JPAAWG 5th General Meeting
[A1-5]大手メールサービスにおけるセキュリティ・なりすまし対策の最新の取り組み

JPAAWG 5th General Meeting
2022/11/7（月）

株式会社NTTドコモ
プロダクトデザイン部

自己紹介

名前

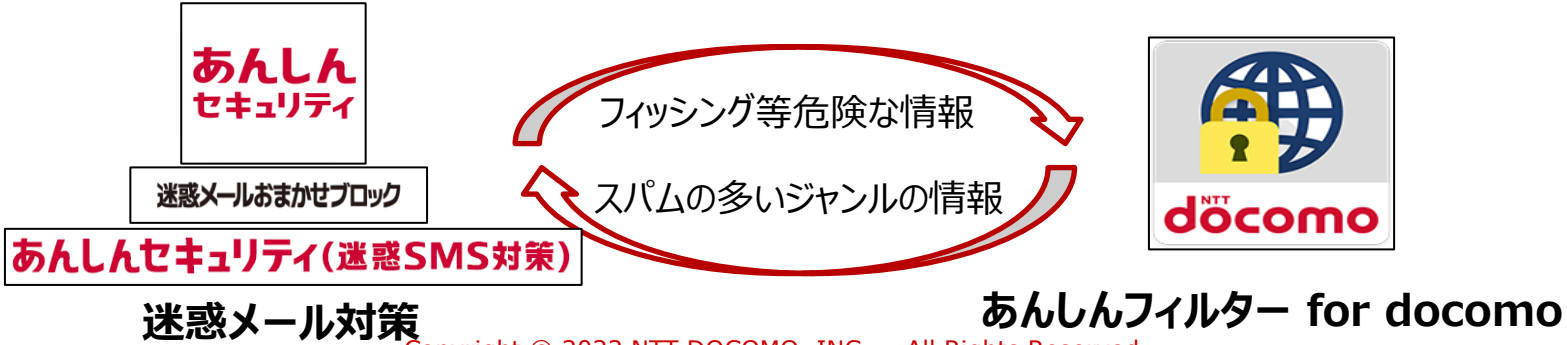
正見　健一朗

所属

株式会社NTTドコモプロダクトデザイン部ライフスタイルイノベーション・ヘルスケア担当

担当業務

・迷惑メール対策に関する企画、運用
・青少年インターネット環境整備（フィルタリング）に関する企画、運用



迷惑メール対策　　あんしんフィルター for docomo

スパム対策に関する主な取り組み事例

FY2018~2019

AIを用いたフィッシング検出基盤の構築

FN申告からフィッシングの特徴を有する検体を自動で分類、出力

FY2019 ***2nd JPAAWG***

検出したフィッシングの送信源への対処

流通量の多い送信元様と協力し、攻撃者の利用停止を実施

FY2020

フィッシングに特化したスパムフィルタ導入

「詐欺/ウイルスメール拒否」を導入し、フィッシングメール用のフィルタを設置

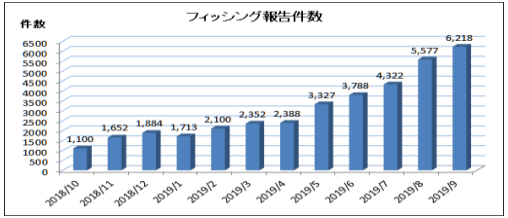
FY2021 ***4th JPAAWG***

ドコモメール公式アカウント開始

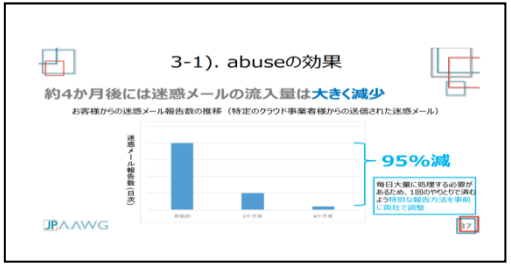
正規のメールをユーザが視認できるよう公式マークの表示を開始

FY2022 ***5th JPAAWG general meeting 2022/11/07***

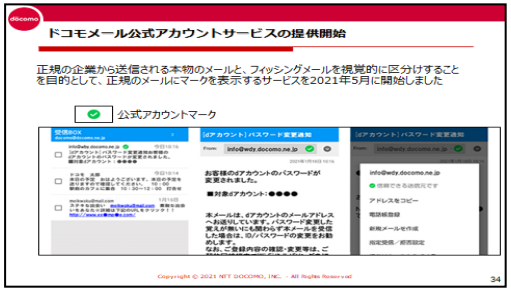
DMARC/DKIMの導入



出展：フィッシング対策委員会2019年9月レポート
https://www.antiphishing.jp/report/monthly/201909.html



出展：2nd JPAAWG　弊社投影資料



出展：4th　JPAAWG　弊社投影資料

スパム対策に関する主な取り組み事例

FY2018~2019
AIを用いたフィッシング検出基盤の構築

FY2019
検出したフィッシングの送信源への対処

FY2020
フィッシングに特化したスパムフィルタ導入

FY2021
ドコモメール公式アカウント開始

FY2022 *5th JPAAWG general meeting*
DMARC/DKIMの導入

即時対処が可能な手段を模索

残存spammer対策として新たな受信対策を実施

すり抜けにより正規メールの信頼性が低下しているため対策を実施

しかし、フィッシングの脅威が高まり続けているため、強めの受信対策を実施

本日は、DMARCの導入によって、どうお客様をフィッシング詐欺が守っていくかについて、弊社の狙いについてお話いたします

フィッシング詐欺のパターン(接続先サイト)

2021年のJPAAWGにおいて下記のようにフィッシングメールに記載されている
URLのリンク先について紹介しました。

①リアルタイムフィッシング型

②マルウェア配布型

③個人情報詐取型

①のケース

②のケース

③のケース

続いて、入り口となるフィッシングメール自体のパターンについて紹介します

フィッシング詐欺のパターン(メール本文)

①ターゲット企業ドメインのなりすまし

From: info@●△-net.com
件名 アカウントの自動退会処理について
●日頃より「」をご利用いただきありがとうございます。
●当社は10月14日にシステムを更新する予定です。　ログインはこちら

②ターゲット企業とは違う、
無関係なメールドメインのなりすまし

From: info@mydocomo.com
件名 【重要】カード会員ご本人認証サービス
【重要】カスタマセンターからのご案内
昨今の第三者不正利用の急増に伴い、弊社では「不正利用監視システム」を導入し、24時間365日体制でカードのご利用に対するモニタリングを行っておりますログインする

③ドメインのなりすましをせず
ランダム文字列などを使用

From: ofnrv172@p3i〇1s3h8.xyz
件名 カードの不正使用防止ご本人確認のお知らせ
このたび、ご本人様のご利用かどうかを確認させていただきたいお取引がありましたので。誠に勝手ながら、カードのご利用を一部制限させていただき、ご連絡させていただきました。
ログイン

本日は、被フィッシング詐欺である**①、②の対策として「DMARCフィルタリング」**、
誤認狙いの**③の対策として「ドコモメール公式アカウント」**についてご紹介します

補足　②のドメイン使いまわしによるスパム

①誤認を狙った類似サービスへの誘導

②単なるドメインの勝手な利用

③キャリアメールドメインのなりすまし

From: info@m.hiroba.dpoint.docomo.ne.jp
件名 【ポイント広場】会員登録完了のおしらせ
早速ログインしてお楽しみください！
↓ ↓ ↓ ↓ ↓
▼ポイント広場TOP▼　https://goo.gl/

From: riomi-emfqy@●●.co.jp
件名 新着メッセージがあります
★お住まいの地域で2人の女性が連絡をお待ちです
http://darere5698.quest/bdia/snslp/bdia02/index01.php?I2I=a03
▼配信停止はこちら

From: 080000000000@docomo.ne.jp
件名 【パズ〇ラ】スマホゲームが課金し放題に！
コロナで収入が激減した俺…なのに、、同じ部署の千夏センパイが最近、やたらと羽振りが良い。。驚愕の事実が明らかに・・・！！▼続きはこちら▼＋

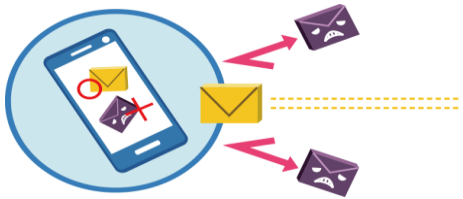
スパムフィルターのすり抜け目的に、単なるスパムも関係ないドメインを騙っている場合が多くあります。DMARCフィルタリングはスパムの流通も防止が可能です

2軸の対策

先ほどご紹介した攻撃への対抗として２つの軸で対策を推進しています

①偽物メールを止める

詐欺/ウイルスメール拒否（DMARCフィルタリングを新たに機能追加）



②正規メールを正しく認知する

ドコモメール　公式アカウント

公式アカウントマーク

①の止めるための技術として今年度DMARC/DKIMを用いたメールフィルタリング技術を導入しました

なぜ、いまDMARCなのか

Spamの特徴

・大量のばらまき
・キャリアメール等ISPメールなどからもばらまく
・本文では射幸心をあおる
・ドメインは適当なものが多い
・アダルトや出会い系などサービスへの誘導が多い

〇大量送信の検知
〇abuse対応
〇本文特徴を使ったフィルタ
×送信ドメイン認証のフィルタ
△URLを用いたフィルタ

フィッシングの特徴

・ターゲットを狙った攻撃
・国外サーバなどから発信
・正規メールの本文を模倣する
・正規ドメインを模倣する
・詐欺行為が行われているサイトへの誘導が多い

×大量送信の検知
×abuse対応
×本文特徴を使ったフィルタ
〇送信ドメイン認証のフィルタ
△URLを用いたフィルタ

・旧来のspam向けの対策ではフィッシングのトレンドに追従できませんでした
・フィッシングは正規ドメインのなりすましが多く、送信ドメイン認証がFailとなっているため、ドメイン認証を用いたフィルタリングと相性が良い

ドメインなりすましのフィッシング検体の実例

①インターネット物品販売に関するフィッシング

From: changeid@●●.co.jp
件名 にご登･のアカウント（名前、パスワ･ド、その他･人情･）
●●に登･いただいたお客･に、アカウントの情･更新をお届けします。
残念ながら、アカウントを更新できませんでした。
･求先住所が･更されたなど、さまざまな理由でカ･ドの情･を更新できませんでした。

②クレジットに関するフィッシング

From: △▲@●●.co.jp
件名 【重要】●●カード本人確認のお知らせ
このたび、ご本人様のご利用かどうかを確認させていただきたいお取引がありましたので、誠に勝手ながら、カードのご利用を一部制限させていただき、ご連絡させていただきました。つきましては、以下へアクセスの上、カードのご利用確認にご協力をお願い致します。

③銀行に関するフィッシング

From: info@●●.co.jp
件名 【●●銀行】重要:必ずお読みください
このたび、ご本人様のご利用かどうかを確認させていただきたいお取引がありましたので、誠に勝手ながら、カードのご利用を一部制限させていただき、ご連絡させていただきました。つきましては、以下へアクセスの上、カードのご利用確認にご協力をお願い致します。

すでにDMARCポリシーを隔離または拒否を宣言済みの正規ドメインに対するフィッシングも日々検出しており、フィルタリングの効果が期待できます

ドコモはすでに送信ドメイン認証をやっていたのでは？

SPFの限界

ドコモは2007年より、SPF認証によるなりすましメール拒否機能を提供しています
しかし、機能的な限界を感じていました

①：正規のメールの認証失敗がそれなりに多い

②：攻撃者は自分のドメインでpassにして攻めてくる

③：SPFのポリシーに対する対処は事業者の判断となっており、厳しく判定することは難しい

正規ドメインにおいてSPFがpassなら正規メールとみなせるが
Fail＝なりすましメールと判断できないことが多い

SPFの限界（Fail時の取り扱い）

SPFは認証失敗時が複数のステータスに分類されるが、
どのようなケースでフィルタリングすることが最適か判断が難しい

認証結果	意味
None	SPFレコードが公開されていない
Neutral	SPFレコードが“?”として公開されている条件にマッチした
Pass	認証処理に成功した
Fail	SPFレコードが公開されているが、認証に失敗した
SoftFail	SPFレコードが“~”として公開されている条件にマッチした
TempError	一時的な障害で認証処理が失敗した
PermError	SPFレコードの記述に誤りがあるなどで認証処理に失敗した

引用：
有害情報対策ポータイルサイト迷惑メール対策編
https://salt.iajapan.org/wpmu/anti_spam/admin/tech/explanation/spf/

弊社からみて、明らかに正規のメールにおいてもNoneやPermError、あるいはSoftFail
といった場合も多数検出しています

更なる対策へ

SPFを活用し、フィッシング対策を実行

・目視で１つ１つ真贋を確認　→都度個別にフィルターを設置
・信頼できる要素のみを活用する　→ドコモメール公式アカウント

そういえば

迷惑メール白書に現状の課題に対する
答え(DMARC)が掲載されていました
(迷惑メール対策推進協議会様ありがとうございます)

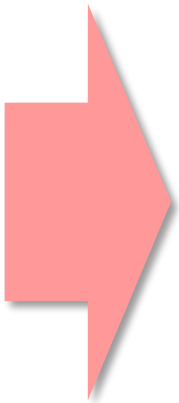
DMARCの導入効果の検討(SPFとの対比)

・SPFは認証結果を用いたフィルタリングの判断が難しい

・SPFは転送に弱い

・スパムメールは独自ドメインによるSPF=passが多い

・SPFは普及率が高い



・DMARCは送信元のポリシーに従いフィルタリング判断が可能

・SPF&DKIMを使えば転送時も適切に判断が可能

・フィッシングメールはドメインなりすましが多く、認証失敗している場合が多い

・フィッシングメールの脅威の高まりにより、送信側での普及拡大が見込まれる

DMARC(&DKIM)はSPFの上位機能としての性格を有しており、
SPFで抱えている課題を解決するには適切であると判断

DMARC導入のユーザメリット

弊社のお客さまである、ドコモメール利用者さま、および利用者さまとコミュニケーションを実施されるメール送信者さま、双方においてメリットがあります

	送信者	受信者（ドコモのお客様）
①	自社の騙りメールを排除できる	フィッシングメールが届かない
②	自身のDNSの宣言で受信側のfilter作成が可能	能動的なドメイン個別カスタマイズが不要
③	Ruaレポート等を通じて、正規設備からの意図しない認証エラーを検知可能	ヘッダ等を通じて認証結果の視認が可能

いま被フィッシングメールの害がない皆様におかれましても、将来のドメインなりすましの防止を企図し、DMARCの導入についてご検討いただければ幸いです

[参考]DMARCの導入検討時の苦労点・御礼

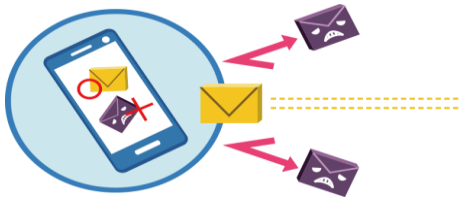
課題	対応
①技術仕様が難しい	迷惑メール白書、送信ドメイン認証導入マニュアルなど皆様の普及にむけた活動を参考にさせていただきました。 受信側として、何を導入し、どう結合し、どうやってお客さまに提供するかについて業界標準が見えにくいため手探りに進めました
②受信/送信双方における導入効果が見えにくい	通信の秘密の関係上、本当に導入したらフィッシングメールを止めることができるのか検証することが難しく、効果の定量化が課題でした。有識者の方のご講演を拝見し、特にフィッシングメールに強みがあることなどが確認でき非常に助かりました。
③検証の難しさ	メールの送信は送信者毎にパターンがあるともいえ、大変多岐にわたっております。今後も安定稼働にむけ、日々調整を実施してまいります。
④普及率	この先どう日本国内で普及をさせるかがまだ継続の課題だと認識しています。弊社としても普及促進に寄与してまいりたいと考えています。

JPAAWGにご参加の皆様の過去からのお取組によって解決できた課題がとてもたくさんありました。改めて御礼申し上げます。

2軸の対策

①偽物メールを止める

詐欺/ウイルスメール拒否（DMARCフィルタリングを新たに機能追加）



②正規メールを正しく認知する

ドコモメール　公式アカウント

公式アカウントマーク

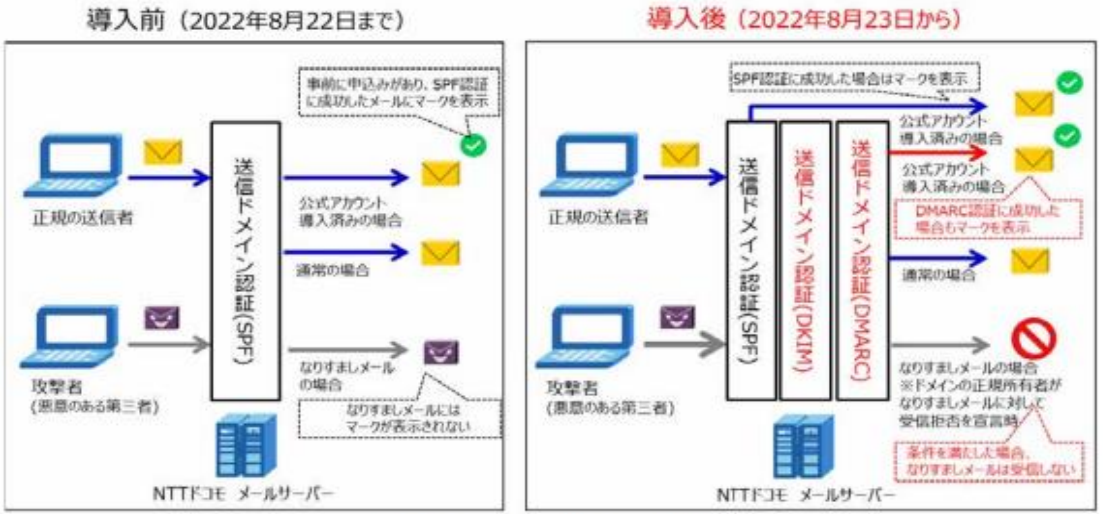
続いて②の対策であるドコモメール公式アカウントの取り組みについてご紹介します

2022/8/23　NTT docomo報道発表資料抜粋

ドコモメールに送信ドメイン認証技術「DMARC」「DKIM」を導入

～なりすましメールの判別精度向上によりフィッシング詐欺の対策を強化～

株式会社 NTT ドコモ（以下、ドコモ）は、お客さまにドコモメールをより安心してご利用いただくため、ドコモメールに送信ドメイン認証技術「DMARC※1」「DKIM※2」（以下、本技術）を、2022 年 8 月 23 日（火）から新たに導入いたします。本技術により、送信ドメインによる認証が強化され、なりすましメールの判別精度が向上いたします。



送信ドメイン認証によるなりすまし対策の概要

ドコモメール公式アカウントのねらい

ドメインはなりすまさず、しかしターゲット企業のメールだと誤認するような攻撃に対し、正規メールと判別するための手段を提供する機能です

From: shigure@sin.skr.jp
件名 【重要】dアカウントで不審な動きが検出されました。
dアカウントで不審な動きが検出されました。 下記の接続から停止原因を確認してください
▼ご利用確認はこちら
https://id.smt.docomo.ne.jp/cgi7/id/men

From: hoax@halting.com
件名 【重要】カード会員ご本人認証サービス
――――――――――――――――――――
docomoから大切なお知らせがございます。
――――――――――――――――――――
日ごろからdocomo端末をお使い頂き誠にありがとうございます。
特典1：キャンペーン対象者となった翌々月下旬に進呈いたします。

攻撃メールの例

From: info@mydocomo.com
件名 【NTTドコモ】ケータイ補償申込み内容のお知らせ
この度は「ドコモオンライン手続き」からケータイ補償の補償申込みをいただき、誠にありがとうございます。
お申込みをいただいた内容を確認させていただき、特に不備等ない場合はご指定頂いた日時にお送り致します。

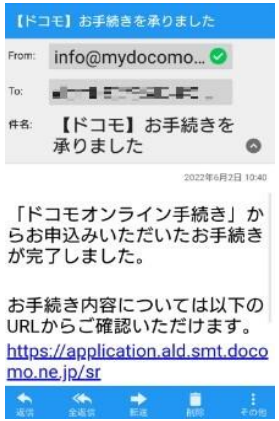
正規メールの例

マークの有無で正規メールかどうかが一目で判別可能になります

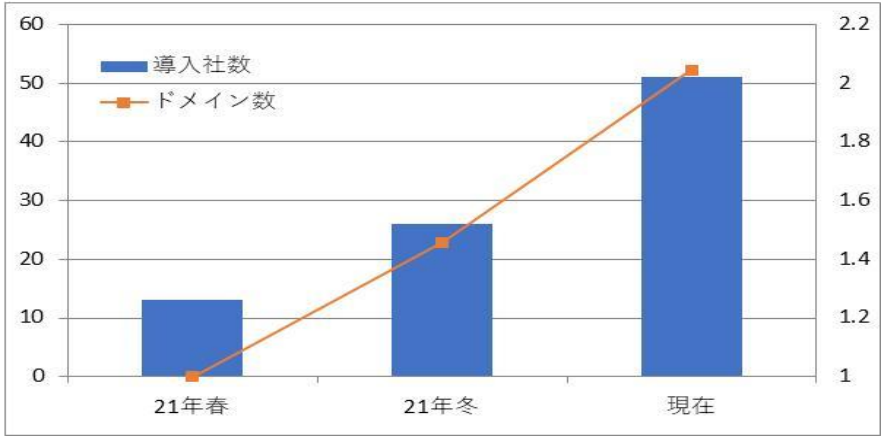
ドコモメール公式アカウント

攻撃者が改変できないアプリのネイティブ部に公式マークを表示し、偽物を判別します

公式アカウントマーク



導入拠点/ドメイン数



※ドメイン数はサービスイン時を1とした場合の増加割合

おかげさまで、フィッシング詐欺に苦慮している企業さまの多くに
ご導入いただいております

機能改善１：DMARC対応

・従来はSPFによって正規メールを判別していたため、技術的な制約があり少々煩雑でした

今後は

送信元さまが保有するHeader from ドメインに対して、DMARCの認証が成功するメールであれば導入が可能、とシンプルになります。

前半でお話したDMARCによるなりすましメール対策を実施したドメインであれば
基本的に公式アカウントの導入が可能です

参考：機能改善によるメリット

①メジャーな組み合わせである、Header fromドメインが企業様独自ドメイン、Envelope fromドメインがメール配信企業さまのドメインの場合でも申し込みができるようになります

	Header from ドメイン	Dkim	Envelope fromドメイン	いままで
申込可能	@tarou.com	@tarou.com	@cloudses.com	NG ※envelopeがドメイン汎用

②Envelope fromドメインの単位での管理が不要となります

	Header from ドメイン	Dkim	Envelope fromドメイン	いままで
１種類のドメイン管理でOKとなる	@tarou.com	@tarou.com	@cloudses.com	Envelope fromドメイン単位での管理が必要
			@cccnote.com	
			@bma.mmmm.com	

機能改善２：送信元組織名の表示

・DMARCによってある程度メールの種別で認証状態を制御できるようになるため、
送信元の組織名を表示する機能を具備しました。

こちらの文字(デフォルトは公式アカウント)を送信元様にご指定いただけるように改善しました。

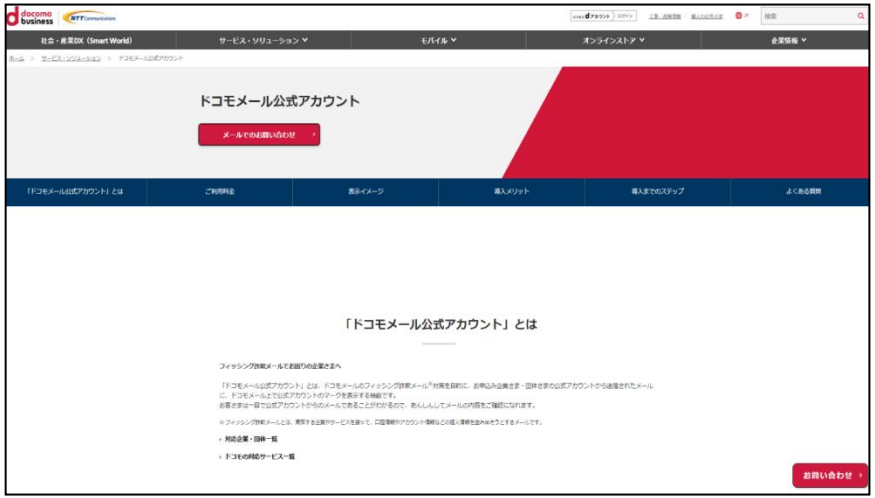
DMARCをご利用の場合はHeader fromドメイン単位で出し分けが可能です

公式アカウントの導入について

・ご検討段階における相談も受け付けておりますのでお気軽に下記よりお問い合わせいただければ幸いです。

・認証部分など技術的な検証などもお手伝いしております

お問い合わせ先：
https://www.ntt.com/business/services/official_account.html



本日のまとめ

まとめ

NTTドコモはフィッシング対策として、
①偽物を止める：DMARCフィルタリング
②正しい認知：ドコモメール公式アカウント
の機能を提供（※）しており、今後も改善に努めてまいります。

※ご利用料金は無料です

両機能ともに、メールの送信元さまにおいても導入を実施いただく必要がございます。フィッシング詐欺やスパムメールにお困りの送信元さまにおかれましては導入についてご検討いただければ幸いです

あなたと世界を変えていく。

NTT docomo

ご清聴ありがとうございました