想定所要時間 35分

Internet Week 2025 / H3
13:00～17:00

なりすましメールと DMARC を考える

DMARC ポリシー強化(p=reject)までの道のり

2025/11/20(木)

株式会社インターネットイニシアティブ (IIJ)
ネットワーク本部 アプリケーションサービス2部 アプリケーションサービス運営課
課長　古賀 勇

Ongoing Innovation

自己紹介

古賀 勇 (Isamu Koga)

株式会社インターネットイニシアティブ (IIJ)
ネットワーク本部 アプリケーションサービス2部
アプリケーションサービス運営課・課長

Power Automate エバンジェリスト (自称) **「自動化は正義」**

法人系メールセキュリティサービスの運用

SecureMX

- ウイルス対策
- 迷惑メール対策
- Sandbox
- 送信ドメイン認証
- 顧客サポート
- 執筆活動・公演活動・エンジニアブログ・技報

WIDE Project

M3AAWG

openSUSE (趣味)

本セッションのおさらい

別紙

（公印及び契印省略）

総基用第 76 号
令和７年９月１日

一般社団法人電気通信事業者協会会長　島田　明　殿
一般社団法人テレコムサービス協会会長　是枝　周樹　殿
一般社団法人日本インターネットプロバイダー協会会長　久保　真　殿
一般社団法人日本ケーブルテレビ連盟会長　塩冶　憲司　殿

総務省総合通信基盤局長
湯本　博信

フィッシングメール対策の強化について（要請）

平素より、情報通信行政に御理解と御協力をいただいておりますことに、厚く御礼申し上げます。

フィッシングメール対策について、政府は、「国民を詐欺から守るための総合対策 2.0（令和７年４月 22 日犯罪対策閣僚会議決定）」において、「詐欺メール、詐欺 SMS による被害防止等のための取組」として、「送信ドメイン認証技術（DMARC 等）への更なる対応促進」を掲げているところです。

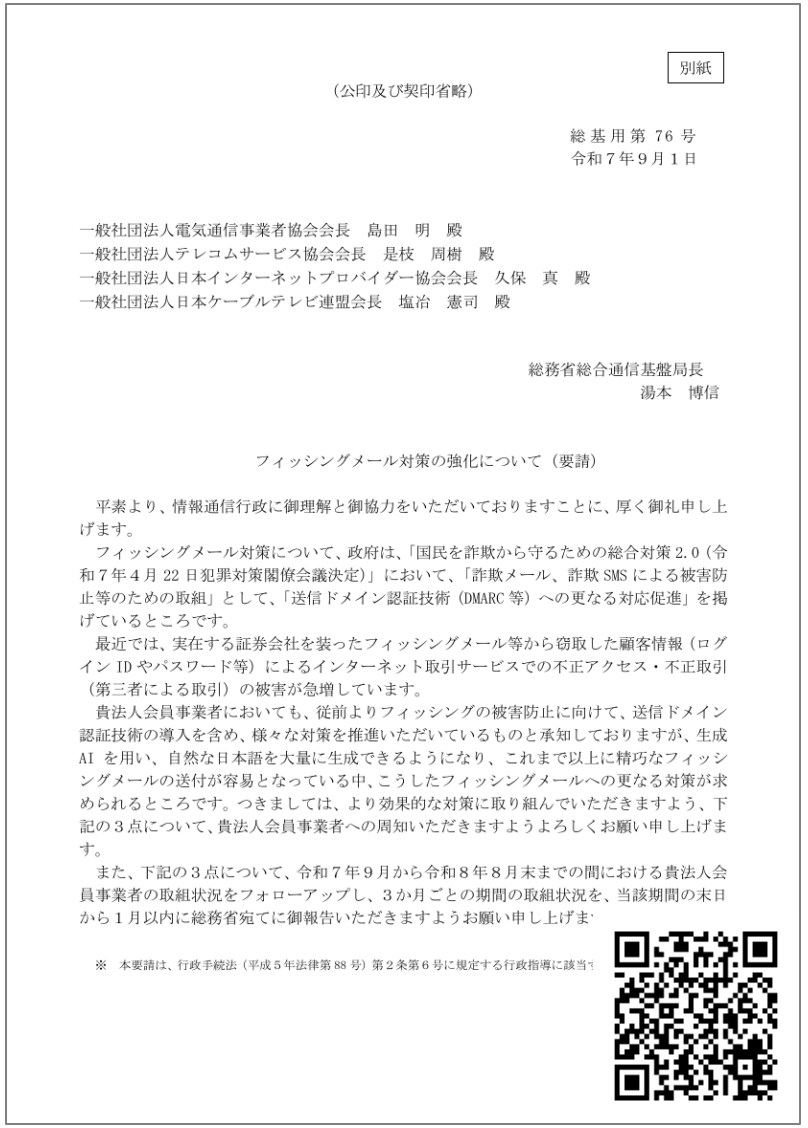
最近では、実在する証券会社を装ったフィッシングメール等から窃取した顧客情報（ログイン ID やパスワード等）によるインターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が急増しています。

貴法人会員事業者においても、従前よりフィッシングの被害防止に向けて、送信ドメイン認証技術の導入を含め、様々な対策を推進いただいているものと承知しておりますが、生成 AI を用い、自然な日本語を大量に生成できるようになり、これまで以上に精巧なフィッシングメールの送付が容易となっている中、こうしたフィッシングメールへの更なる対策が求められるところです。つきましては、より効果的な対策に取り組んでいただきますよう、下

https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000260.html

総務省「フィッシングメール対策の強化について（要請）」

事業者団体を通じて電気通信事業者への要請文章



別紙

（公印及び契印省略）

総基用第 76 号
令和７年９月１日

一般社団法人電気通信事業者協会会長　島田　明　殿
一般社団法人テレコムサービス協会会長　是枝　周樹　殿
一般社団法人日本インターネットプロバイダー協会会長　久保　真　殿
一般社団法人日本ケーブルテレビ連盟会長　塩冶　憲司　殿

総務省総合通信基盤局長
湯本　博信

フィッシングメール対策の強化について（要請）

平素より、情報通信行政に御理解と御協力をいただいておりますことに、厚く御礼申し上げます。

フィッシングメール対策について、政府は、「国民を詐欺から守るための総合対策 2.0（令和７年４月 22 日犯罪対策閣僚会議決定）」において、「詐欺メール、詐欺 SMS による被害防止等のための取組」として、「送信ドメイン認証技術（DMARC 等）への更なる対応促進」を掲げているところです。

最近では、実在する証券会社を装ったフィッシングメール等から窃取した顧客情報（ログイン ID やパスワード等）によるインターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が急増しています。

貴法人会員事業者においても、従前よりフィッシングの被害防止に向けて、送信ドメイン認証技術の導入を含め、様々な対策を推進いただいているものと承知しておりますが、生成 AI を用い、自然な日本語を大量に生成できるようになり、これまで以上に精巧なフィッシングメールの送付が容易となっている中、こうしたフィッシングメールへの更なる対策が求められるところです。つきましては、より効果的な対策に取り組んでいただきますよう、下記の３点について、貴法人会員事業者への周知いただきますようよろしくお願い申し上げます。

また、下記の３点について、令和７年９月から令和８年８月末までの間における貴法人会員事業者の取組状況をフォローアップし、３か月ごとの期間の取組状況を、当該期間の末日から１月以内に総務省宛てに御報告いただきますようお願い申し上げま

※　本要請は、行政手続法（平成５年法律第 88 号）第２条第６号に規定する行政指導に該当

https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000260.html

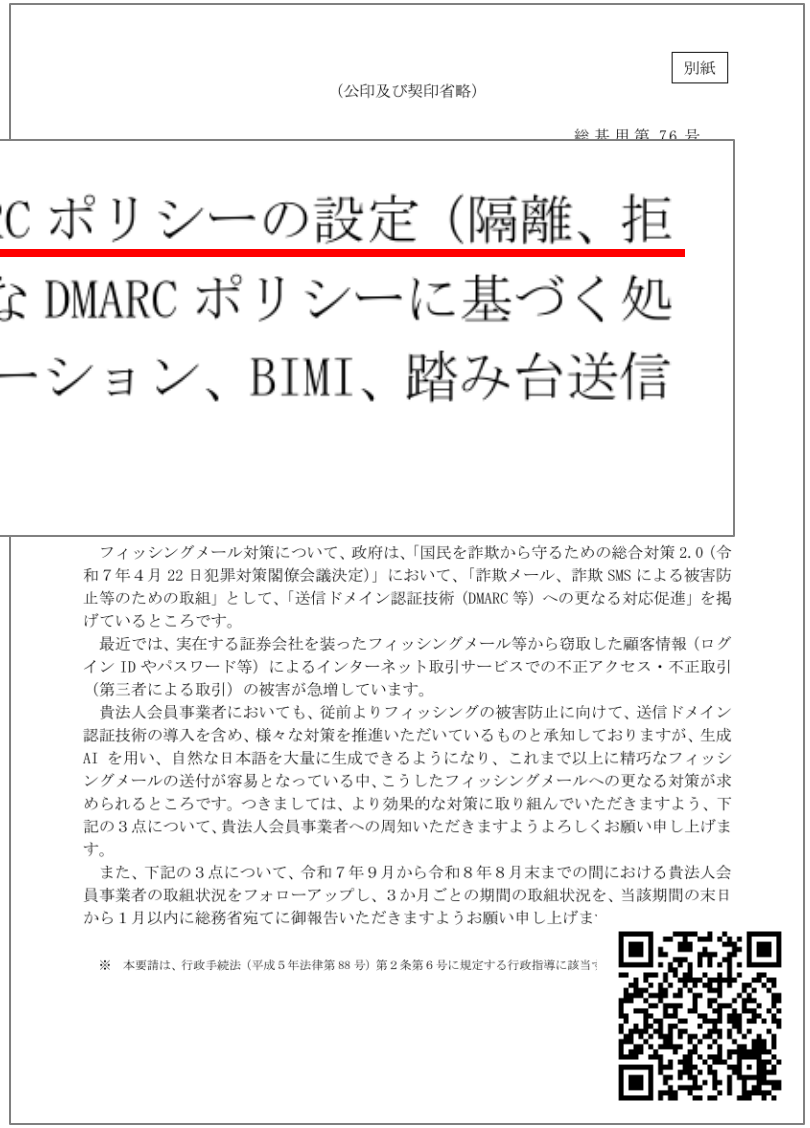
総務省「フィッシングメール対策の強化について（要請）」

事業者団体を通じて電気通信事業者への要請文章

（２）なりすましメール対策として有効な DMARC の導入や DMARC ポリシーの設定（隔離、拒否）を行うこと。送信側だけでなく受信側についても、適切な DMARC ポリシーに基づく処理やレポート送信を設定すること。また、ドメインレピュテーション、BIMI、踏み台送信対策等の更なる対策の導入を積極的に検討していくこと。

DMARC ポリシーの設定（**隔離、拒否**）を行うこと

p=quarantine/reject の話だ！



別紙

（公印及び契印省略）

総基用第 76 号

フィッシングメール対策について、政府は、「国民を詐欺から守るための総合対策 2.0（令和７年４月 22 日犯罪対策閣僚会議決定）」において、「詐欺メール、詐欺 SMS による被害防止等のための取組」として、「送信ドメイン認証技術（DMARC 等）への更なる対応促進」を掲げているところです。

最近では、実在する証券会社を装ったフィッシングメール等から窃取した顧客情報（ログイン ID やパスワード等）によるインターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が急増しています。

貴法人会員事業者においても、従前よりフィッシングの被害防止に向けて、送信ドメイン認証技術の導入を含め、様々な対策を推進いただいているものと承知しておりますが、生成 AI を用い、自然な日本語を大量に生成できるようになり、これまで以上に精巧なフィッシングメールの送付が容易となっている中、こうしたフィッシングメールへの更なる対策が求められるところです。つきましては、より効果的な対策に取り組んでいただきますよう、下記の３点について、貴法人会員事業者への周知いただきますようよろしくお願い申し上げます。

また、下記の３点について、令和７年９月から令和８年８月末までの間における貴法人会員事業者の取組状況をフォローアップし、３か月ごとの期間の取組状況を、当該期間の末日から１月以内に総務省宛てに御報告いただきますようお願い申し上げま

※　本要請は、行政手続法（平成５年法律第 88 号）第２条第６号に規定する行政指導に該当

https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000260.html

対策をサボると
どういう被害が出るのか

サービス利用者側ではなく、提供者側の話をします

よくある被害ケース (1) - 信用の低下

迷惑メール対策でフィルタされたり、「このドメイン名は危ないから見ないでおこう...」というユーザの行動心理につながる

「えきねっと」アカウントの自動退会処理について - メッセージ (HTML 形式)

ファイル　メッセージ　実行したい作業を入力してください...

2022/10/16 (日) 6:39

eki-net <info@eki-net.com>

「えきねっと」アカウントの自動退会処理について

宛先　koga@iij.ad.jp

●日頃より「えきねっと」をご利用いただきありがとうございます。

●当社は10月16日にシステムを更新する予定です。

●アカウントに長期間ログインしていないため、

●24時間以内にアカウントにログインして関連情報を更新してください。

●アカウント情報を更新しない場合は、アカウントを削除させていただきます。

●ご協力ありがとうございます。

ログインはこちら

●本メールは送信専用メールアドレスから送信されます。返信をいただいても返事ができませんので、ご了承ください。

【発行】「えきねっと」。

東京都杉並区荻窪4丁目8番5号

auPAYカード本人確認を完了してください。 - メッセージ (HTML 形式)

ファイル　メッセージ　実行したい作業を入力してください...

2022/10/15 (土) 11:07

auto <auto@connect.auone.jp>

auPAYカード本人確認を完了してください。

宛先　koga@iij.ad.jp

いつもご利用いただきありがとうございます

・au PAY カード会員サイトでは、セキュリティ保護の観点から緊急の措置として、アカウントメンテナンスに取り組んでいます。

※「24時間以内」に下記のＵＲＬより本人確認を完了してください。
au PAY

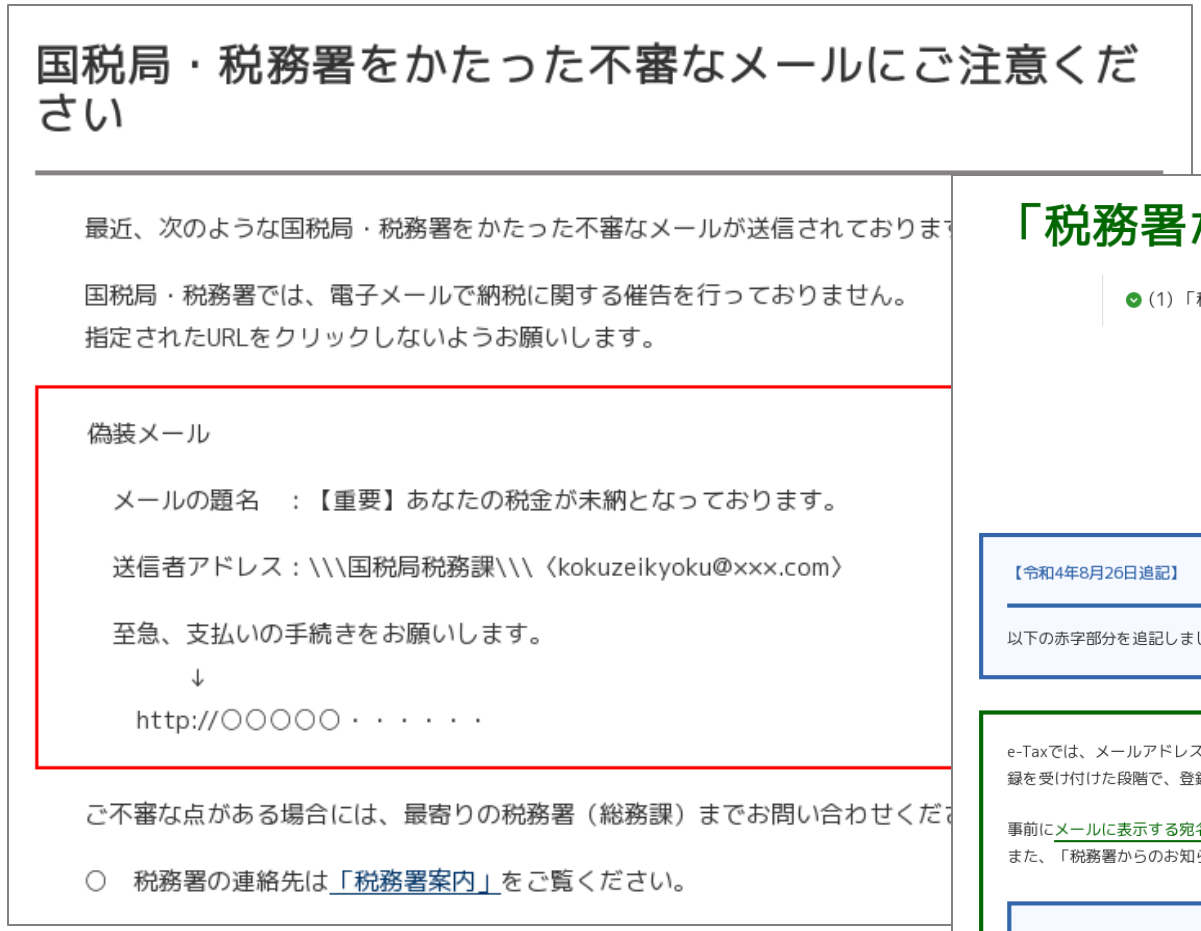
■ご利用確認はこちら

注意事項(必読)
・確認がお済みでない場合、サービスのご利用を停止させていただきますので、ご了承ください。
・お客様にはご不便、ご面倒をお掛けすることもあるかと存じますが、
・何卒ご理解いただきますようお願い申し上げます。

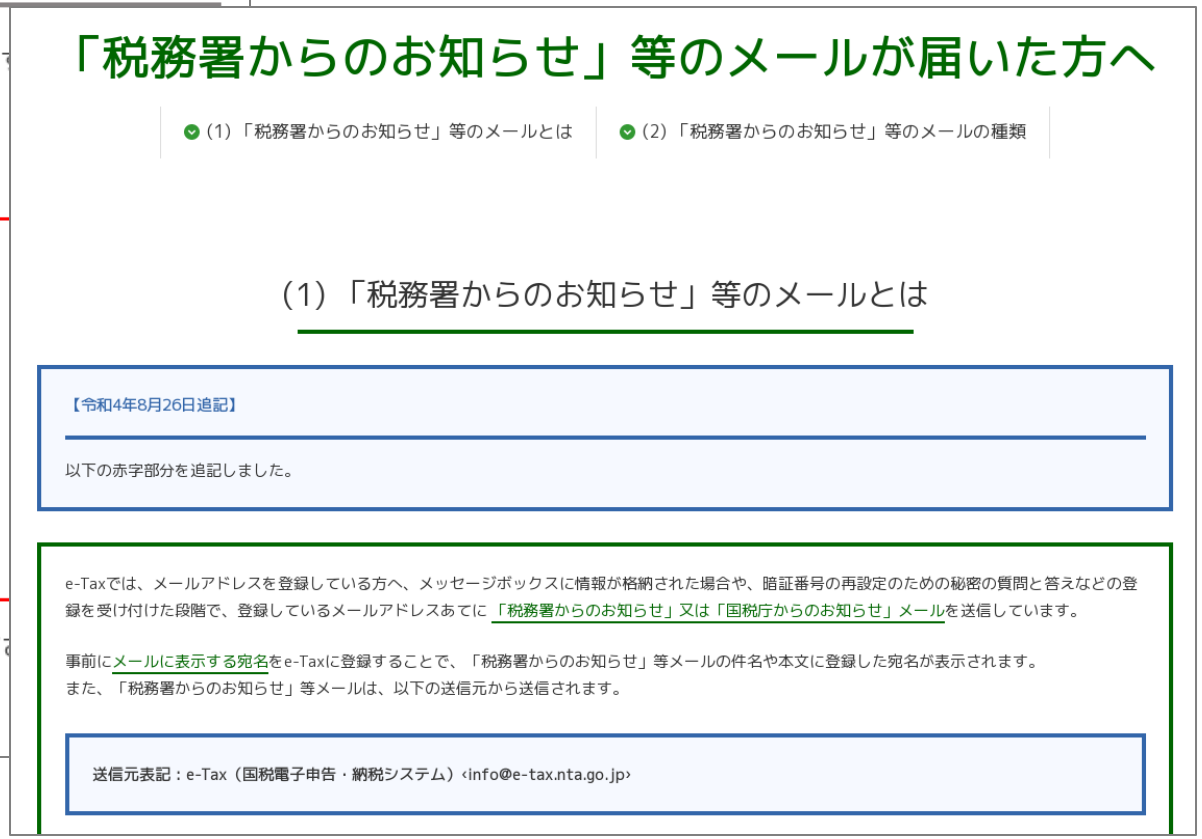
COPYRIGHT ©KDDI CORPORATION ALL RIGHTS RESERVED

よくある被害ケース (2) - 問い合わせコストの増加

「こんなメールを受信したんですけど、なんですか?」といった問い合わせが殺到する



「税務署からのお知らせ」等のメールが届いた方へ
https://www.e-tax.nta.go.jp/topics/topics_oshirase_mail.htm



(国税庁) 不審なメールや電話にご注意ください
https://www.nta.go.jp/information/attention/attention.htm

よくある被害ケース (3) - 風評被害

なりすまされたドメイン名で、特定の主義・主張に利用される

安倍元首相「国葬」中止求める脅迫メール、全国の自治体で確認…同一人物の可能性

2022/07/27 19:43　安倍元首相銃撃

国内の実在するドメイン・個人名を差出人として
某ホスティング事業者から送信されていた

安倍晋三・元首相の「国葬（国葬儀）」を巡り、中止を求める内容の脅迫メールが全国の自治体に送られていることがわかった。自治体は警察と連携し、注意を呼びかけている。

▸山上容

同趣旨の脅迫メールは、大阪市、堺市、京都市、兵庫県姫路市、大津市、奈良県天理市、広島県呉市、鳥取県境港市などで確認されている。メールの差出人が同じ個人名を名乗っているケースがあり、同一人物が送った可能性もある。

る」「国葬会場に濃硫酸をまく」といった文面のメールが届いたと発表した。両市とも地元警察署に通報し、施設の点検や地域の見回りを強化している。

安倍元首相「国葬」中止求める脅迫メール、全国の自治体で確認…同一人物の可能性
https://www.yomiuri.co.jp/national/20220727-OYT1T50264/

対策をしないと出る被害は大きい

「悪」はあなたのドメイン名を狙っている

信用の低下

「このドメインは危ないから見ないでおこう…」

問い合わせ増加

「こんなメールを受信したんですけど…」

風評被害

なりすましたドメイン名で特定の主義・主張をされる

メールを使っていなくても対策は必要!! (使っている場合はもちろん)

セッションの本題

(1) p=none から先に進めない背景とその整理

(2) 転送やメーリングリストとの関係

(3) 検証結果をどのように示し、どのように対応につなげるか

セッションの本題

- **(1) p=none から先に進めない背景とその整理**
- (2) 転送やメーリングリストとの関係
- (3) 検証結果をどのように示し、どのように対応につなげるか

3大 p=none から進めない「ない」要因

1. 動機がない
いま困っていない

2. 怖い・分からない

3. 環境の整理が
追いついていない

3大 p=none から進めない「ない」要因

1. 動機がない
いま困っていない

2. 怖い・分からない

3. 環境の整理が
追いついていない

3大 p=none から進めない「ない」要因

(1)-1. 動機がない、いま困っていない

■ p=none はモニタリングモード

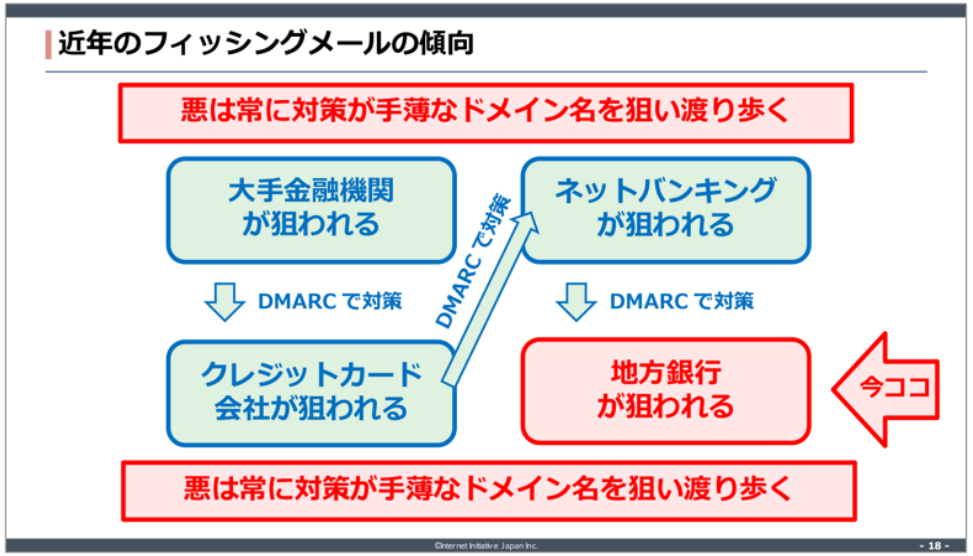
- Google Sender Guidelines が最低限要求しているレベル。
- アライメントを検証できる、DMARC レポートを受信できるようになるので最初の一歩としてよい。
- 「仮に DMARC の検証に失敗(fail)したとしても、ドメインのオーナーは『何もしなくて良い』と宣言している」という意味。(RFC7489 §6.3)

■ 困る前に対策する

- 「悪」は常に対策が手薄なドメイン名を狙い渡り歩く
- 次はあなたのドメイン名の番かもしれない
- **(IIJ 古賀の予想)**
  次、Google は p=quarantine 以上を要求してくる

> p: Requested Mail Receiver policy (plain-text; REQUIRED for policy records). Indicates the policy to be enacted by the Receiver at the request of the Domain Owner. Policy applies to the domain queried and to subdomains, unless subdomain policy is explicitly described using the "sp" tag. This tag is mandatory for policy records only, but not for third-party reporting records (see Section 7.1). Possible values are as follows:
>
> none: The Domain Owner requests no specific action be taken regarding delivery of messages.

RFC7489 Domain-based Message Authentication, Reporting, and Conformance (DMARC)
https://datatracker.ietf.org/doc/html/rfc7489#section-6.3



2023 年度版 迷惑メール動向と対策事例の紹介 (第6回 JPAAWG)
https://meetings.jpaawg.org/6th2023/wp-content/uploads/2023/11/B2-3_koga_2.pdf

3大 p=nor

(1)-1. 動機が

- **p=none はモニ**
  - Google Sende
  - アライメントを
    ようになるので
  - 「仮に DMARC
    のオーナーは
    いう意味。(RF
- **困る前に対策す**
  - 「悪」は常に対
  - 次はあなたのド
  - **(IIJ 古賀の予**
    次、Google は

（公印及び契印省略）

総基用第 76 号
令和７年９月１日

一般社団法人電気通信事業者協会会長　島田　明　殿
一般社団法人テレコムサービス協会会長　是枝　周樹　殿
一般社団法人日本インターネットプロバイダー協会会長　久保　真　殿
一般社団法人日本ケーブルテレビ連盟会長　塩冶　憲司　殿

総務省総合通信基盤局長
湯本　博信

フィッシングメール対策の強化について（要請）

平素より、情報通信行政に御理解と御協力をいただいておりますことに、厚く御礼申し上げます。

フィッシングメール対策について、政府は、「国民を詐欺から守るための総合対策 2.0（令和７年４月 22 日犯罪対策閣僚会議決定）」において、「詐欺メール、詐欺 SMS による被害防止等のための取組」として、「送信ドメイン認証技術（DMARC 等）への更なる対応促進」を掲げているところです。

最近では、実在する証券会社を装ったフィッシングメール等から窃取した顧客情報（ログイン ID やパスワード等）によるインターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が急増しています。

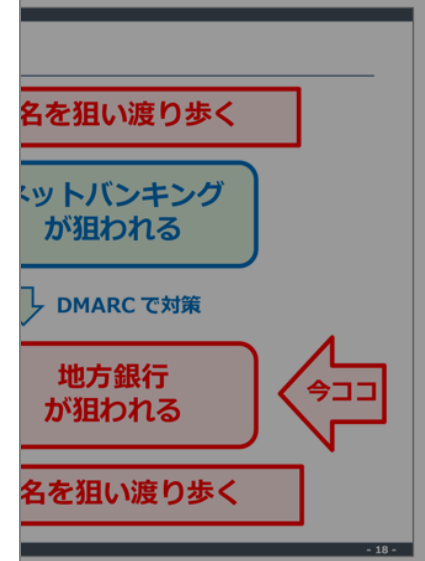
貴法人会員事業者においても、従前よりフィッシングの被害防止に向けて、送信ドメイン認証技術の導入を含め、様々な対策を推進いただいているものと承知しておりますが、生成 AI を用い、自然な日本語を大量に生成できるようになり、これまで以上に精巧なフィッシングメールの送付が容易となっている中、こうしたフィッシングメールへの更なる対策が求められるところです。つきましては、より効果的な対策に取り組んでいただきますよう、下

-text; REQUIRED for policy
e enacted by the Receiver at
licy applies to the domain
domain policy is explicitly
tag is mandatory for policy
y reporting records (see
s follows:

specific action be taken

uthentication, Reporting,

l/rfc7489#section-6.3



例の紹介 (第6回 JPAAWG)
23/wp-
a_2.pdf

3大 p=none から進めない「ない」要因

(1)-1. 動機がない、いま困っていない

■ p=none はモニタリングモード

- Google Sender Guidelines が最低限要求しているレベル。
- アライメントを検証できる、DMARC レポートを受信できるようになるので最初の一歩としてよい。
- 「仮に DMARC の検証に失敗(fail)したとしても、ドメインのオーナーは『何もしなくて良い』と宣言している」という意味。(RFC7489 §6.3)

■ 困る前に対策する

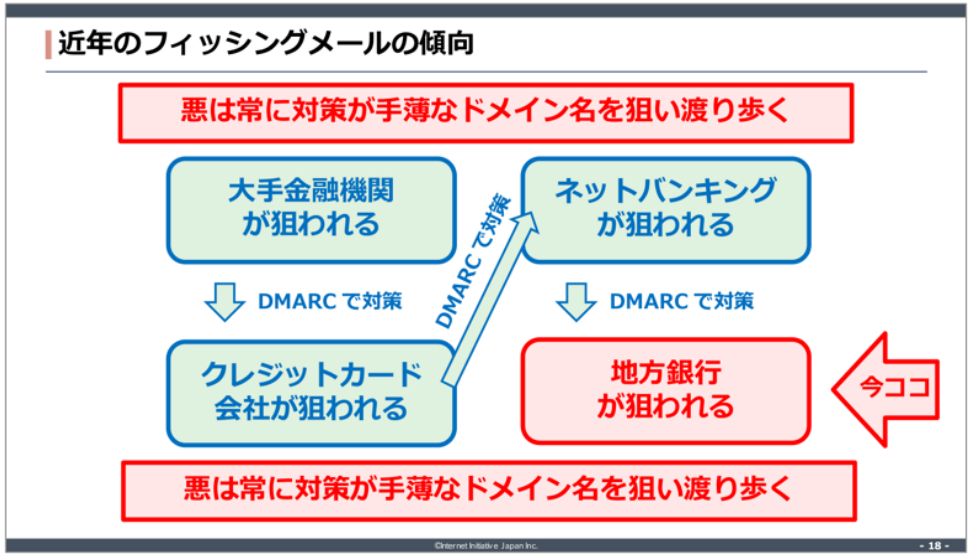
- 「悪」は常に対策が手薄なドメイン名を狙い渡り歩く
- 次はあなたのドメイン名の番かもしれない
- **(IIJ 古賀の予想)**
  次、Google は p=quarantine 以上を要求してくる

■ 総務省がやれと言っている

- 経営層を説得させるのに十分な材料

> p: Requested Mail Receiver policy (plain-text; REQUIRED for policy records). Indicates the policy to be enacted by the Receiver at the request of the Domain Owner. Policy applies to the domain queried and to subdomains, unless subdomain policy is explicitly described using the "sp" tag. This tag is mandatory for policy records only, but not for third-party reporting records (see Section 7.1). Possible values are as follows:
>
> none: The Domain Owner requests no specific action be taken regarding delivery of messages.

RFC7489 Domain-based Message Authentication, Reporting, and Conformance (DMARC)
https://datatracker.ietf.org/doc/html/rfc7489#section-6.3



2023 年度版 迷惑メール動向と対策事例の紹介 (第6回 JPAAWG)
https://meetings.jpaawg.org/6th2023/wp-content/uploads/2023/11/B2-3_koga_2.pdf

3大 p=none から進めない「ない」要因

**1. 動機がない
いま困っていない**

- p=none はモニタリングモード
- 困る前に対策する
- 総務省がやれと言っている

2. 怖い・分からない

3. 環境の整理が
追いついていない

3大 p=none から進めない「ない」要因

1. 動機がない
いま困っていない

- p=none はモニタリングモード
- 困る前に対策する
- 総務省がやれと言っている

2. 怖い・分からない

3. 環境の整理が
追いついていない

IIJ での事例

DMARC 導入 ～ ポリシー強化までの進めかた

DMARC 導入 ～ ポリシー強化(p=reject)までの進めかた

導入して様子見

まずは p=none で
レポート受信

(是正が終わるまでに半年くらい)

- DMARC レポートで自組織の
  流通するメールを透明化。
- 送信元 IP アドレスから
  メールサーバを特定し、
  配送経路をひたすら是正。
- 必要に応じて SPF、DKIM
  の設定状況を確認・是正。

DMARC 導入 ～ ポリシー強化(p=reject)までの進めかた

導入して様子見

まずは p=none で
レポート受信

(是正が終わるまでに半年くらい)

- DMARC レポートで自組織の流通するメールを透明化。
- 送信元 IP アドレスから メールサーバを特定し、配送経路をひたすら是正。
- 必要に応じて SPF、DKIM の設定状況を確認・是正。

2021年 12月変更

p=quarantine に
変更して様子見

(3か月くらい)

- 迷惑メールフォルダや、ごみ箱のある事業者なら受信拒否はされない(はず)。
- IIJ では、目に見える変化や社内問い合わせはなかった。

DMARC 導入 ～ ポリシー強化(p=reject)までの進めかた

導入して様子見

まずは p=none で
レポート受信

(是正が終わるまでに半年くらい)

- DMARC レポートで自組織の流通するメールを透明化。
- 送信元 IP アドレスからメールサーバを特定し、配送経路をひたすら是正。
- 必要に応じて SPF、DKIM の設定状況を確認・是正。

2021年 12月変更

p=quarantine に
変更して様子見

(3か月くらい)

- 迷惑メールフォルダや、ごみ箱のある事業者なら受信拒否はされない(はず)。
- IIJ では、目に見える変化や社内問い合わせはなかった。

2022年 3月変更

p=reject へ

- 思い切って p=reject を宣言。

大きな混乱なし

DMARC 導入 ～ ポリシー強化(p=reject)までの進めかた

IIJ の技報 (IIR Vol.55)、YouTube「IIJ Tech チャンネル」の解説もぜひご覧ください

https://www.iij.ad.jp/dev/report/iir/055.html

https://www.youtube.com/watch?v=3N5G5mP3FxU

(参考)
日本国内 4 キャリアで見る DMARC ポリシー

(参考) 日本国内 4 キャリアの DMARC ポリシー

(参考) 日本国内 4 キャリアの DMARC ポリシー

全社 p=quarantine/reject 設定済み

```
$ dig _dmarc.docomo.ne.jp txt +short
"v=DMARC1; p=quarantine; sp=quarantine;
   pct=100; rua=mailto:docomo00001-ra@dmarc25.jp"
```

p=quarantine (隔離)

```
$ dig _dmarc.ezweb.ne.jp txt +short
"v=DMARC1; p=reject;
   rua=mailto:kddi00001-ra@dmarc25.jp,
   mailto:report_dmarc_rua.ez@ezweb.ne.jp"
```

p=reject (拒否)

```
$ dig _dmarc.i.softbank.jp txt +short
"v=DMARC1; p=quarantine;
   rua=mailto:softbankmail00001-ra@dmarc25.jp"
```

p=quarantine (隔離)

```
$ dig _dmarc.rakumail.jp txt +short
"v=DMARC1; p=reject;
   rua=mailto:dmarc-report-a@rx.rakuten.co.jp"
```

p=reject (拒否)

NTT ドコモさんの見解 2024

次のSTEPであるなりすましメールの排除へ

p=quarantine/rejectへ進む時です

	具体例	第三者チェック	なりすましメールの排除	DMARC ※header fromの認証	SPF ※envelope fromの認証
	ドコモメール公式アカウント	○	○		
	BIMI	○	○		
新しい基準	p=quarantine/reject	×	○		
	p=none	×	×		
古い基準	DMARC未導入	×	×		
	認証失敗	×	×		

JPAAWG

第7回 JPAAWG General Meeting
https://meetings.jpaawg.org/program/

まとめ

・DMARCの**p=noneは順調**に普及！

・**次はp=quarantine/reject**を導入すべき！

・並行して、**正規メールのPR**も！

JPAAWG

16

KDDI さんの見解 2024

第7回 JPAAWG General Meeting
https://meetings.jpaawg.org/program/

auが発信するメールへのDMARC対応

au系ドメイン：通信／金融／各種サービスのサブドメイン多数

2023/10 全社横断でDMARC(p=reject)推進で方針決定
2024/02 p=reject化完遂へ

DMARC導入の背景と課題

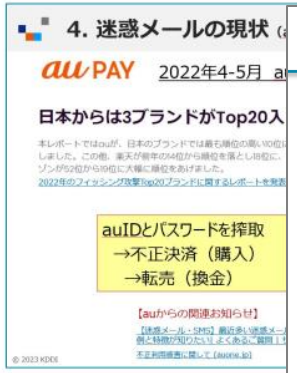
DMARCレポート分析	お客様からの迷惑メール情報分析
詐称ドメイン多数・・・	DMARCすり抜けメール増加傾向

DMARC(p=reject)／BIMI導入

au主要ドメイン：au.com/ezweb.ne.jp/auone.jp
サブドメインを含め、全ドメインでDMARC reject化完了！

JPAAWG

6th General-Meeting資料抜粋



金融やEC系業界等を中
当社のau PAYなども

まとめ

・キャリアメールは国内1億人のDMARC対応メール

・DMARC みんなでReject 目指しましょう！（字余り

・Reject化は（少し大変だけど）怖くない！
結構あっさり実現できます！

・Reject化終われば次はBIMIで正規メールアピールを！

by KDDI
（懐かしい

JPAAWG

28

ソフトバンクさんの見解 2024

p＝reject

絶大な効果あり！！

DMARCポリシーをrejectに変更した
なりすましメールのブロック件数急増
さらに、**なりすましメール通数自体が減**

JPAAWG

第7回 JPAAWG General Meeting
https://meetings.jpaawg.org/program/

まとめ

①なりすましドメインとして実在するサービスのドメインが悪用されている

・金融、宅配、決済可能なキャリアや企業のドメインが悪用されていたが、
フリマ系、某大手倉庫店のドメインを悪用するパターンも増加傾向

②キャリアでDMARCフィルタ導入

・国内3キャリアはデフォルトON！1億ユーザーが適用中！！

・DMARCポリシーを「reject」に変更するだけで大きな効果

ここ重要！！

③転送メールサービスはARC署名で対策！？

・受信側ARCに対応する企業は増えるのか？

JPAAWG

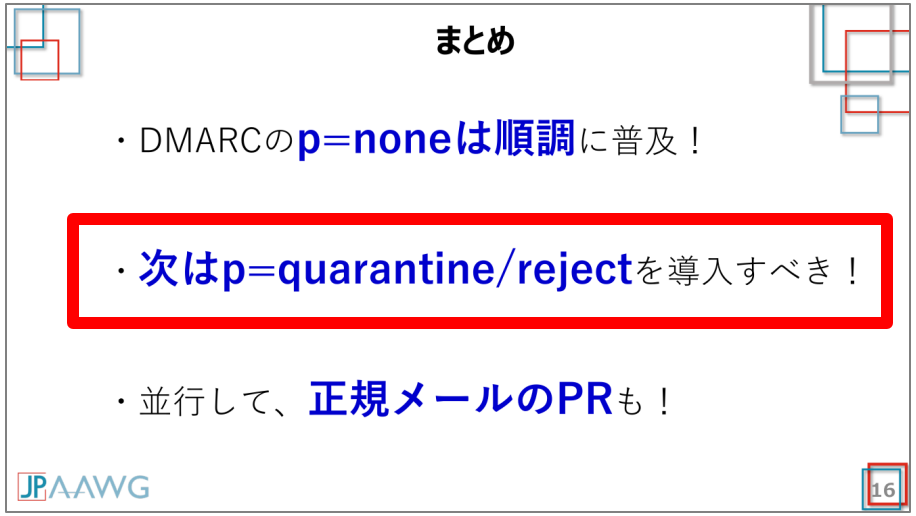
38

(IIJ 古賀の予想2) DMARC p=reject の時代がきます

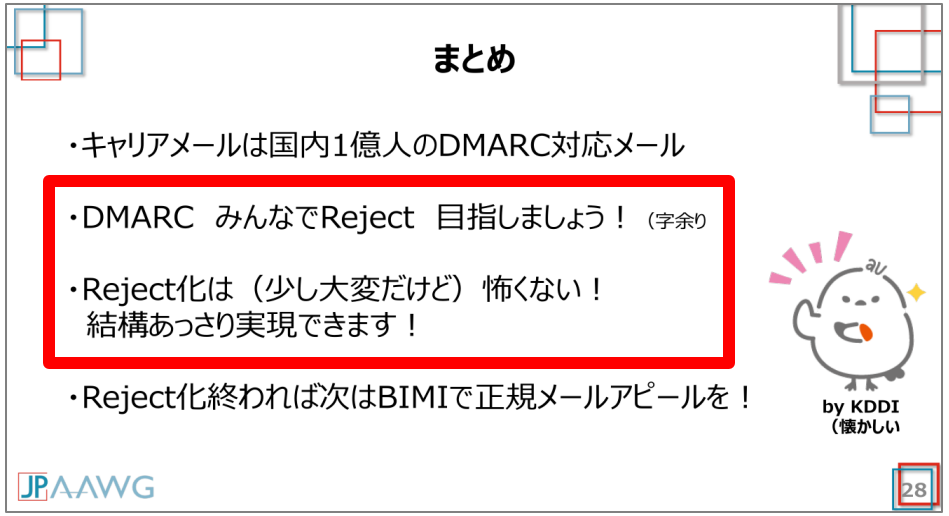
国内 3キャリアが声を揃えて p=reject 共同声明

第7回 JPAAWG General Meeting
https://meetings.jpaawg.org/program/

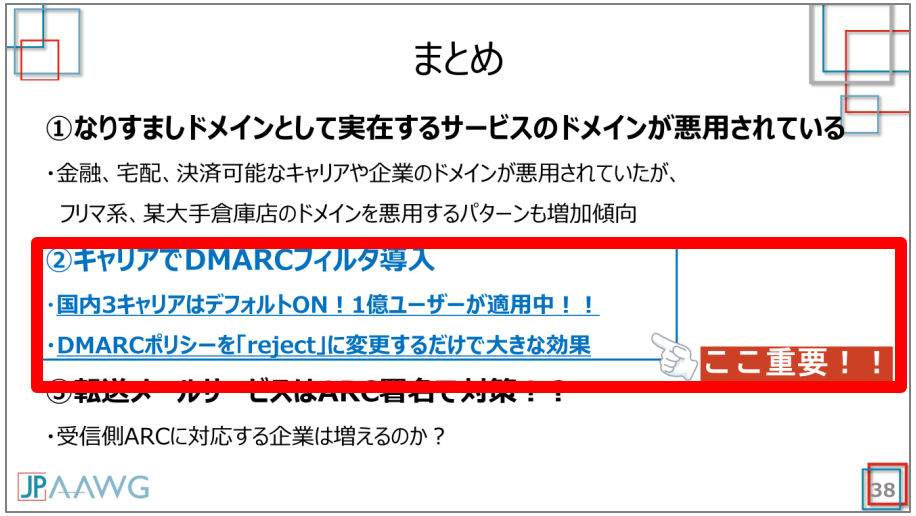
NTT ドコモ



KDDI



ソフトバンク



p=reject にしないと
届かない時代へ突入間近
(準備がまだなら急いで)

Yahoo! Japan も追従

Yahoo!メール
ドメイン認証技術「DMARC」について

DMARCとは

DMARC（Domain-based Message Authentication, Reporting, and Conformance）とは、なりすましメール対策の技術で、電子メールの送信元のドメインを認証する技術の一つです。
Yahoo!メールでは以前からSPF（※1）、DKIM（※2）というなりすましメール対策技術を導入しています。
これらがYahoo!メール側でなりすましを判断する技術であるのに対して、2020年3月より順次導入されるDMARCは「なりすまされたメールの扱い（ブロック、迷惑メール判定など）を設定」することで、ユーザーの皆様になりすまされたメールが届かないようにするための技術となります。
これによって今まで以上になりすましメール対策が強化され、より安心・安全なメールとしてお使いいただけるようになります。

メール送信事業者様へ

DMARC導入によって貴社になりすましたメールを自発的に防ぐことができるようになります。
※DMARCレポートの送信については、現在Yahoo!メールでは対応しておりません。

DMARCの仕組み

DNSサーバ

```
$ dig _dmarc.yahoo.co.jp txt +short
"v=DMARC1; p=quarantine;
   rua=mailto:ymail_dmarc_report@yahoo.co.jp"
```

Yahoo!メール ドメイン認証技術「DMARC」について
https://mail.yahoo.co.jp/antispam/dmarc.html

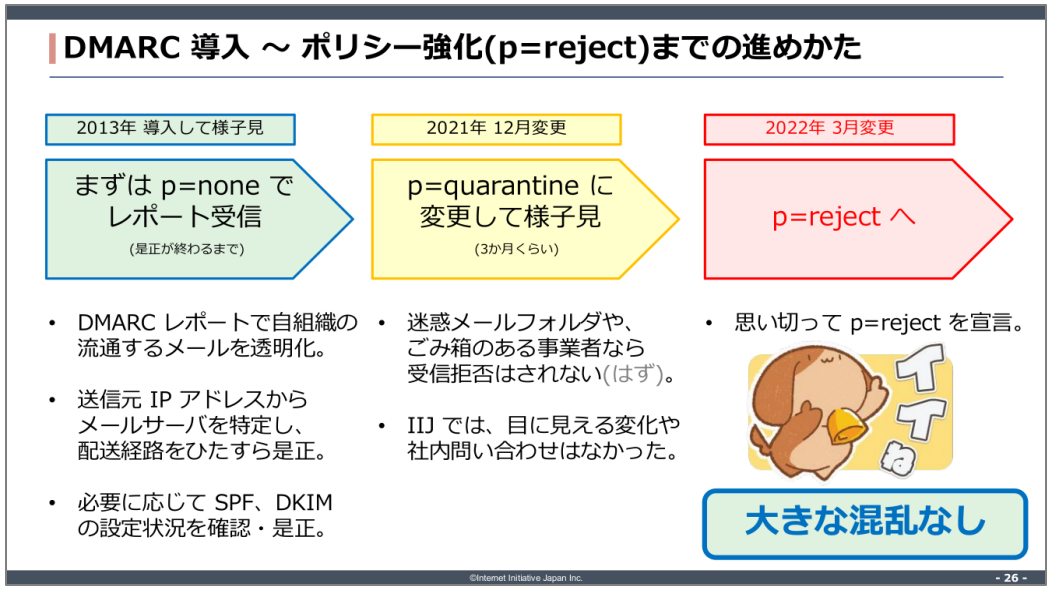
3大 p=none から進めない「ない」要因

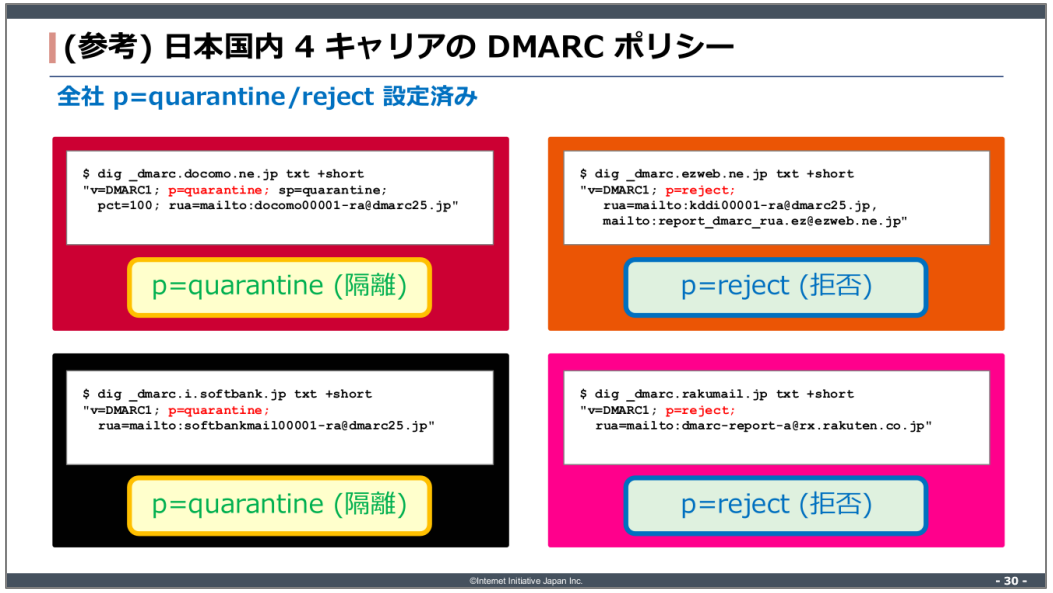
(1)-2. 怖い、分からない

- **手順・前例あり、近道はないので地道に対策する**
  - DMARC レポートを見れば、どのメールが影響を受けそうか洗い出せるのが DMARC の良いところ。
  - 一度ポリシーを強化したあと、問題を発見したらまた戻せば良い。少しずつでいい。

- **国内 4 キャリアも対策済み**
  - **p=reject 案外怖くない**
  - 「もう、周りのみんなはやっている」

- **それでも不安なことは Internet Week で解決！**
  - このあとのディスカッションでお困りごとの相談、解決に向けた情報共有をしていきましょう！





3大 p=none から進めない「ない」要因

1. 動機がない
いま困っていない

- p=none はモニタリングモード
- 困る前に対策する
- 総務省がやれと言っている

2. 怖い・分からない

- 手順・前例あり、地道に対策する
- 国内 4 キャリア対策済み
- p=reject 案外怖くない

3. 環境の整理が
追いついていない

3大 p=none から進めない「ない」要因

**1. 動機がない
いま困っていない**

- p=none はモニタリングモード
- 困る前に対策する
- 総務省がやれと言っている

2. 怖い・分からない

- 手順・前例あり、地道に対策する
- 国内 4 キャリア対策済み
- p=reject 案外怖くない

**3. 環境の整理が
追いついていない**

3大 p=none から進めない「ない」要因

(1)-3. 環境の整理が追いついていない

3大 p=none から進めない「ない」要因

(1)-3. 環境の整理が追いついていない

3大 p=none から進めない「ない」要因

(1)-3. 環境の整理が追いついていない

■ 優先順位をつける

- 限られたリソース・時間・予算の中でどこまで投資できるか分かる。
- 経営リスクがどこにあるのか特定できる。
- 「千里の道も一歩から」

■ アウトソースするのも選択肢の一つ

- レガシーなシステムから脱却をする良い機会と捉える。
- 現状のインフラに機能がない場合は、乗り換えの検討を開始する。

■ 諦めの「軸」を持つ

- ときには DMARC レポートを見ても特定できないものも出てくる。思い切って諦めることも肝心。
- 優先度の低いシステムの対応に引きづられたり、時間を掛けすぎてしまったりして、顧客やユーザを危険に晒し続けてはいけない。
- (例)「お金の流れと関係ないものは諦める」
  → お金の流れと関係あるものは、経理・財務部門に聞けば分かる。
  → お金の流れと関係ないものは、失敗してもダメージは小さい。

3大 p=none から進めない「ない」要因

1. 動機がない いま困っていない

- p=none はモニタリングモード
- 困る前に対策する
- 総務省がやれと言っている

2. 怖い・分からない

- 手順・前例あり、地道に対策する
- 国内 4 キャリア対策済み
- p=reject 案外怖くない

3. 環境の整理が 追いついていない

- 優先順位をつける
- アウトソースの選択肢
- 諦めの「軸」を持つ

セッションの本題

(1) p=none から先に進めない背景とその整理

▶ **(2) 転送やメーリングリストとの関係**

(3) 検証結果をどのように示し、どのように対応につなげるか

DMARC とメーリングリスト

✕ SPF が使えない

- 差出人サーバと受信者の間にメーリングリストサーバが入る
- IP アドレスに依存しているため SPF での評価ができない

✕ DKIM の検証ができない

- 件名にリスト名やシーケンス番号を挿入
- 本文の末尾に署名を挿入するなどで本文が書き換わる

送信ドメイン認証の最後の砦

DMARC とメーリングリスト - 回避策 (1)

メーリングリストサーバで From ヘッダを書き換える

送信前

```
MAIL FROM: <koga@iij.ad.jp>
RCPT TO: <list@example.jp>

From: Isamu Koga <koga@iij.ad.jp>
To: list@example.jp
Subject: Hello!
```

メーリングリスト通過後

```
MAIL FROM: <owner-list@example.jp>
RCPT TO: <koga@iij.ad.jp>

From: Isamu Koga <list@example.jp>
To: list@example.jp
Cc: Isamu Koga <koga@iij.ad.jp>
Subject: [List] Hello!
```

SPF の
アライメント一致

✔ **DMARC に完全対応**
差出人情報を Cc や Reply-To に残す方法もある

✘ **From アドレスが全員同じ**
Display-name を削られると誰が誰だか分からない

dmarc-discuss, JANOG はこの方式で回避、最新の Mailman3 にも本機能あり

DMARC とメーリングリスト - 回避策 (2)

メーリングリストのドメイン名を分離してスコープを狭める

送信前

```
MAIL FROM: <koga@iij.ad.jp>
RCPT TO: <list@ml.example.jp>

From: Isamu Koga <koga@iij.ad.jp>
To: list@ml.example.jp
Subject: Hello!
```

メーリングリスト通過後

```
MAIL FROM: <owner-list@ml.example.jp>
RCPT TO: <koga@iij.ad.jp>

From: Isamu Koga <koga@iij.ad.jp>
To: list@example.jp
Subject: [List] Hello!
```

アライメント
不一致

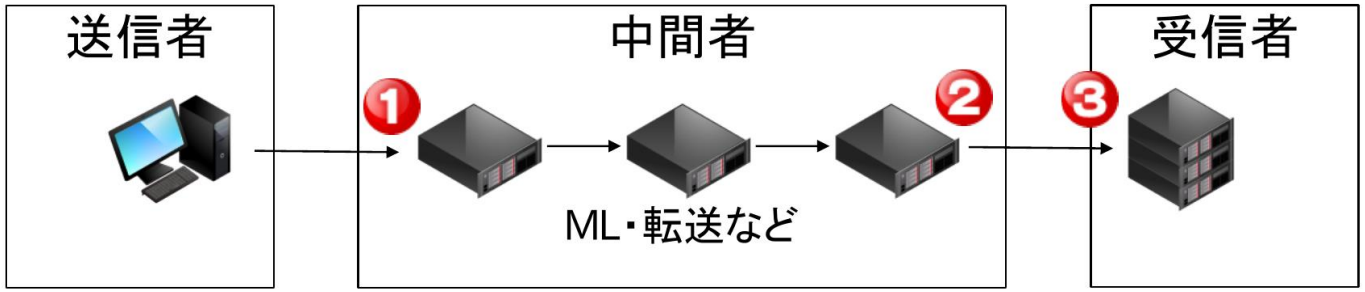
✔ メーリングリストサーバに手を入れなくて良い
DMARC の対応スコープから外せる

✖ メーリングリストのアドレスを変更する必要がある
アライメントの不一致で DMARC は fail し続ける

米国 DHS はこの方式でを回避するよう各省庁に勧めた (と話していた)

DMARC とメーリングリスト - 回避策 (3)

ARC – Authenticated Received Chain (RFC 8617) に対応する



差出人から最初に受け取った際の
認証結果をリレーする仕組み

- ❷ で ❶ の認証結果を保存し、署名をする
- ❸ は ❷ が署名した ❶ の認証検証を参照できる

送信ドメイン認証 導入指南 2018
(Internet Week 2017)
https://www.nic.ad.jp/ja/materials/iw/2017/proceedings/s12/s12-suzuki.pdf

✔ **DKIM も対応可能 (検証できるのは直前の署名のみ)**
最大 50ホップまで対応

✘ **通過するサーバすべてが ARC 対応する必要あり**
ホップする中間者がすべて信頼できることが前提

最新の Mailman3 で対応済み

(参考) GNOME メーリングリスト終了のお知らせ

The Register

The GNOME Project is closing all its mailing lists

Everyone has to join Discourse··· although you can still participate via email

Liam Proven Thu 27 Oct 2022 // 11:33 UTC

The GNOME Project is preparing to shut down its mailing lists due to problems maintaining the project's GNU Mailman instance - which relies on Python 2 - and a lack of moderators.

The community's leaders maintain a substantial selection of mailing lists, hosted via the GNU Project's Mailman tool. It also hosts its own instance of the Discourse web forum tool, notably also used by Canonical to host the official Ubuntu forums.

That's going to change, and very soon: at the end of this month. Announcements on several of the lists, such as here on the list for the Evolution email client, state that the lists are closing down, and discussions must move to Discourse.

Former GNOME Project Executive Director Neil McGovern told *The Reg*:

The GNOME Project is closing all its mailing lists
https://www.theregister.com/2022/10/27/the_gnome_project_is_closing/

セッションの本題

(1) p=none から先に進めない背景とその整理

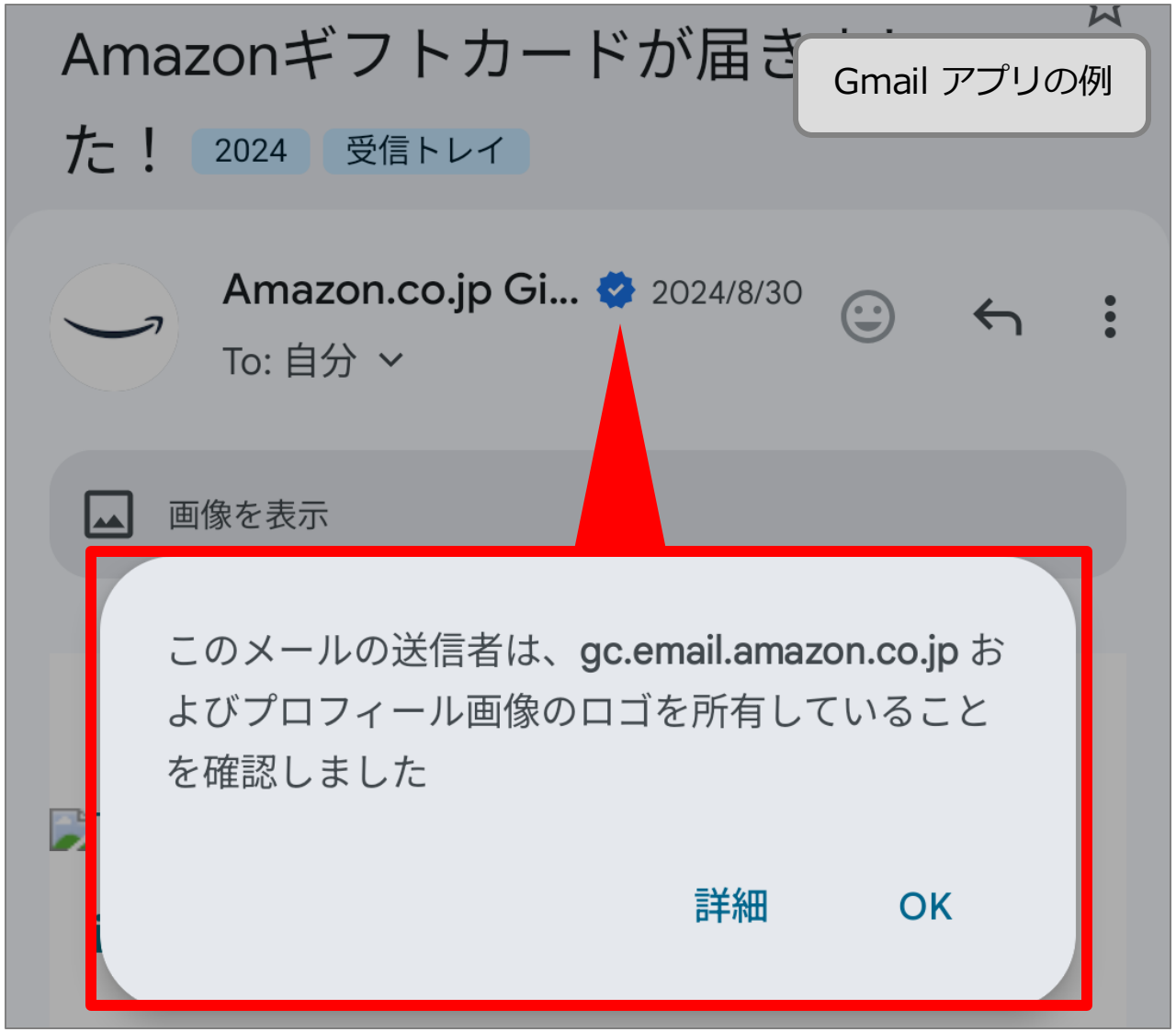
(2) 転送やメーリングリストとの関係

▶ **(3) 検証結果をどのように示し、どのように対応につなげるか**

← このマークが超重要 (Gmail の場合)

BIMI(VMC)認証されたことを示す証拠

- **マークの示し方は各社それぞれ**
  - 利用しているアプリ・Web メールの案内を参照
  - UI/UX 設計者は、非認証メールと誤認しないよう注意しながら、利用者の学習コストが小さくなるようにする
- **Gmail の場合、アバターとの違いに注意**
  - アバターの場合は マークがない
  - ただし CMC 証明書で BIMI 認証された場合、ロゴは表示されるが マークがない
  - (このあたりがちょっとややこしい)
- **やはり DMARC p=reject が最重要**
  - なりすましメールを受信者に届かせない世界が最も大切



※ VMC = Verified Mark Certificate (厳しい認証条件あり)
※ CMC = Common Mark Certificate (VMC より取りやすい認証条件)

まとめ

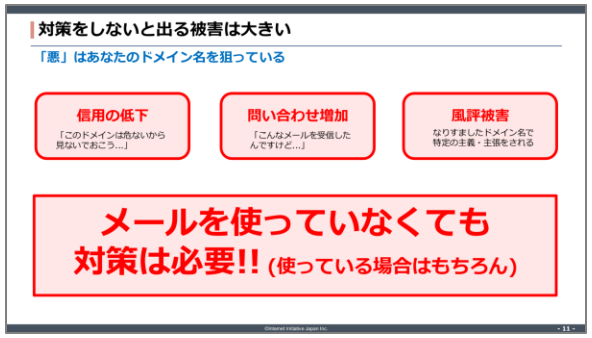
まとめ

今こそ DMARC ポリシーを強化して、もう一段階進めるとき

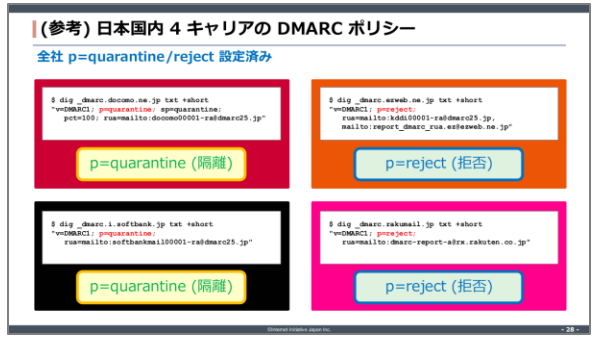
フィッシングメール対策が国策として急務

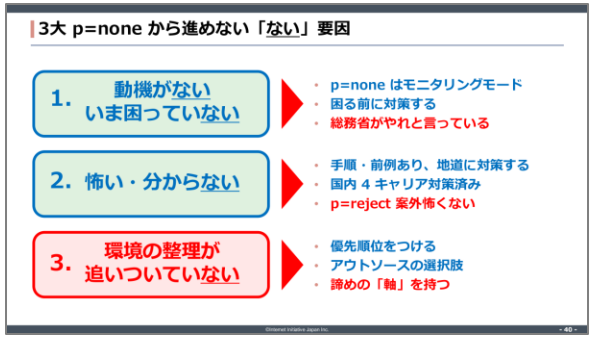
p=reject 意外に怖くない

■ 総務省からも要請されている、被害は甚大



■ 大手キャリアも対応済み、世の中は p=reject へ





補足資料

時間の都合で割愛した内容

メールを送らない/受け取らない宣言・Null MX

「このドメイン名でメールは送受信しないので、受信したら偽物です」という宣言

```
example.jp.              IN   MX    0 .
example.jp.              IN   TXT   "v=spf1 -all"
_dmarc.example.jp.       IN   TXT   "v=DMARC1; p=reject"
```

DMARC は組織ドメインに書けば自動的にサブドメインにも適用される!!

今すぐ書きましょう!!

- メールを使っていないドメイン
- 利用を終えたドメイン

※ rua や ruf も書けば、そのドメインを使ったなりすましメールが出ていないか監視できる。

RFC7505 - A "Null MX" No Service Resource Record for Domains That Accept No Mail
https://www.rfc-editor.org/rfc/rfc7505

DMARC (送信ドメイン認証) で自社ドメイン名のブランドを守る

送信ドメイン認証とは

△ 受信者がなりすましメールを見分けるための技術

◎ 送信者がドメイン名のブランドを守るための技術

- DMARC で第三者による悪用(窃用)からドメイン名を保護する
- 悪の組織が取得したドメインも DMARC 対応はしてくる

(悪の視点) 送信ドメイン認証に失敗するドメイン名はなりすます価値がない

IIJ Internet Initiative Japan

Lead Initiative

日本のインターネットは1992年、IIJとともにはじまりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ――IIJはいつもはじまりであり、未来です。

Ongoing Innovation