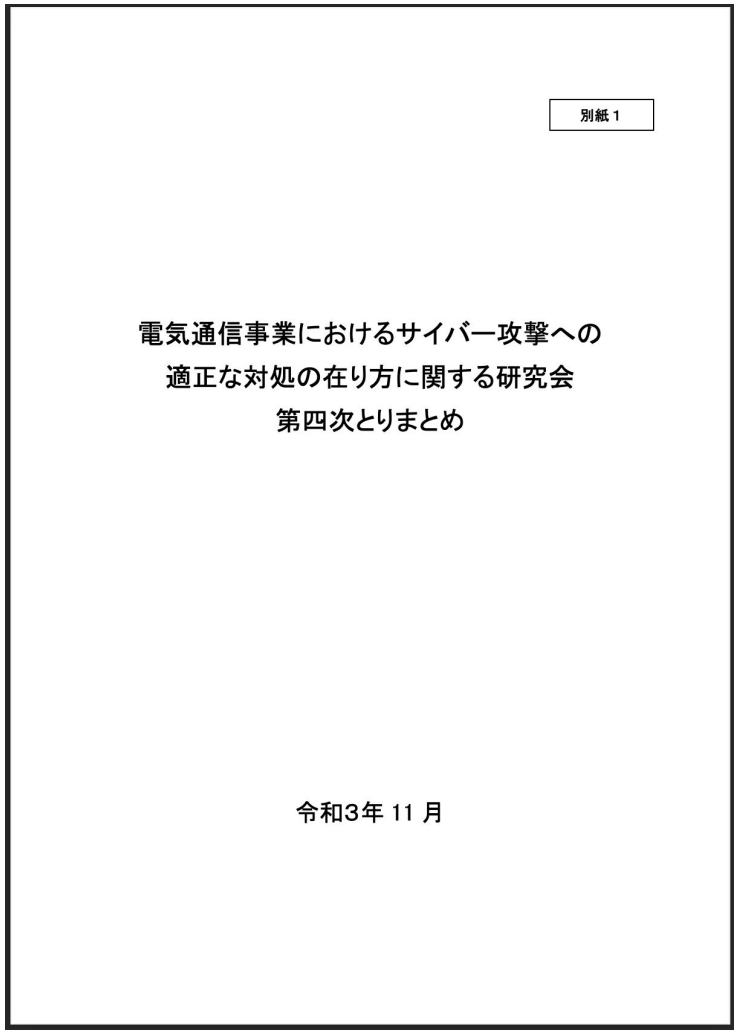
BIMI では、送信ドメイン認証技術で認証されたドメイン名を対象に、DMARC のポリシーが quarantine あるいは reject であった場合、BIMI レコードの参照を試みます。BIMI レコードが存在する場合、BIMI レコードに示された BrandIndicator(ロゴ)の存在場所を示す URI から、ロゴ情報を取得します。これをメールクライアントで適切に表示することになります。

ロゴの情報は URI で示されますので、その場所がわかってしまえば同じデータを取得して、あたかも自分のロゴであるかのように別のドメイン名を用いて、ロゴをなりすますこともできてしまいます。こうしたなりすましを防ぐために、VMC(Verified Mark Certificate)の仕組みも提案されています。簡単に言えば、認証局が発行した証明書を検証することで、なりすましを防ぐ仕組みです。

BIMI はまだ IETF で正式な仕様にはなっていませんが、DMARC もそうであったように、既に幾つかのメールサービスプロバイダで利用可能になっています。そのため、BIMI レコードを設定するドメイン名も増えてきています。

図表３－２－２２　BIMI の表示例(Google 社の Blog [注68]より)

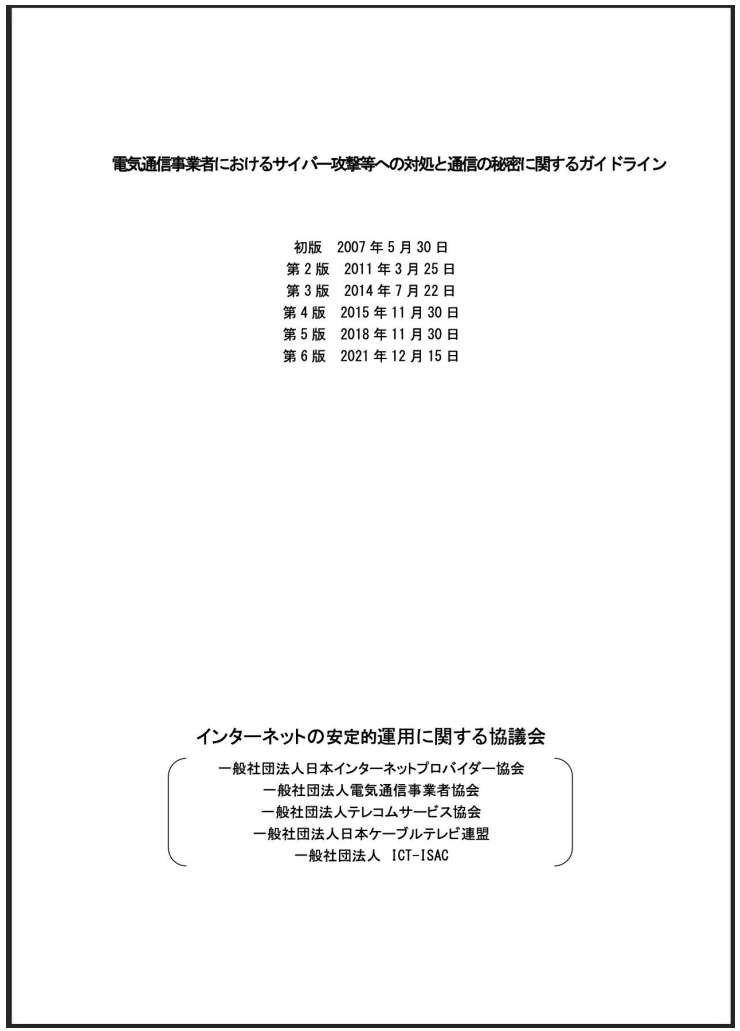
建設的なアプローチ②
サイバー攻撃への適正な対処の在り方



別紙１

電気通信事業におけるサイバー攻撃への
適正な対処の在り方に関する研究会
第四次とりまとめ

令和3年 11 月



電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン

初版　2007 年 5 月 30 日
第 2 版　2011 年 3 月 25 日
第 3 版　2014 年 7 月 22 日
第 4 版　2015 年 11 月 30 日
第 5 版　2018 年 11 月 30 日
第 6 版　2021 年 12 月 15 日

インターネットの安定的運用に関する協議会
一般社団法人日本インターネットプロバイダー協会
一般社団法人電気通信事業者協会
一般社団法人テレコムサービス協会
一般社団法人日本ケーブルテレビ連盟
一般社団法人　ICT-ISAC

JPAAWG

建設的なアプローチ③
DMARC 2.0 (MAAWG、IETFで議論中)

参考資料

・Googleおよび米国Yahoo!のアナウンス

https://blog.google/products/gmail/gmail-security-authentication-spam-protection/

https://blog.postmaster.yahooinc.com/post/730172167494483968/more-secure-less-spam

・日本ドメインのDMARC普及率調査

https://kitazaki.github.io/dmarc/

・ブログ記事

https://note.com/kitazaki/m/m1c77f4ceb818

Thank you for your listening!

登壇資料

JANOG54 Meeting in NARA

Gメールショック!
メールインフラを安心・安全に変える(た)、
にわとりたまご問題の結論とは。

～ソフトバンクの取り組み～

2024年7月5日

Google 送信者ガイドライン

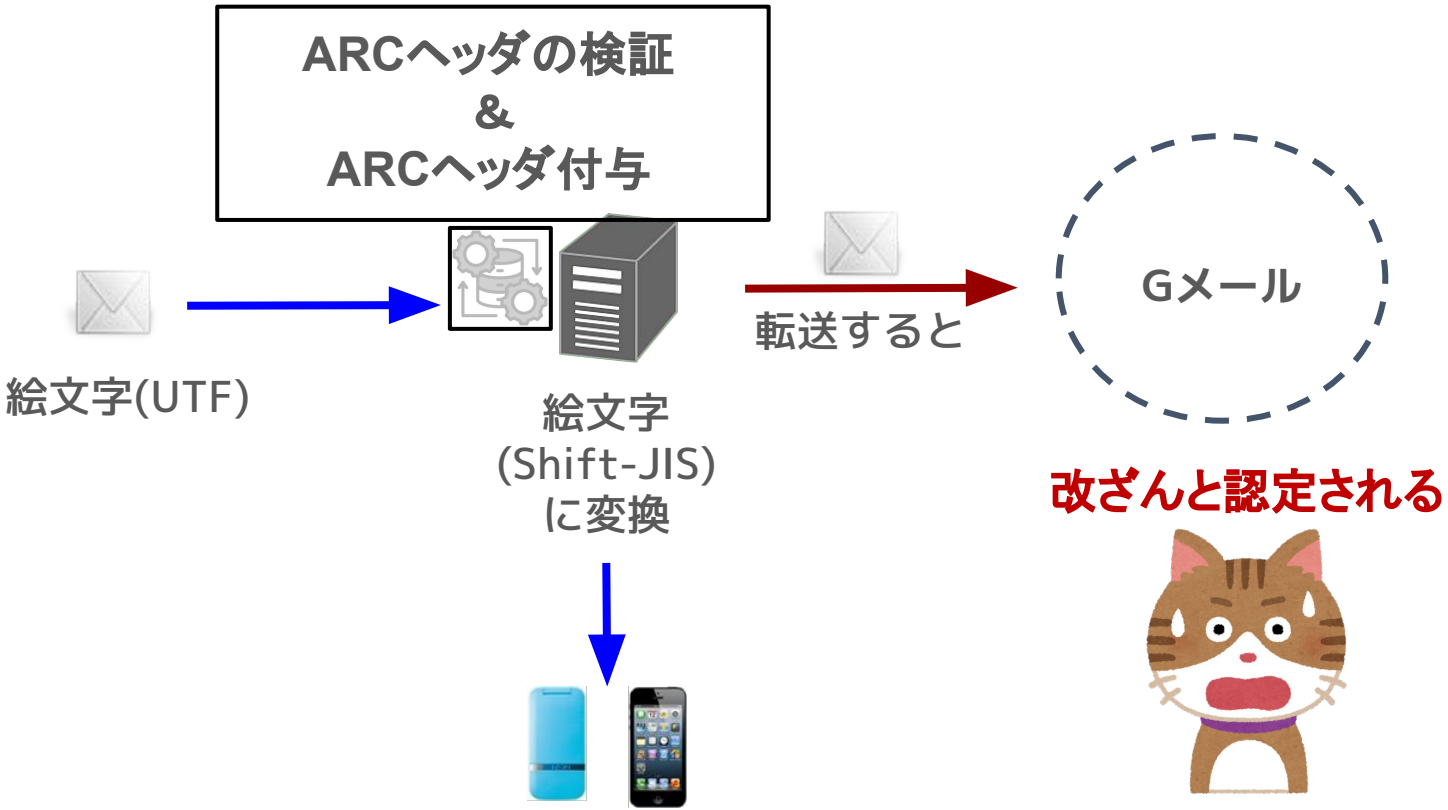
今後の取り組み

Google/YahooUS 送信者ガイドライン

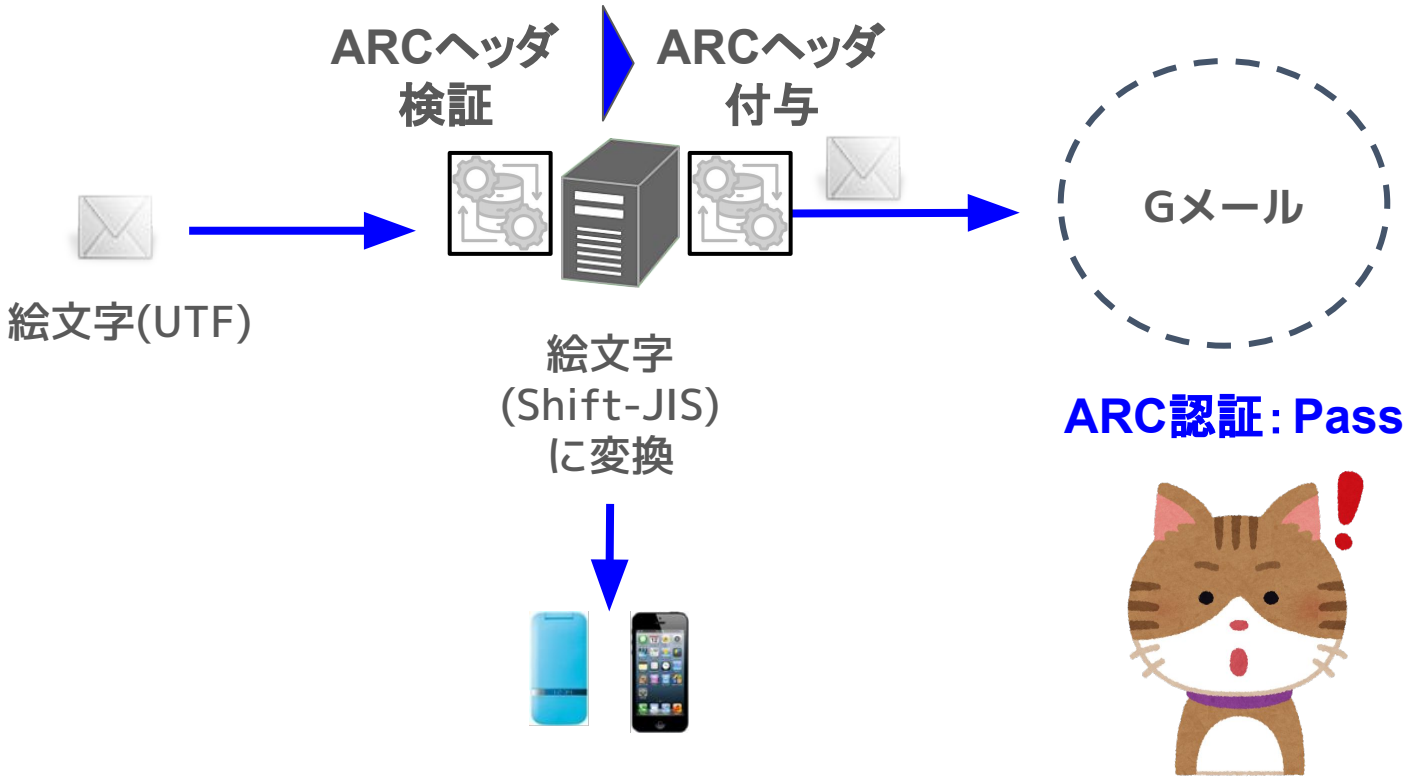
		SoftBank				
		S!メール	Email(i)	メアド 持ち運び		ODN SpinNet
				S!メール	Email(i)	
送信ドメイン認証	SPF	5月末までに対策完了				
	DKIM					
	DMARC					
ARC(推奨)						
SMTP TLS						
迷惑メール率 0.3%以下		困難な状況				

ARCは課題があり苦労しました・・

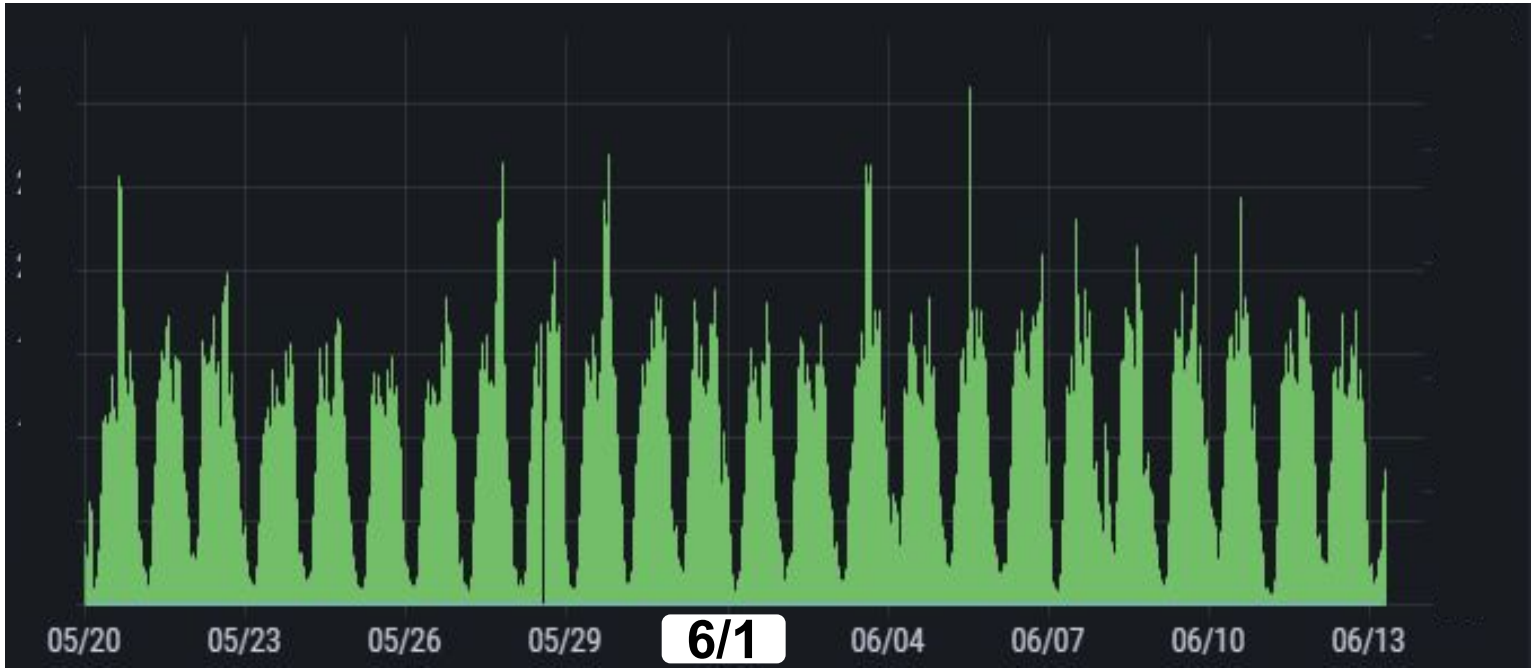
ARCは考慮が必要



転送時にARCヘッダ付与



Googleから6月以降で規制強化のアナウンスあり



送信トラフィック観点では6月以降の傾向は変わらず

Google 送信者ガイドライン

今後の取り組み

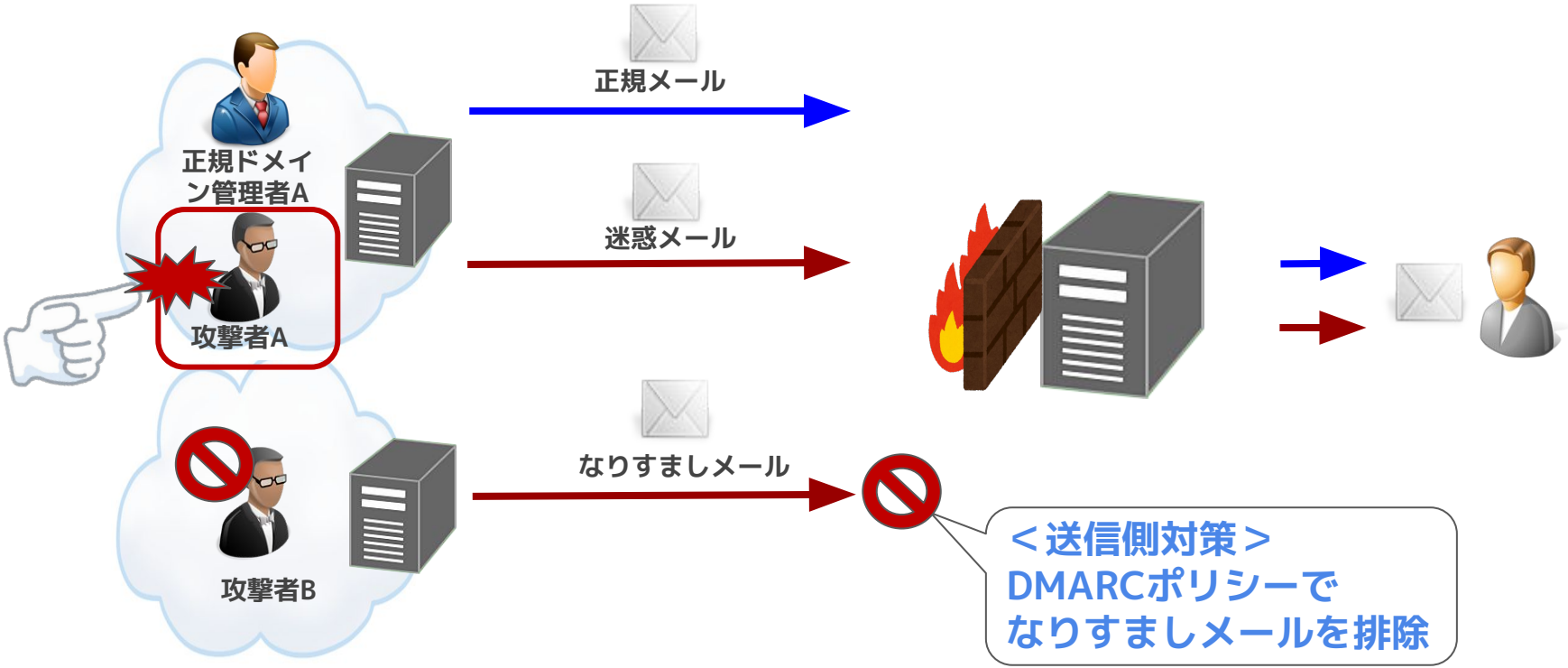
迷惑メールのトレンド変化

迷惑メール⇒フィッシングメール

コンテンツフィルタだけでは防ぎ知れない

フィッシングメールに有効な
ドメイン認証フィルタを
導入

これからは送信側対策が必要



課題：契約者が迷惑メールを送信

ソフトバンクも導入したい

【他事業者の導入事例】

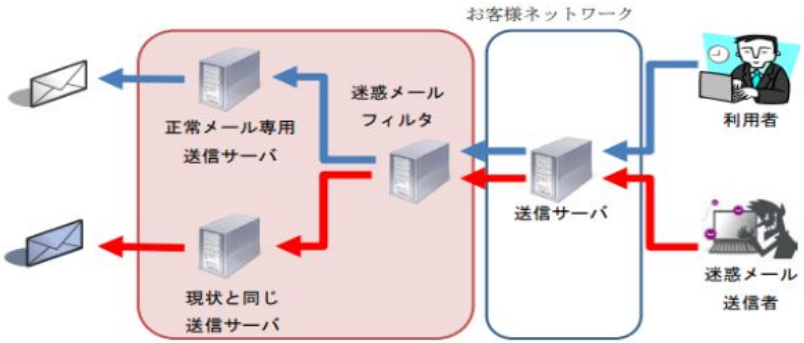


図1-5　送信IPアドレスの分離

特定電子メール等による電子メールの送受信上の支障の防止に資する技術の研究開発及び電子メールに係る役務を提供する電気通信事業者によるその導入の状況（総務省2016年12月）
http://www.soumu.go.jp/main_content/000591040.pdf

【もっと厳しく！！】

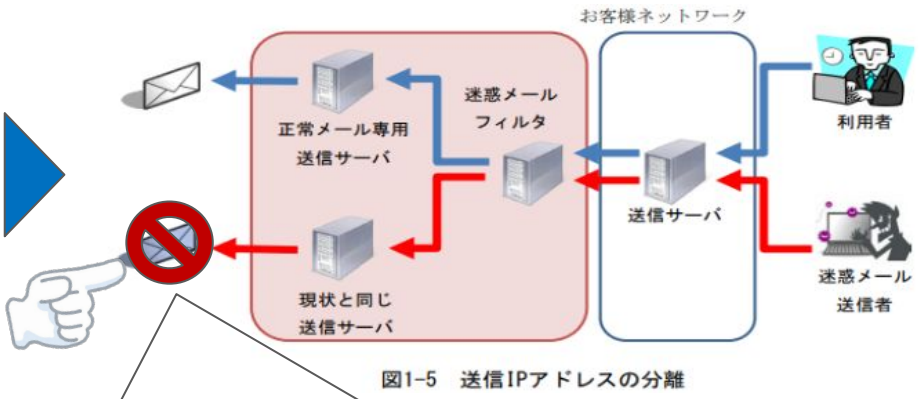
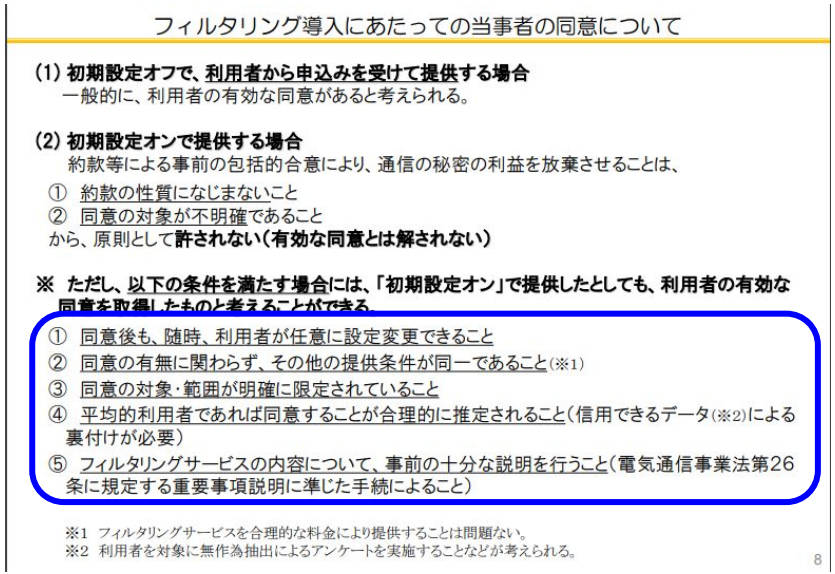


図1-5　送信IPアドレスの分離

迷惑メールを送信しない
そのためにはオプトアウトの仕組みは必要になる

迷惑メール送信者はオプトアウトするんだろうな
対策できるといいな

導入にあたっては・・



フィルタリング導入にあたっての当事者の同意について

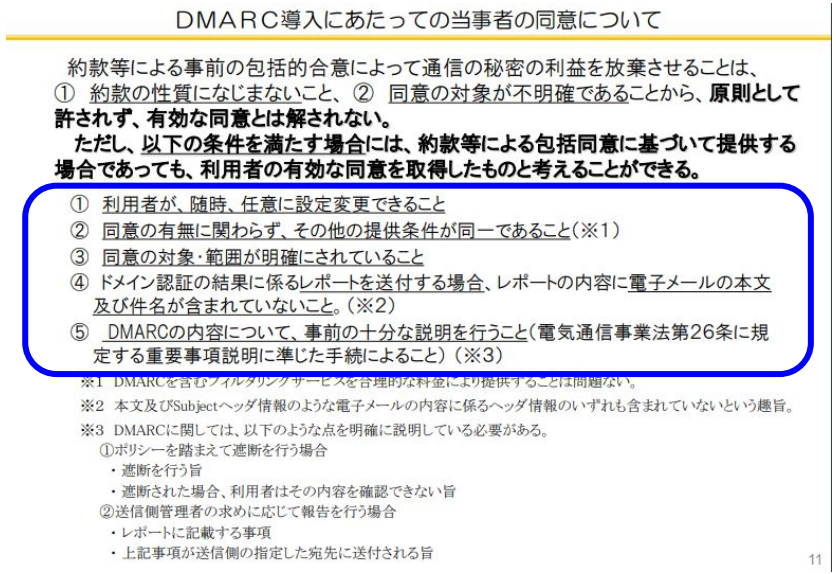
(1) 初期設定オフで、利用者から申込みを受けて提供する場合
一般的に、利用者の有効な同意があると考えられる。

(2) 初期設定オンで提供する場合
約款等による事前の包括的合意により、通信の秘密の利益を放棄させることは、
① 約款の性質になじまないこと
② 同意の対象が不明確であること
から、原則として**許されない（有効な同意とは解されない）**

※ ただし、以下の条件を満たす場合には、「初期設定オン」で提供したとしても、利用者の有効な同意を取得したものと考えることができる。
① 同意後も、随時、利用者が任意に設定変更できること
② 同意の有無に関わらず、その他の提供条件が同一であること（※1）
③ 同意の対象・範囲が明確に限定されていること
④ 平均的利用者であれば同意することが合理的に推定されること（信用できるデータ（※2）による裏付けが必要）
⑤ フィルタリングサービスの内容について、事前の十分な説明を行うこと（電気通信事業法第26条に規定する重要事項説明に準じた手続によること）

※1 フィルタリングサービスを合理的な料金により提供することは問題ない。
※2 利用者を対象に無作為抽出によるアンケートを実施することなどが考えられる。

8



DMARC導入にあたっての当事者の同意について

約款等による事前の包括的合意によって通信の秘密の利益を放棄させることは、
① 約款の性質になじまないこと、② 同意の対象が不明確であることから、**原則として許されず、有効な同意とは解されない。**
ただし、以下の条件を満たす場合には、約款等による包括同意に基づいて提供する場合であっても、利用者の有効な同意を取得したものと考えることができる。
① 利用者が、随時、任意に設定変更できること
② 同意の有無に関わらず、その他の提供条件が同一であること（※1）
③ 同意の対象・範囲が明確にされていること
④ ドメイン認証の結果に係るレポートを送付する場合、レポートの内容に電子メールの本文及び件名が含まれていないこと。（※2）
⑤ DMARCの内容について、事前の十分な説明を行うこと（電気通信事業法第26条に規定する重要事項説明に準じた手続によること）（※3）

※1 DMARCを含むフィルタリングサービスを合理的な料金により提供することは問題ない。
※2 本文及びSubjectヘッダ情報のような電子メールの内容に係るヘッダ情報のいずれも含まれていないという趣旨。
※3 DMARCに関しては、以下のような点を明確に説明している必要がある。
①ポリシーを踏まえて遮断を行う場合
・遮断を行う旨
・遮断された場合、利用者はその内容を確認できない旨
②送信側管理者の求めに応じて報告を行う場合
・レポートに記載する事項
・上記事項が送信側の指定した宛先に送付される旨

11

https://www.soumu.go.jp/main_content/000499986.pdf

電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン

https://www.jaipa.or.jp/other/mtcs/guideline_v6.pdf

EOF

【JANOG54 Meeting in NARA講演資料】

Gメールショック！
メールインフラを安心・安全に変える(た)、にわとりたまご問題の結論とは。

GメールショックへのKDDIの取り組み

KDDI株式会社
中島　直規

2024/07/05

Tomorrow, Together
KDDI
おもしろいほうの未来へ。
au

本日のおしながき

1. Gメールショックを振り返る
2. 6月を迎えて
3. au発の迷惑メールを防げ！(対策強化)
4. 誰が悪者なの？っていうか誰が判断するの？問題
5. 今後議論していきたいコト！

お断り

本講演資料は、

・個人の見解を述べたものであり、会社としての見解・業界としての見解ではありません。

・スクリーンショット等にて引用させていただいたものは2024/06/27現在の情報です。
　資料同ページ内に引用元URLの記載、またはハイパーリンクを掲載しております。

・上記いずれも各会社の商号、商標または登録商標です。

・一部イラストには著作権フリーイラスト／弊社キャラクターを利用させて頂きました。

1. Gメールショックを振り返る

■2023/10 ～

Google/米Yahoo!より大量送信者向けガイドライン公表

ISPメールやキャリアメールは対象なのか？
どこまでやる必要があるの？？
業界関係の方とも話しながら、右往左往……情報収集に追われる

■2023/12 ～

キャリアメール/ISPメールの送信DKIM対応など

短納期での開発～試験～導入でテンヤワンヤも、なんとか滑り込み……

■2024/4 ～

迷惑メール報告率が指針（0.3%未満）を大きく超えている事実に気付く

これもISPやキャリアメールは対象なのか？
指針を越えたらどうなるの？どこまで真面目に対策必要なの？？
業界関係の方とも話しながら、右往左往……情報収集に追われる
（2度目

1. Gメールショックを振り返る（答えのない悩み編

Google

マーケティングメールだけが対象！
トランザクションメールは対象外だ！

・どうやって分類しているの？
・ちゃんと「トランザクションメール」と判断してくれるの？

この判断如何によって大きく変わるハズなのに、
結局“最悪パターン”だけを考えて対策せざるを得なかった

Google

「迷惑メール報告率」とは受信したユーザーが
迷惑メールだよボタンを押した割合のこと！

・フィッシングメールじゃなくても、その人が「要らない！」と思ったメルマガやお知らせのメールなどもカウントされてしまうのでは・・・？
＃購読解除対応がこのための対応の一部であることは理解しているつもり

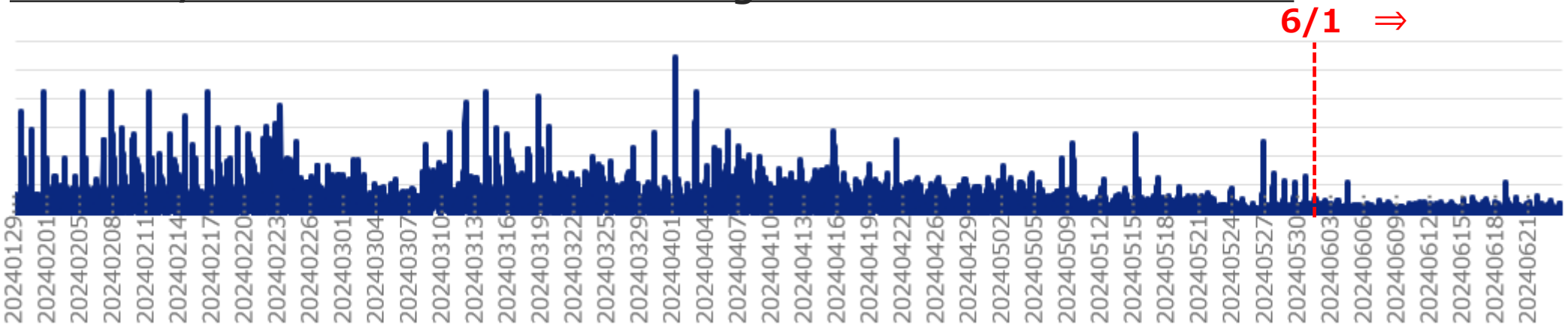
Google社独自指標のため、正確に解釈しようがない
「迷惑」と極力報告されないようにする対策を検討するしかなかった

2.　6月を迎えて

0.3%を超過した状態が継続中。

※0.3%の壁はほぼ突破状態

ですが、6/1を過ぎても（今のところ）Google宛のエラー数は平常値で推移。



3.　au発の迷惑メールを防げ！(対策強化)

【auメール発の迷惑メール対策】

①1日の最大送信通数(1000通/日)を制限 ※常時実施中

⇒　（更に絞ると）正規のお客様も改悪／多数不正契約されれば効果は薄くなる

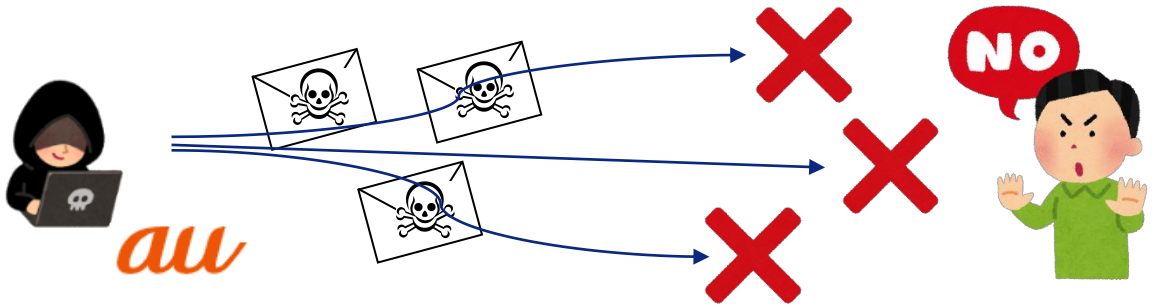
②送信メールを一律スパムチェック＆スパム判定メールは別IPアドレス帯から送信 ※常時実施中

⇒　配信自体は規制できない／ドメイン単位での迷惑メール率悪化は防げない

③「怪しい大量送信者」を日々監視＆停止 **※今回強化実施（①を繰り返す送信者は停止措置）**

⇒　もっと「怪しい」送信行為に踏み入って規制したい…

もっとアグレッシブに「悪者」を見つけて、対処を進めたい！
迷惑メールを防ぎたい！！・・・でも。



4. 誰が悪者なの？っていうか誰が判断するの？問題

【ケース1】 “悪者”判断可能（根拠：約款明記）
送っているメールのうちの一定数以上が「宛先不明」なメール

約款上、「宛先不明」なメールを多数送っている場合に
利用を制限する可能性ありと約款で規定あり

(12) その契約者回線から送信したＬＴＥ　ＮＥＴ電子メール（その契約者回線の契約者が、当社が別に定める電気通信設備を利用して送信したものを含みます。）において、宛先として指定されたメールアドレスののべ数の合計が、その日の開始時から起算して1000に達した場合、以後、同日中においては、その契約者回線からのＬＴＥ　ＮＥＴ電子メールの送信（その契約者回線の契約者が、当社が別に定める電気通信設備を利用して行うものを含みます。）を行うことはできません。この場合において、宛先として指定されたメールアドレスが存在しないものであった場合であっても１のメールアドレスとして数えます。

第52条　前条の規定による場合のほか、当社は、次の通信利用の制限を行うことがあります。
（1） 通信が著しくふくそうする場合に、通信時間又は特定地域の契約者回線等への通信の利用を制限すること。
（2） 電子メール（別表１に規定する５Ｇ　ＮＥＴ電子メールをいいます。以下この条において同じとします。）に係る通信が著しくふくそうする場合に、電子メールの配信を制限すること。
（3） 電子メールに係る通信において、多数のメールアドレスを指定して送信された電子メールであって、その電子メールのあて先に実在しないメールアドレスが著しく多いと当社が認めた場合に、その電子メールの配信を拒否すること。
（4） 契約者が電子メールを利用して送信した電子メールについて、その電子メールの転送を継続して行うことがａｕ（５Ｇ）通信サービスの提供に重大な支障を及ぼすと当社が認めた場合に、その電子メールの転送を停止すること。
（5） 契約者回線を当社が別に定める一定時間以上継続して保留し当社の電気通信設備を占有する等、その通信がａｕ（５Ｇ）通信サービスの提供に支障を及ぼすおそれがあると当社が認めた場合に、その通信を切断すること。
（6） 当社の電気通信設備において取り扱う通信の総量に比し過大と認められる通信を発生させる等、その契約者回線を用いて行われた通信が当社の電気通信設備の容量を逼迫させた、若しくは逼迫させるおそれを生じさせた、又は他の契約者回線に対する当社のａｕ（５Ｇ）通信サービスの提供に支障を及ぼした、若しくは及ぼすおそれを生じさせたと当社が認めた場合に、その契約者回線に係る通信の帯域を制限すること。

【ケース2】 “悪者”判断可能（根拠：不正対応HPに明記）
auユーザー様からの迷惑メール申告で申告が一定数以上あり

「不正な行為に関する通報・申告対応、当社の対応」についての中で
「利用制限」を行う可能性に言及あり
Eメールを利用した不正な行為に関する通報・申告方法、当社の対応 | 迷惑メールへの取り組み | au

【ケース3】 問題はコイツ。
送っているメールのうちの一定数以上が**怪しい**メール
怪しい例）セキュリティエンジンで「スパム・ウイルス」判定されている
毎日大量にメールを送信している　等

怪しい？悪者ってこと？
「なんの情報」を基にして“怪しい”とするの？
怪しい人を見つけたら…個別対応はしてよいの？一体どこまでしてよいの？
っていうか、誰が判断するの？

Tomorrow, Together KDDI　おもしろいほうの未来へ。au

5.　今後議論していきたいコト！

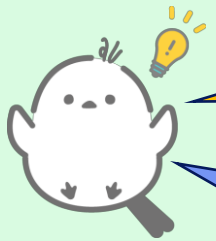
“通秘”が通用しない国の企業のショックに対応していくために！

大量受信
大量アクセス
不正ID搾取による大量送信等

→ 既存ガイドライン等に基づき緊急避難措置などで対処
※大量通信等への対処と通信の秘密に関するガイドライン等

フィッシングメールの送信（流布行為）
設備容量ひっ迫を引き起こさない不正送信等

→ **誰が悪なの？誰が判断するの？（二度目**



なんで迷うのか？なんで誰も判断したがらないのか？
メール疎通を脅かす“迷惑メール送信行為”に言及するガイドライン類の不足！

各社／担当者に責任を押し付けず、通秘を言い訳に対策が進まない世界を抜け出して、
堂々とクリーンなメッセージング環境を維持できる業界を目指して。
“迷惑メール送信行為”に対応できるガイドライン整備へ動きたい！

【議論していきたいコト】

- 不正を判断するために利用できる情報の拡大と明示
  - ☞　「何の情報」を「どのような前提」で利用してよいか？
- 不正行為への判断内容と事前同意の有無などの明示
  - ☞　どこまでの措置が可能？事前同意なく緊急避難で実施可能？　　など

Tomorrow, Together
KDDI
おもしろいほうの未来へ。
au

「つなぐチカラ」を進化させ、
誰もが思いを実現できる社会をつくる。

KDDI VISION 2030

JANOG54 Meeting in Nara

Gメールショック!
メールインフラを安心・安全に変える（た）、
にわとりたまご問題の結論とは。
~NTTドコモの取り組み~

2024/7/5

株式会社NTTドコモ
第一プロダクトデザイン部

Google送信者ガイドラインは**対応が急遽必要**となった項目もあり大変だった

送信者ドメイン認証	SPF,DKIM,DMARCの必須化
ワンクリック購読解除	1クリックでオプトアウト可能にする
TLS化	START TLSに対応する
DNSの適正化	逆引きなどにきちんと対応する
スパム率への考慮	ユーザからの迷惑メール申告0.3%以下

ISPメール提供者視点で見た場合、**ドメイン認証などは必須化**されてほしい

送信者ドメイン認証	SPF,DKIM,DMARCの必須化
ワンクリック購読解除	1クリックでオプトアウト可能にする
TLS化	START TLSに対応する
DNSの適正化	逆引きなどにきちんと対応する
スパム率への考慮	ユーザからの迷惑メール申告0.3%以下

本対応により、Eメールがドメインレピュテーション可能になる

スパムフィルタの精度を検証するうえで重要な手掛かりとなる

安心安全なEメール環境のためにはHeader fromドメインが信頼性が重要

Eメールの主な構成要素(スパムフィルタ観点)

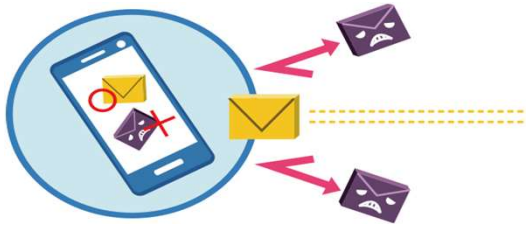
正規メールドメインの**すべてがDMARC認証されている**ことが理想

Header fromドメイン	従来はなりすましが容易だったが、DMARCにより認証が可能となった
Envelope fromドメイン	SPFにより認証が可能。しかし送信元とは無関係のドメインの場合も多い
ディスプレイネーム	なりすましが容易。認証手段も存在しない
件名	自由に設定可能。スパムは句読点等で難読化している場合が多い
本文	一定のスパム特徴は存在するが、自由度が高く判別は難しい
送信元IPアドレス	共用IPを利用している拠点は多く、活用は慎重に行う必要がある
本文内のURL	スパムはランダムドメインで難読化している場合が多い

NTTドコモは近年DMARCにより①**フィルタ強化、②正規メール判別**を強化

①フィルタ強化

DMARCを用いたスパムフィルタの導入



技術の導入に積極的なメールドメインはなりすましの流通リスクが低減

②正規メールの判別

ドコモメール公式アカウントの提供

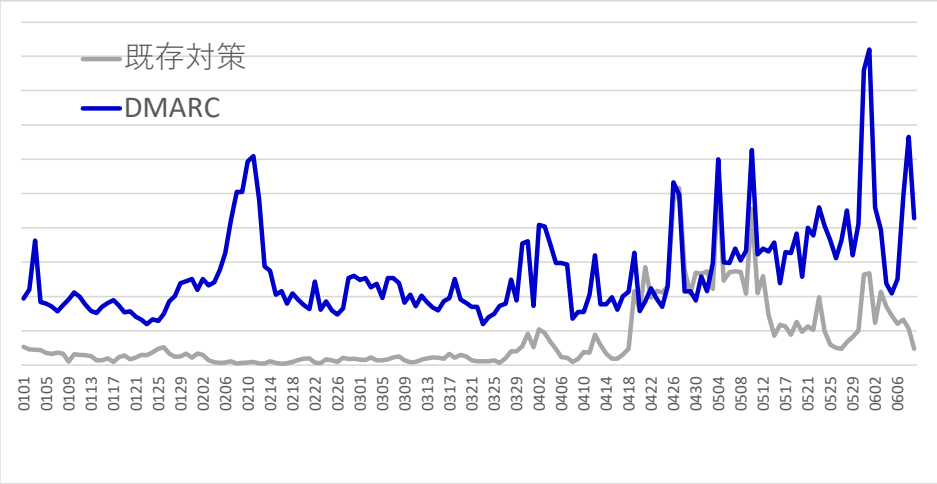
DMARC導入済のドメインなら、簡単な手続きで、ユーザ側で正規メールの判別が可能となる

技術導入に積極的なドメインにおいて**上々の効果**

①フィルタ強化

DMARCを用いたスパムフィルタの導入

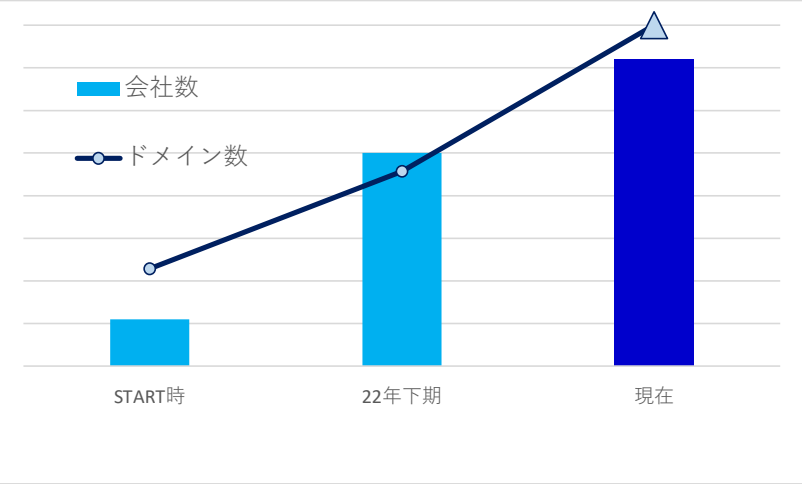
・既存対策の**数十倍のフィッシングメールを検知**



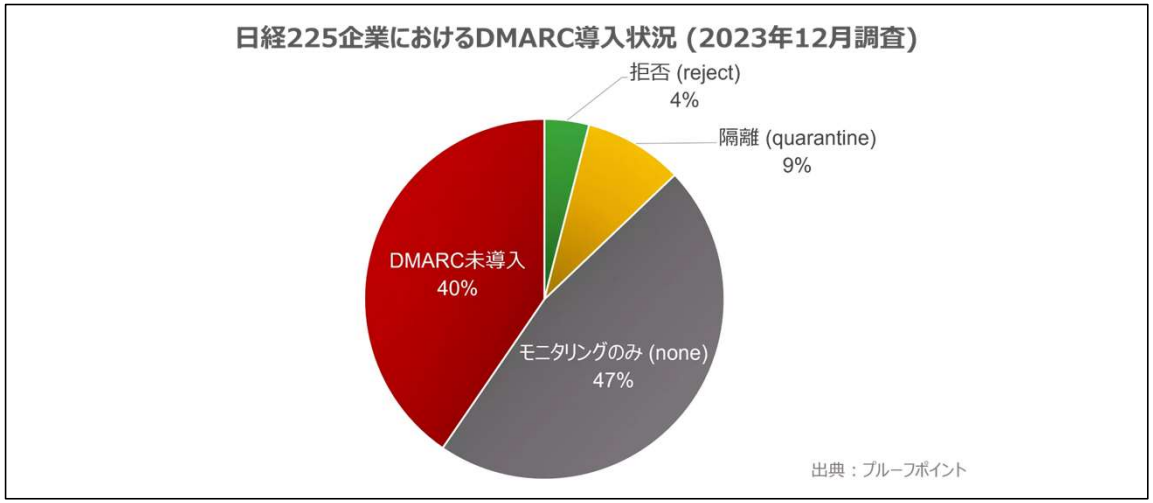
②正規メールの判別

ドコモメール公式アカウントの提供

・多くの企業さまが導入済



しかし、日本国内では**DMARCの普及が今一つ**



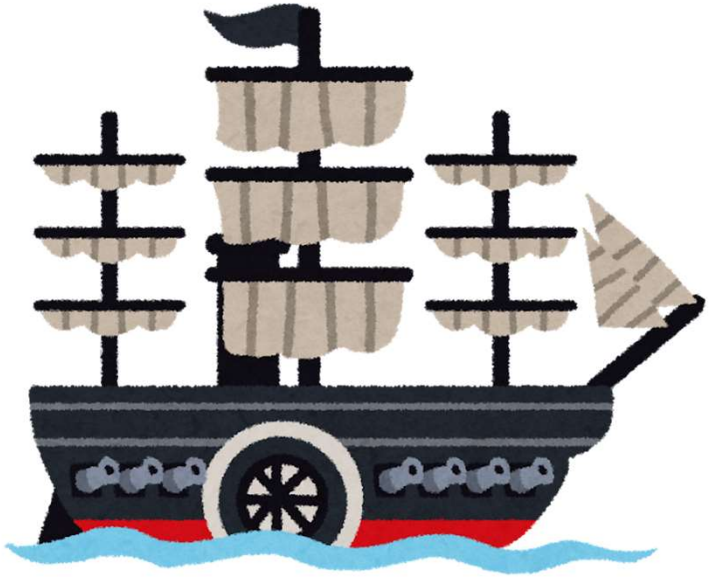
引用：【DMARC導入率グローバル調査 2023】日本はようやく60%が対応に着手するも実効性ではいまだ最下位
https://www.proofpoint.com/jp/blog/email-and-cloud-threats/Global-DMARC-Adoption-Rate-Survey-2023

想定される課題

・非フィッシング被害企業への広がり
・ドメイン認証技術自体のわかりにくさ
・やらないことによる**デメリットのなさ**

きっかけが必要

Googleのガイドラインはまさに黒船相当の衝撃



送信者ドメイン認証	SPF,DKIM,DMARCの必須化
ワンクリック購読解除	1クリックでオプトアウト可能にする
TLS化	START TLSに対応する
DNSの適正化	逆引きなどにきちんと対応する
スパム率への考慮	ユーザからの迷惑メール申告0.3%以下

NTTドコモもDMARCが当たり前になるよう、新たな対策を開始します

DMARCを用いた警告表示機能の概要

身元確認（ドメイン認証）ができていないメールは**一律警告を表示**
提供開始時期：**2024年10月以降**

目的

・**基準レベルをDMARC導入済**に引き上げる
・基準を満たしたメールはドメインなりすましはないので、**ドメイン単位でレピュテーション**を行う
・基準未達、またはレピュテーションの結果に従い、ユーザが**視覚的にわかりやすい警告**を行い詐欺を**未然に防止**する

正規メールの証明やポリシー変更が実施されているほど信頼できると想定

安心安全なEメール環境の想定

信頼できる

危険

状態	
ドコモメール公式アカウント導入済	ユーザ側で正規のメールを判別可能な状態
BIMI導入済	
DMARC導入済（p=quarantine以上）	Header fromの検証に失敗したメールが流通しない状態
DMARC導入済(p=none)	受信設備でHeader fromの検証が可能な状態
DMARC未導入	受信設備でHeader fromの検証ができず、なりすましメールの可能性を除去できない
DMARC認証失敗	

基準

まずは、Lv1を目指していく状況。そのために**DMARCの普及拡大が必要**

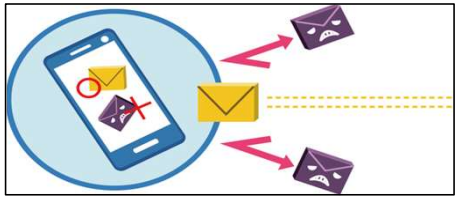
Lv0:検証不可能	・Header fromなど送信者の情報から正当性が確認できない
Lv1：検証可能	・DMARCによりHeader fromの検証が可能　等
LV2：正当なメールの判別可能	・公式アカウントやBIMI等で正規メールの判別が可能 ・p=rejectポリシー等でなりすましメールの流通を根絶 ・DMARC導入済の正規メールのドメインの一覧化　等

まとめ

・①フィルタ強化のため**2024/10にDMARCの必須化を行います**

・**DMARCの普及拡大**によるドメインの信頼性判定を実現していきたい

①フィルタ強化



ユーザ設定のルールベースフィルタ

セキュリティ製品を活用したフィルタ

DMARCポリシーを活用したフィルタ

DMARC導入有無による警告表示

②正規メールの判別

ドコモメール公式アカウント

BIMI

議論ポイント

・SPF同様、DMARC認証が導入済が当たり前となるために必要なことは？

・正規メールの判別方法の普及（公式アカウント、BIMI）のために、送信者側が必要とするインセンティブはなにか？