JPAAWG 6th General Meeting
[A1-7]キャリアメール側から見たフィッシング被害がない企業も含めたDMARC化のメリット

JPAAWG 6th General Meeting

2023/11/6（月）

株式会社NTTドコモ

自己紹介

名前

正見　健一朗

所属

株式会社NTT　第一プロダクトデザイン部

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

あんしん
セキュリティ

迷惑メールおまかせブロック

NTTドコモの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	フィッシングの特徴を有する検体を自動で検出
FY2019	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機能の導入
FY2021	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	DMARC/DKIMの導入	DMARCを用いたフィルタリングの開始
FY2023	DMARCレポート送信開始	**DMARC導入企業さま向けに、DMARCレポート送信開始**

DMARCの技術を利用して、さらにあんしん安全なEメールの利用環境を提供すべく今後も改善を行っていきます

本日お伝えしたいこと

送信側におけるDMARCの普及はいろいろなプレーヤーにメリットがあります

- 被フィッシング詐欺の実害がある企業
- フィッシング詐欺とは無縁の企業
- Eメールを受信するユーザ
- Eメール送信をビジネス基盤とする配信サービス企業

本日は多くの企業にとって普及が進まない障害を軽減できればと考え、
メールを送信する企業さま、そしてそのメールを受け取るユーザ観点でのメリット
についてお話いたします

本日のお話の背景

DMARCの導入が進まない理由について以下の事例があると拝見しました

・費用がもったいない
・導入のしかたがよくわからない
・フィッシング被害にあっていない

確かに自社のメールサーバで多数のドメインのメールを送信する企業の場合はそうかもしれません

しかし、DMARCは簡単に導入できる場合もありますし、セキュリティ以外のメリットもございます。
本日はその観点にてお話をさせていただければと思います。

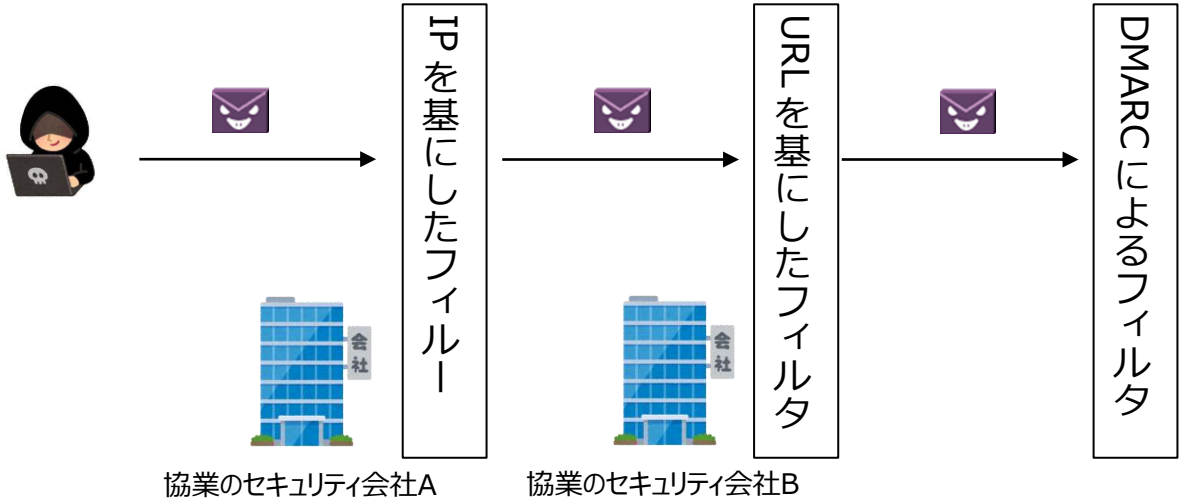
まずおさらいとして、DMARCの直接的なメリットについてお話します。
さきほどのメリットの享受者の例でいう

被フィッシング詐欺の実害がある企業

が該当します

NTTドコモにおけるフィッシングメールの防御機構

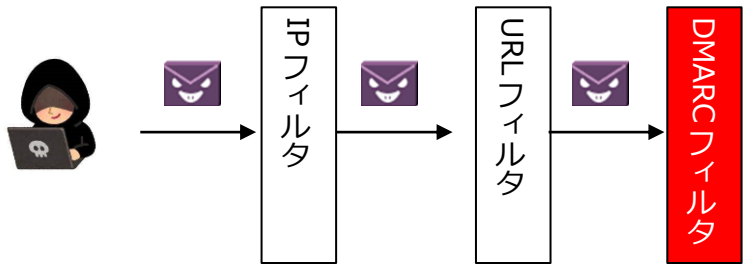
フィッシングメールに対して行っている代表的なフィルターは以下の３つです（順番は実際の動きと異なります）

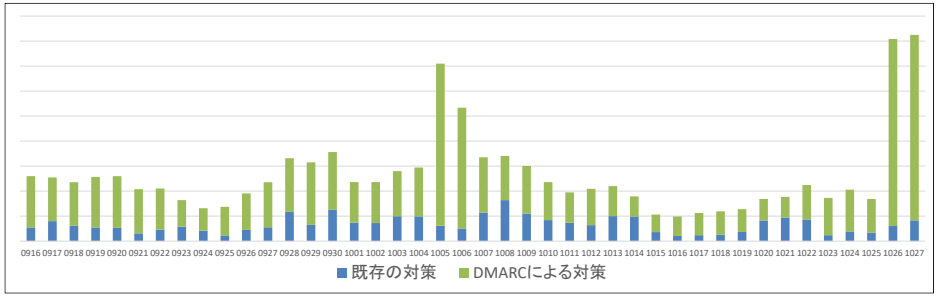


どれが一番効果が高いと思われますでしょうか？

NTTドコモにおけるフィッシングメールの防御機構

圧倒的にDMARCによるフィルタの検出数が多いです。





NTTドコモのスパムフィルタのフィッシングメールの検出数

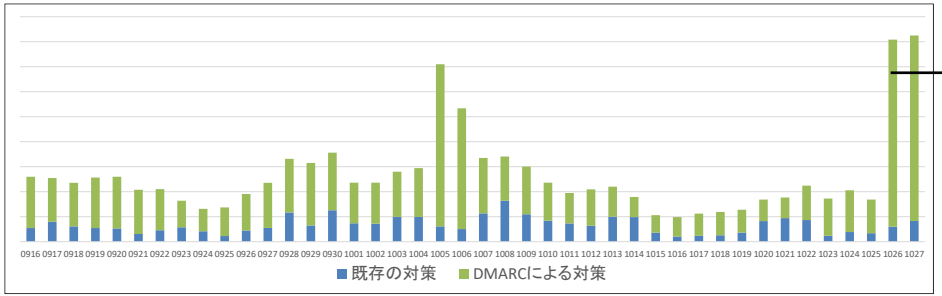
・まだ**国内で導入がしているドメインが少ない**現状でも**圧倒的な効果**が出ています

フィッシング詐欺攻撃の対象ドメインがDMARCを導入していることが多いという偏りのせいかもしれません

・しかし逆に見れば、ブロック覚悟で正規ドメインを成りすますケースが多いということでありDMARCの導入をしておくことで**自社ドメインを騙ったフィッシングメールの発生リスクを低減可能**と判断できます

既存のスパムフィルタと比較したDMARCフィルタのメリット

①攻撃が開始時点からフィルタが発動するため、**パターンマッチした場合すり抜けがない**



＜特定日に大量送信される場合＞
・IPやURLフィルタの場合
→攻撃開始直後の何割かはすり抜けとなる

・DMARCの場合
→**全数遮断が可能**

②DMARCフィルタは、レポート機能によりメール送信元が**早期になりすまし攻撃を検知可能**

NTTドコモや大手WEBメールサービスがレポートで分析に十分な情報が取得可能です

攻撃有無が知りたい

攻撃者のホストが知りたい

攻撃の分量が知りたい

攻撃時期が知りたい

レポート機能にて解決が可能です！

参考：DMARCレポート機能でわかること

・自社メールのドメイン認証の成功状態を監視可能

・認証が成功している、または失敗しているenvelope fromドメインなどの洗い出しが可能

・なりすましと思われる攻撃の検知が可能

これらはp=noneでも享受可能です。
弊社に届くレポートからは、Googleさまと弊社から送信するruaレポートにて相応の量が分析可能です。
分析を行うためのSaaSのサービスも複数ありますので、まずはDNSにレポート送信先を記載をお勧めします。

続いて現在フィッシングの攻撃をうけていない企業にもメリットがあることについてお話します

フィッシング詐欺とは無縁の企業

こちらです。

被フィッシング被害がある業界の場合

・フィッシング対策協議会さまから注意喚起されておりますが、クレジット・信販系、通信事業者・メールサービス系、金融系、配送系、EC 系、オンラインサービス系などは集中的に狙われています。

・そのため、現在狙われていなかったとしても次にやられる可能性があるため本業界についてはDMARC化していくほうが安全であると思います。

しかし

自分の業界は狙われてないし、今後も発生しないから関係ない

多くの場合、このようにDMARCをやろう、と思われなくても不思議はありません。

受信側からみたDMARCの価値

この場の皆様においてはご存じだと思いますが、改めて受信側から見たDMARCのメリットを洗い出します

①**Header fromドメインが**従来の技法よりセキュアに**認証できる**こと

②DKIMを上手に使うことで**Envelope fromドメインに依存せず認証が可能**なこと

③p=quarantineやp=rejectの宣言によりなりすましメールの流通を抑えることが可能なこと

③はメリット、デメリット含めてとてもインパクトが大きいため、③だけを見て、自社はなりすましメールがないからDMARCは導入不要と思われてしまうかもしれません。

しかし**受信側から見た場合、①と②もとても重要な意味**を持ちます。

よくある「メールが届かない」ことに関する送信側からのご指摘

メールドメインを伝えるから、なんとかしてくれ。

IPアドレスを伝えるから、なんとかしてくれ。

上記では、受信側としては何もできません。
実際のメールが、お申し出企業さまから伺った内容と一致しているかどうか確認する手段がないからです。

<u>しかし、DMARCにより、メールドメインの正当性が確認できるようになりました</u>

DMARC以前の問題点

投影限り

・以下のような場合、SPFの検証では正当性の確認ができませんでした

Header from	Envelope from	以前は検証が不十分だった理由	DMARCの認証結果
Sample.com	bma.mpse.jp	SPFがpassしていても、汎用ドメインのためheader fromドメインの証明にならない	SPFではfailとなる DKIMでsample.comの署名が必要
Sample.com	fcxxxx.cuenote.jp	xxxxのところが専用サブドメインのようにもみえるが機械的には判断できない	SPFではfailとなる DKIMでsample.comの署名が必要
Sample.com	xxx.sample.jp	Sampeのところは一致しており、人間が見れば同一企業に見えるが機械的に判断できない	SPFではfailとなる DKIMでsample.comの署名が必要

・DKIMは必ずしもHeader fromのドメインと一致しているものが署名されているとは限らず、正当性が確認できませんでした

DMARCによって解決されたこと

・Header fromとEnvelope fromの組織ドメインの一致が必要であり、SPFが信頼できるようになった

・Header fromと同じ組織ドメインの証明書が必要であり、DKIMが信頼できるようになった

つまり

DMARCが通っている〇〇というドメインについて、対応してほしい

とお伝えいただければ、正当性の確認が可能です。送受信双方にとって幸せな状態だと考えております

参考　DMARC導入時の注意事項

投影限り

・まれに、DMARCが失敗しているまま送信を続けている企業さまがいらっしゃるようです

Header from	Envelope from	ドメイン認証結果	想定される理由
Sample.com	sendgrid.net	SPF:　Fail DKIM:none	DMARCにおけるSPFの解釈誤り
Sample.com	xxx.amazonses.com	SPF:Fail DKIM:pass(amazonses.com)	DKIMで署名するドメイン誤り
Sample.com	Point.sample.jp	SPF:Fail DKIM:none	社内でHeader fromは統一したが、部分的に違う組織ドメインのenvelope fromから送っている場合など

・認証誤りを起こさないためには
　①可能ならばHeader fromとEnvelope fromは同じ組織ドメインを使う
　②同じ組織ドメインでpassだったとしても、可能な限りDKIM署名を付ける（転送対策）
が必要となります。

相当数のお客さまがPCメールからキャリアメールに転送されております。
①をやったとしても②がないとDMARC認証に失敗します。

DMARC化は簡単に可能です

メールの配送を専用サービスに業務委託している場合は、**簡単に実現可能**な場合があります

・私が担当しているサービスのメールについてDMARC化したときは、以下の手順で実施可能でした

①メール配信企業さまにDKIM化の相談をし、署名のペアを作成してもらう
②自社のメールのDNSにDKIMの認証に必要な情報を書き込む
③メール配信企業さまにDKIM署名の付与を開始してもらう
④自社のメールのDNSにDMARCの宣言を書き込む

この間１カ月かからなかったと思います。
ちなみに、この時はDKIMが必須というドメイン構成でした。その場合でも簡単に実現が可能です。

Header from	Envelope from	DMARC SPF	DMARC DKIM	DMARC認証結果
anshinmode-docomo.jp	Shared.bma.mptx.jp	Fail	d=anshinmode-docomo.jpの署名付与	DKIM側でPass

そして、お客さまの観点についてお話いたします

Eメールを受信するユーザ

お客さまから届く声で多いこと

SPAMが届くことが不満

フィッシングメールはメールサーバの時点で明らかにわかるのだから遮断してほしい

不快なメールは見えないようにしてほしい

SPAMの内容について気になってしまう

１億円当選というメールがきたが、本物かどうか確認する手段はあるか

本物のメールが不安になってきた

支払いに関するメールがきたが、フィッシングかどうか判断できなくて困っている

お客さまの問題点の解決にむけて

SPAMが届くことが不満

メール遮断性能の向上

p=quarantine以上の普及拡大

本物のメールが不安になってきた

メールのドメイン認証結果説明の簡単化

・ドコモメール公式アカウントの普及拡大
・BIMIの普及拡大

SPAMの内容について気になってしまう

メールの怪しさ加減の見える化

・p=none以上の普及拡大
・正規メールの認証失敗事例の撲滅

本日話す項目

SPAMが届くことが不満

メール遮断性能の向上

p=quarantine以上の普及拡大

本物のメールが不安になってきた

メールのドメイン認証結果の簡単化

・ドコモメール公式アカウントの普及拡大
・BIMIの普及拡大

SPAMの内容について気になってしまう

メールの信頼性の見える化

・p=none以上の普及拡大
・正規メールの認証失敗事例の撲滅

DMARC認証の結果について

①DMARC認証に失敗していたら、それは悪いメールであると判断可能か？

→p=quarantine以上の場合、これは真と考えています。DMARCで実現できたことの一つです

②DMARC認証が成功していたら、それは良いメールであると判断可能か？

→これは偽です。DMARC認証をpassしているspamはあります。
こちらに関しては、旧来のSPF/DKIMの課題を内包したままとなっています

From:
xxxx@XXXngelylongitude.site
Title:
3000万円振、込みます
Body:
メッセージが届いています
ワrよヨこhxxp://XXXugzpfw8gqr61u13.11762.strangelylong.site

独自ドメイン

From:
xxxx@Xmail.com
Title:
みずほ銀行のATMで振！り = 込 ^ みます！
Body:
家の玄関を出て、徒歩3分です！
3000万をなかった事にしたいので、もし良ければ受け取ってもらえませんか…？
無理にとは言いません！
https..data;http:¥¥;http://XXX-f7517flyzmqvna0 HTMLWWW1

ISPメール

どうすれば、メールの信頼性が判断ができるようになるのか？

既存のドメイン認証に加えて、**第三者によるチェックが必要**と考えております

DMARCによって担保されるHeader fromドメイン自体が正当な
目的をもって使われているか審査する

導入時に審査工程がある

NTTドコモ　ドコモメール公式アカウント

公式アカウントマーク

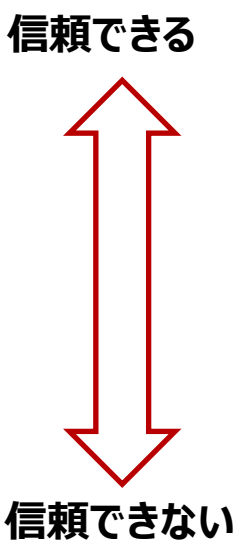
YAHOO!メール ブランドアイコン

BIMI

ドメイン認証の結果による信頼性判断

認証のレベル、そして第三者チェックの有無によって信頼性が定義できると考えています

具体例	第三者チェック	なりすましメールの排除	DMARC ※heade fromの認証	SPF ※envelope fromの認証
BIMI	○	○	○	○
公式アカウント	○	○	○	○
p=quarantien以上	×	○	○	○
P=none	×	×	○	○
DMARC未導入	×	×	×	○
認証失敗	×	×	×	×



お客さまの抱える課題解決にむけて

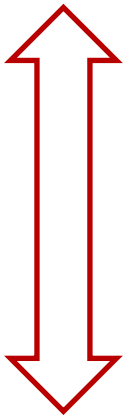
あんしん安全なEメール環境のため、最低限のラインがDMARC導入以上となることを期待しています

具体例	第三者チェック	なりすましメールの排除	DMARC ※heade fromの認証	SPF ※envelope fromの認証
BIMI	○	○	○	○
公式アカウント	○	○	○	○
p=quarantien以上	×	○	○	○
P=none	×	×	○	○
DMARC未導入	×	×	×	○
認証失敗	×	×	×	×

将来的に

受信したメールの認証状況、第三者チェックの有無等を総合的に勘案し、適切なUIを提供していくことを検討しております

信頼できる



信頼できない

具体例
BIMI
公式アカウント
p=quarantien以上
P=none
DMARC未導入
認証失敗

メールのドメイン認証結果の簡単化

・ドコモメール公式アカウントマークの表示（実施済）
・BIMIなど高度な技術を導入済のメールの見える化

メールの信頼性の見える化

・DMARC未導入メールに対するポリシーの定義
・認証失敗のメールの見える化

NTTドコモ　ドコモメール公式アカウント 無料

・ドコモメール公式アカウントは審査の過程でドメイン認証の状態を調査させていただいています
・**ドメイン認証がpassとなるよう支援も行っております**ので、DMARC p=none以上の導入をご検討されている場合は、**<u>ぜひお申込みください</u>**

公式アカウントマーク

https://www.docomo.ne.jp/info/spam_mail/official_account/

最後に、本日もいらっしゃってると思われますメール配信企業様の
メリットについて簡単にお話します

Eメール送信をビジネス基盤とする配信サービス企業

メール配送時のドメイン

・少なくない場合において、
　Header fromドメイン：顧客のドメイン
　Envelope fromドメイン：事業者さまのドメイン
を設定されている場合が多いかと思います。

Header from	Envelope from
Sample.com	bma.mpse.jp
Sample.com	fcxxxx.cuenote.jp

この場合、多いケースとしてEnvelope　fromのDKIM署名が付与されていますが、
受信側としてはHeader fromドメインのDKIM署名を欲しております。

顧客にDKIM署名の導入を案内しても難しい場合があるかと存じます。

ただ、**DMARCは疎通そのものにメリットがある**ことをお伝えし、**顧客ドメインのDKIM署名、およびDMARCの宣言**について進めてきたく存じます

NTTドコモ　ドコモメール公式アカウント 無料

・最終的な申し込みについてはHeader fromドメインを保有している企業さまからのお申込みをお願いすることになるかと思いますが、技術的な相談であれば顧客から依頼されている場合は**メール配信企業さまからの相談も受付しております**

・BIMIと違い、**ランニングコストがかからないというメリット**もございます
・ぜひ顧客のDMARC化のメリットの訴求材料としてご活用いただければ幸いです

公式アカウントマーク

https://www.docomo.ne.jp/info/spam_mail/official_account/

まとめ

被フィッシング詐欺の実害がある企業

・DMARCによるフィルタリングは、**既存機能と比較しても高い効果**がでています
・引き続き、p=quarantien以上の宣言をご検討願います

フィッシング詐欺とは無縁の企業

・メール疎通にもメリットがあります。送信側におけるDMARCの導入をお願いします
・**よくわからない場合でも、ぜひドコモメール公式アカウントにお申込みください。お手伝いします**

Eメールを受信するユーザ

・**DMARC認証が行われていることを前提**にして、受信ユーザ向けの機能改善を図っていきます

Eメール送信をビジネス基盤とする配信サービス企業

・顧客にDMARC推進をお願いします。**商材として公式アカウントなら無料で導入可能です**

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