IIJ Internet Initiative Japan

ブランドを守るために必要な送信ドメイン認証

2022/11/29

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部　運用技術課
課長　古賀 勇

Ongoing Innovation

想定所要時間 40分

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部 運用技術課 課長
(兼) 社長室

Power Automate エバンジェリスト (自称)

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・情報発信 (エンジニアブログ・技報)

WIDE Project

M3AAWG

openSUSE (趣味)

先日、こんなことがありました

家族で夕飯を食べていたときの会話

アニメーション製作会社がサイバー攻撃受けたんだって?

ITmedia NEWS > 速報 > 「プリキュア」新作放送を約1カ月延期　東映アニメ...

「プリキュア」新作放送を約1カ月延期　東映アニメーションへの不正アクセスで

2022年03月14日 11時51分 公開　[ITmedia]

印刷　1480　Share　B!　48　1

ABCテレビは3月13日、アニメ「デリシャスパーティプリキュア」6話以降の放送が4月10日以降になると明らかにした。アニメを制作している東映アニメーションが第三者による不正アクセスを受けた影響で作品の制作が困難な状態になった。

ABCテレビの発表

「プリキュア」新作放送を約1カ月延期　東映アニメーションへの不正アクセスで
https://www.itmedia.co.jp/news/articles/2203/14/news083.html

先日、こんなことがありました

家族で夕飯を食べていたときの会話

アニメーション製作会社がサイバー攻撃受けたんだって?


ITmedia NEWS > 速報 > 「プリキュア」新作放送を約1カ月延期　東映アニメ...

「プリキュア」新作放送を約1カ月延期　東映アニメーションへの不正アクセスで

2022年03月14日 11時51分 公開　[ITmedia]

印刷　1480　Share　B!　48　1

ABCテレビは3月13日、アニメ「デリシャスパーティプリキュア」6話以降の放送が4月10日以降になると明らかにした。アニメを制作している東映アニメーションが第三者による不正アクセスを受けた影響で作品の制作が困難な状態になった。

ABCテレビの発表

さいばーこうげき? ってなに?

子

「プリキュア」新作放送を約1カ月延期　東映アニメーションへの不正アクセスで
https://www.itmedia.co.jp/news/articles/2203/14/news083.html

先日、こんなことがありました

家族で夕飯を食べていたときの会話

アニメーション製作会社がサイバー攻撃受けたんだって?

さいばーこうげき? ってなに?

子

悪い人がインターネットを使って、会社の中に入ってウイルスをばらまいたり、パソコンを使えなくしちゃうんだよ

先日、こんなことがありました

家族で夕飯を食べていたときの会話

アニメーション製作会社がサイバー攻撃受けたんだって?

さいばーこうげき? ってなに?

子

悪い人がインターネットを使って、会社の中に入ってウイルスをばらまいたり、パソコンを使えなくしちゃうんだよ

プリキュアの制作止まって、放送できなくなっちゃうかもね

妻

先日、こんなことがありました

家族で夕飯を食べていたときの会話

アニメーション製作会社がサイバー攻撃受けたんだって?

さいばーこうげき? ってなに?　子

悪い人がインターネットを使って、会社の中に入ってウイルスをばらまいたり、パソコンを使えなくしちゃうんだよ

プリキュアの制作止まって、放送できなくなっちゃうかもね　妻

え、ちょっとパパ！ 何とかしてよ！ **インターネットの会社でしょ!?**　子

先日、こんなことがありました

家族で夕飯を食べていたときの会話

アニメーション製作会社がサイバー攻撃受けたんだって?

さいばーこうげき? ってなに?　子

悪い人がインターネットを使って、会社の中に入ってウイルスをばらまいたり、パソコンを使えなくしちゃうんだよ

プリキュアの制作止まって、放送できなくなっちゃうかもね　妻

え、ちょっとパパ！ 何とかしてよ！ **インターネットの会社でしょ!?**　子

なぜメールなのか

2分で復習します

なぜメールなのか（復習）

特定企業に依存しないインフラ

- SNS やチャットは特定企業が全情報をコントロール
- Twitter, Facebook, Slack, Teams, ...

なぜメールなのか（復習）

特定企業に依存しないインフラ

- SNS やチャットは特定企業が全情報をコントロール
- Twitter, Facebook, Slack, Teams, ...

オープン

- 通信のプロトコルは RFC で公開
- 誰でも参入できる

なぜメールなのか（復習）

特定企業に依存しないインフラ

- SNS やチャットは特定企業が全情報をコントロール
- Twitter, Facebook, Slack, Teams, ...

オープン

- 通信のプロトコルは RFC で公開
- 誰でも参入できる

フラット

- 誰もが平等
- 資本や立場、政治的な事情で不利な扱いをされたりしない

なぜメールなのか（復習）

特定企業に依存しないインフラ

オープン

フラット

個人を識別するためのID

企業(組織)間のコミュニケーションツールとして依然重要なインフラ

なぜメールなのか（復習）

なので、

ちゃんとしましょう

（悪の組織に狙われないように）

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

国税局・税務署をかたった不審なメールにご注意ください

最近、次のような国税局・税務署をかたった不審なメールが送信されております

国税局・税務署では、電子メールで納税に関する催告を行っておりません。
指定されたURLをクリックしないようお願いします。

偽装メール

メールの題名　：【重要】あなたの税金が未納となっております。

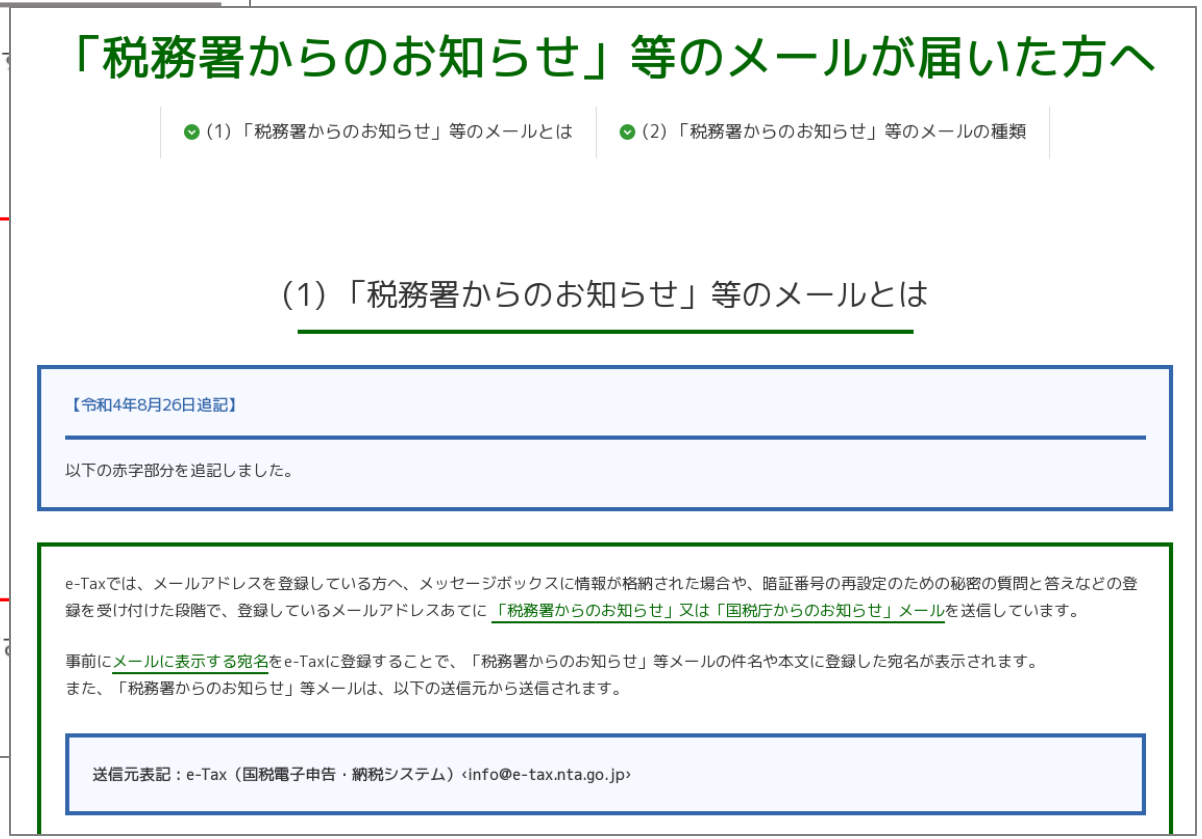
送信者アドレス：\\\国税局税務課\\\〈kokuzeikyoku@xxx.com〉

至急、支払いの手続きをお願いします。
↓
http://○○○○○・・・・・・

ご不審な点がある場合には、最寄りの税務署（総務課）までお問い合わせくだ

○　税務署の連絡先は「税務署案内」をご覧ください。

「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



国税局・税務署をかたった不審なメールにご注意ください
https://www.nta.go.jp/about/organization/kantoshinetsu/topics/nise/01.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

国内の実在する組織のドメインを差出人として
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。

▸山上容疑者の鑑定留置延長、取り消しを求める準抗告を申し立て…安倍元首相銃撃事件

滋賀県栗東市と愛媛県今治市は２７日、２５日に「国葬を中止しなければ、全国の子供を誘拐する」「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」は使われているドメインを狙っている

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)

Domain-based **M**essage **A**uthentication, **R**eporting, and **C**onformance (DMARC)
https://datatracker.ietf.org/doc/html/rfc7489

送信ドメイン認証 (DMARC)

なりすましを防ぎ、ブランドを守るための技術

Domain-based **M**essage **A**uthentication, **R**eporting, and **C**onformance (DMARC)
https://datatracker.ietf.org/doc/html/rfc7489

STEP 1

必ず理解して欲しい DMARC

- なぜ DMARC か
- ここがすごいぞ DMARC
- SPF、DKIM と DMARC の関係
- まず DMARC 対応するには
- 事例で見る DMARC レコード

なぜ DMARC か (SPF, DKIM の課題)

差出人側 (ドメイン所有者)

メールの出口の洗い出し、DKIM の実装が大変

サブドメインが多くて対応しきれない

SPF, DKIM の認証に fail (失敗) したメールを受信者にどう扱ってほしいのか伝えられない

SPF, DKIM の効果測定ができない

受信者側

SPF, DKIM の認証に pass(成功) したとして
そのメールが正規なものかどうかが分からない

(例) example.com.　IN TXT "v=spf1 +all"

```
Envelope From: badguy@example.com
Header From: Isamu Koga <koga@iij.ad.jp>
```

メーラーで見えるのはこの部分 ▲

SPF, DKIM の認証に fail (失敗) したメールを送信者がどう扱って欲しいと思っているのか分からない

ここがすごいぞ DMARC

差出人側 (ドメイン所有者)

受信者側から SPF, DKIM の結果を**レポートしてくれる** (仕組みがある)

DMARC レコードを書けば**サブドメイン全てに適用する**ことができる

差出人ドメインの所有者が、DMARC の認証に fail (失敗) したメールを「どう扱って欲しいか」**明示できる**

SPF か DKIM のどちらかに対応すれば DMARC 対応できる

受信者側

DMARC のポリシーに従ってメールをフィルタすればなりすましメールを排除し、正当なメールを受け取りやすくなる

アライメント(後述)の概念により、確かにそのドメインの管理するところから送信されていることを確信できる

SPF, DKIM と DMARC の関係

SPF

DKIM

◀ 認証ロジックの話

DMARC

◀ ポリシーの話

SPF > DMARC >>>>> DKIM

絶対やる　　絶対やる　　必要に応じてやる

SPF → DKIM → DMARC では(必ずしも)ない

まず (最低限) DMARC 対応するには

Header From のドメインの _dmarc に書く

```
"v=DMARC1; p=none"
```

事例サンプル (example.jp の場合):

```
_dmarc.example.jp.   IN   TXT    "v=DMARC1; p=none"
```

v=DMARC1	example.jp は DMARC に対応
p=none	DMARC の認証に失敗(fail)したときは何もしなくてよい

※ "v" や "p" を「タグ」と呼ぶ。DMARC に必須なのは v と p のみ。

上記 DMARC レコードを書いても悪影響はない (と考えていい)

事例で見る DMARC レコード (Amazon)

```
_dmarc.amazon.com.      IN    TXT    "v=DMARC1; p=quarantine; pct=100;
rua=mailto:report@dmarc.amazon.com; ruf=mailto:report@dmarc.amazon.com"
```
（実際は一行）

v=DMARC1	amazon.com は DMARC に対応 • 必ず先頭に書く
p=quarantine	DMARC の認証に失敗(fail)したときは隔離(quarantine)してほしい • p= は none, quarantine, reject のいずれかのみ
pct=100	ポリシー(p=)のアクションを適用する確率は 100% • pct= は 0～100 の整数値 (省略すると 100)
rua=mailto:(略)	集計レポートは report@dmarc.amazon.com に送ってほしい • 宛先は "," で区切って複数指定できる
ruf=mailto:(略)	DMARC 認証に失敗したメールのコピーを report@dmarc.amazon.com に送ってほしい • 宛先は "," で区切って複数指定できる

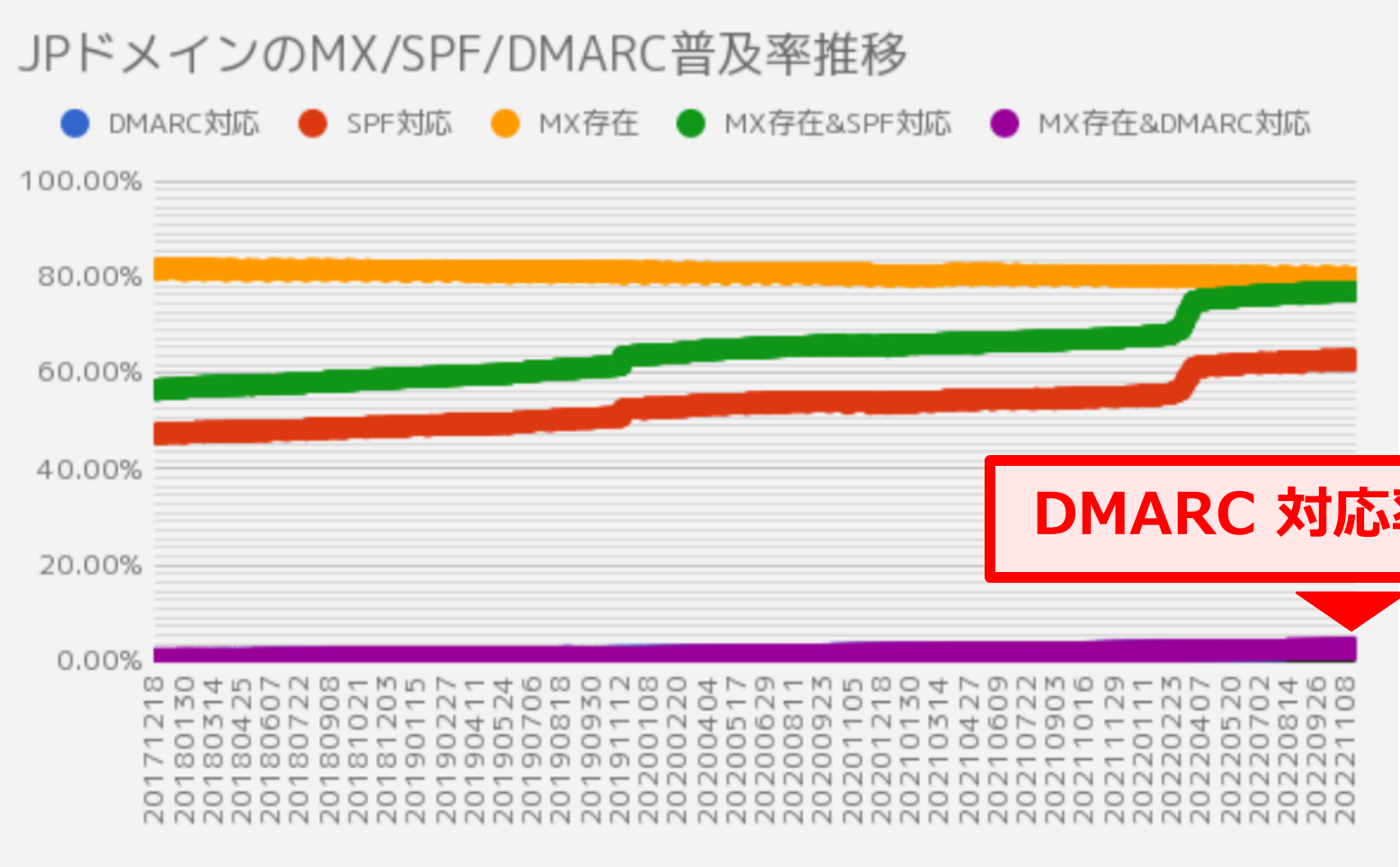
- 受信者のアクションを定義できて
- なりすまし対策もできて
- レポートもタダでもらえる

DMARC 最高すぎでは?

なのに...

JP ドメインの DMARC 普及率

いつ悪の組織に狙われてもおかしくない状況



DMARC 対応率 2.67%

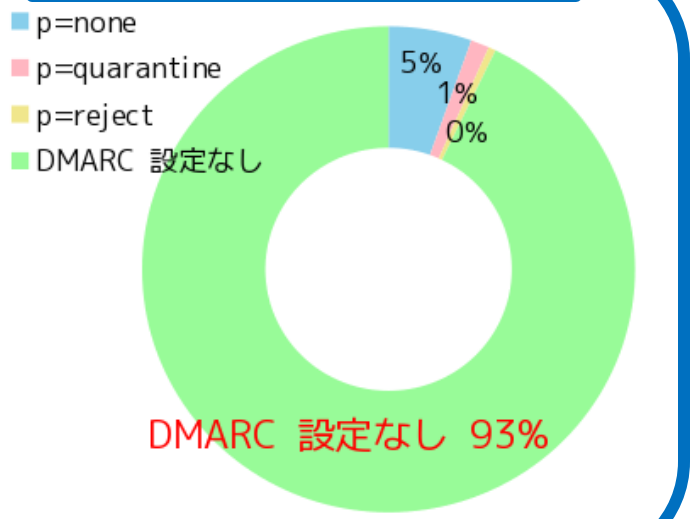
※ 2022/11/20 時点

DMARC adoption statistics of JP domains
https://kitazaki.github.io/dmarc/

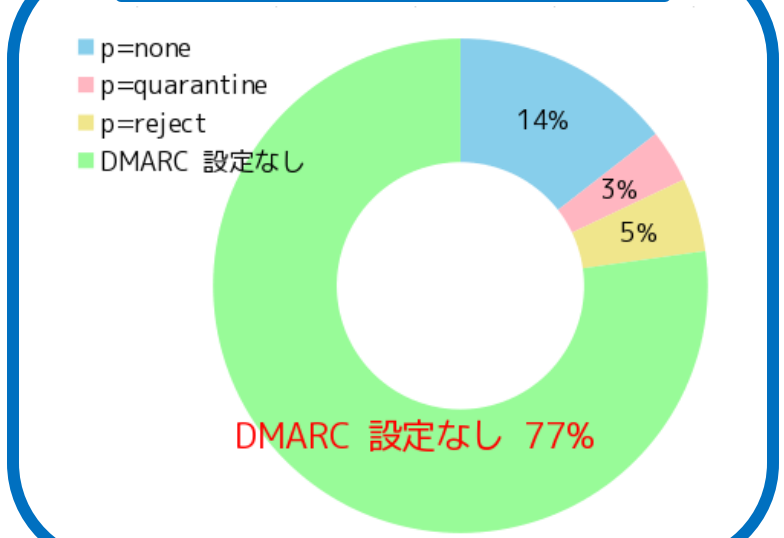
日本 属性別ドメインの DMARC 対応状況

いつ悪の組織に狙われてもおかしくない状況

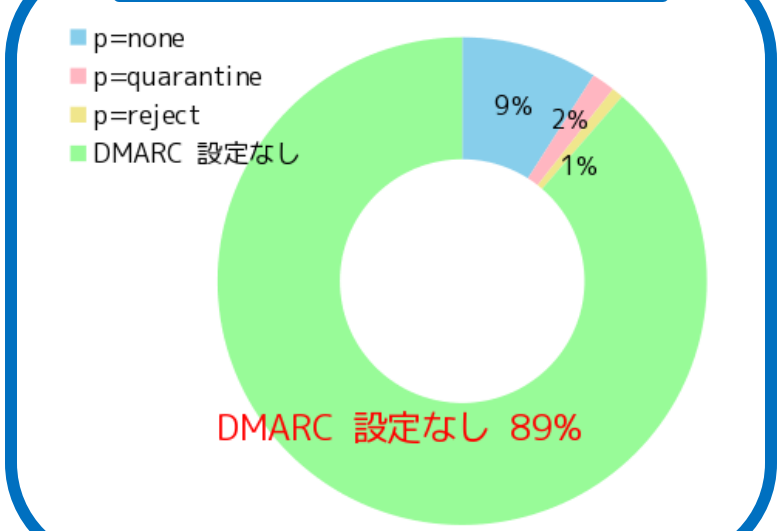
日本政府組織



日本金融機関



TOPIX 銘柄企業



「日本DNSオペレーターズグループ・統計」よりデータ引用
https://dnsops.jp/stats/

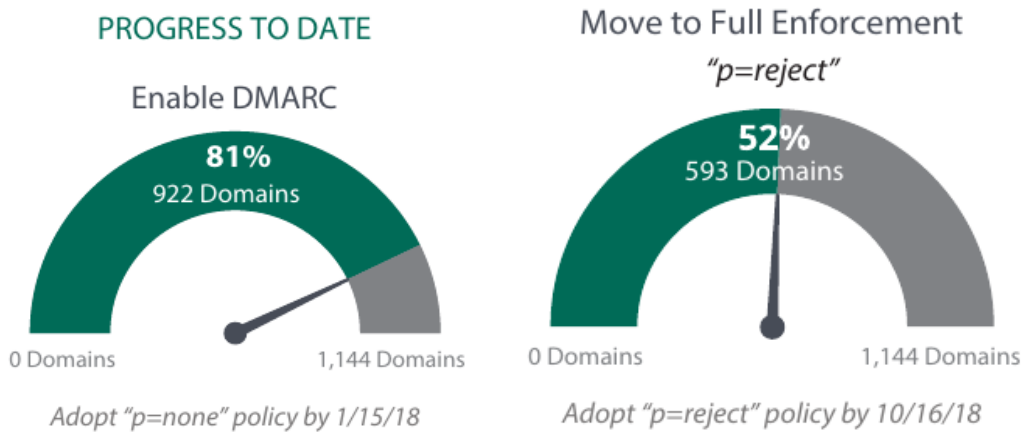
(参考) 米国国土安全保障省 (DHS) - BOD 18-01

「アメリカ政府のドメイン(.gov)は、必ず DMARC せよ」という通達

▶ DMARC の普及と、なりすましメールの撲滅に大きく貢献

- **Binding Operational Directive 18-01 - Enhance Email and Web Security**
  - https://www.cisa.gov/binding-operational-directive-18-01 (2017/10/16 発行)
  - **90日以内に** "p=none" を宣言すること
  - **1年以内に** "p=reject" を宣言すること

- **How to Comply with BOD 18-01 and Secure Email**
  - July 2018 BOD 18-01 Progress Report (2018/07 発行)
    https://www.agari.com/industries/government/bod-18-01



本日、メール屋の私から DNS オペレータの皆さまへのお願いです

重要

みなさん、今すぐ

DMARC 書きましょう

STEP 2

理解して欲しい DMARC

- 「アライメント」という概念 (SPF)
- 「アライメント」という概念 (DKIM)
- 組織ドメインの考えかた
- 事例で見る DMARC レコード

「アライメント(Alignment)」という概念（SPF）

重要

SPF に要求されるアライメント

strict (aspf=s)	Envelope From ドメイン = Header From ドメイン **完全に一致**
relaxed (aspf=r)	Envelope From の**組織ドメイン** = Header From の**組織ドメイン**

例	strict	relaxed
(1) Envelope From: koga@iij.ad.jp Header From: koga@iij.ad.jp	一致	一致
(2) Envelope From: koga@bounce.iij.ad.jp Header From: koga@iij.ad.jp	不一致	一致

組織ドメイン (Organizational Domain)とは

- iij.ad.jp のような、みんなのもの**ではないもの**。
  - .com / .co.jp / .jp / .tokyo.jp は、みんなのもの (誰かが .com を独り占めすることはできない)
- みんなのドメインリスト (Public Suffix List)
  - https://publicsuffix.org/list/public_suffix_list.dat (240KB)

「アライメント(Alignment)」という概念（DKIM）

重要

DKIM に要求されるアライメント

strict (adkim=s)	署名ドメイン(d=) = Header From ドメイン **完全に一致**
relaxed (adkim=r)	署名ドメイン(d=) の**組織ドメイン** = Header From の**組織ドメイン**

例	strict	relaxed
DKIM-Signature: v=1; a=rsa-sha1; (略) d=ml.**iij.ad.jp**; h=From:To:...(略) Header From: koga@**iij.ad.jp**	不一致	一致

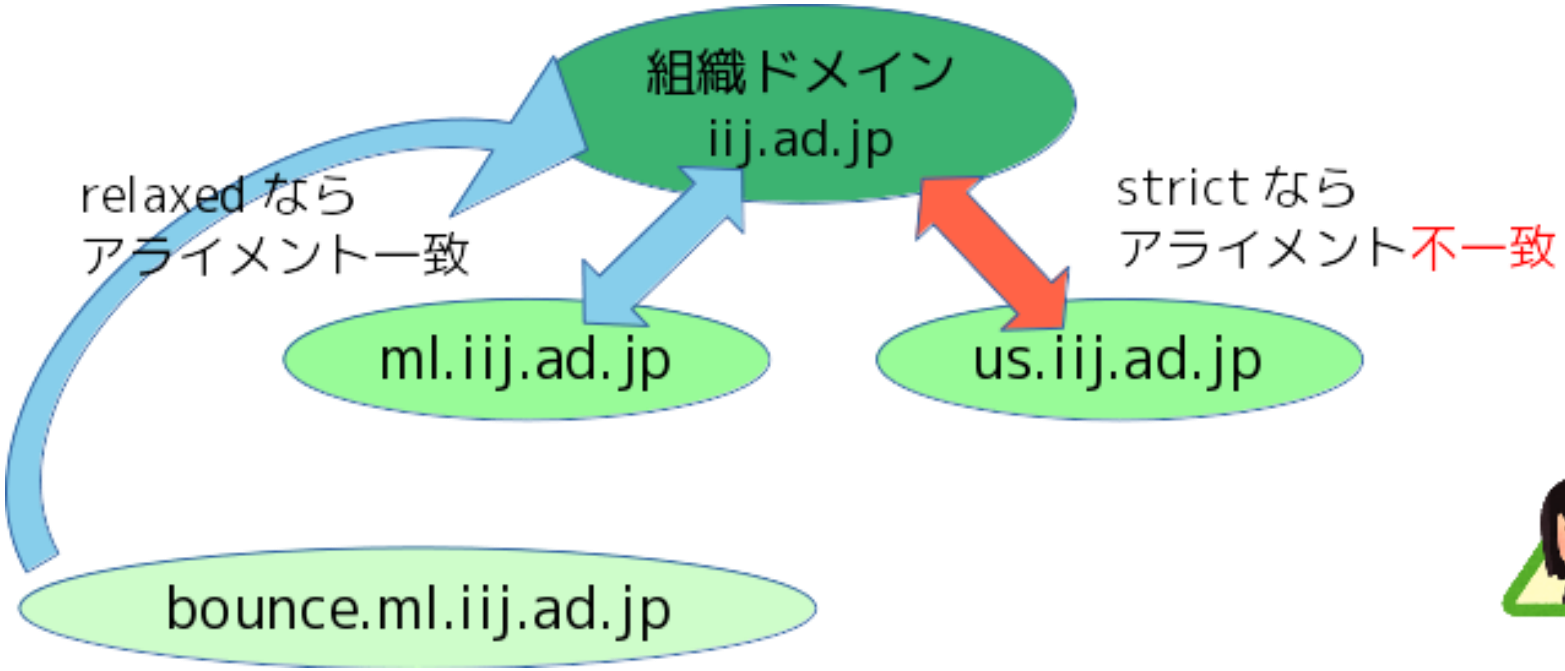
組織ドメイン (Organizational Domain)とは

- iij.ad.jp のような、みんなのもの**<u>ではないもの</u>**。
  - .com / .co.jp / .jp / .tokyo.jp は、みんなのもの (誰かが .com を独り占めすることはできない)
- みんなのドメインリスト (Public Suffix List)
  - https://publicsuffix.org/list/public_suffix_list.dat (240KB)

組織ドメインの考えかた

重要

Public Suffix List に掲載されている一つ下のラベルが組織ドメイン



※ bounce.ml.iij.ad.jp の組織ドメインは、**ml.iij.ad.jp ではない**

事例で見る DMARC レコード (IIJ)

```
_dmarc.iij.ad.jp.      IN    TXT    "v=DMARC1; p=reject;
  adkim=s; aspf=s; rua=mailto:dmarc-rua@dmarc.iij.ad.jp"
```

（実際は一行）

v=DMARC1	iij.ad.jp は DMARC に対応
p=reject	DMARC の認証に失敗(fail)したときは受信拒否(reject)してほしい • p= は none, quarantine, reject のいずれかのみ
adkim=s	DKIM の署名ドメインと Header From ドメインは strict モードで評価 (完全一致) • d= のドメインと、Header From ドメインは必ず一致する。省略すると relaxed。
aspf=s	SPF の Envelope From と Header From ドメインは strict モードで評価 (完全一致) • Envelope From と Header From のドメインは必ず一致する。省略すると relaxed。
rua=mailto:(略)	集計レポートは dmarc-rua@dmarc.iij.ad.jp に送ってほしい • 宛先は "," で区切って複数指定できる

DMARC 認証の成功(dmarc=pass)となるには

重要

DMARC 認証 成功の条件

spf=pass & アライメント一致

または (OR)

dkim=pass & アライメント一致

⚠ **spf=pass & dkim=pass でも、アライメント不一致だと dmarc=fail となることに注意**

(例) 第三者署名で DKIM 署名された送信事業者から送られたメール

```
Envelope From: bounce+koga_iij_ad_jp@sender.example.org
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=dkim1;
    d=sender.example.org; h=From:To:...(以下略)
Header From: koga@iij.ad.jp
```

差出人ドメインの iij.ad.jp と sender.example.org の関係性が不明

DMARC レポートで認証結果が fail となっていたときの想定ケース

個々の状況に応じて判断する必要あり

優先度	考えられるケース	状況・対応指針
高	悪の組織が なりすましメールを 送っている	• 「悪」が、あなたのドメインを騙ってメールを送信している。 • 受信者は、なりすまされたメールを受信している可能性あり。 • DMARC のポリシー p=reject に強化することを検討する。
高	管理外のメール サーバからメール が送信されている	• あずかり知らぬ場所からメールが出ている。 • 管理外のメールサーバか、SPF の登録漏れ。 • DMARC レポートではこうした事案も早期に察知できる。
中	転送メールが 出ている	• 転送メールは、通常 Envelope From を変更せずに転送先のメールアドレスへ送信するため、SPF の認証が失敗する。 • DMARC レポートには IP アドレスが掲載されているため、対象サーバの特定は比較的容易。
低	メーリングリストを 経由している	• メーリングリスト側で回避策が必要。 • 例えば、メーリングリストサーバ側で Header From を書き換える、メーリングリストのドメインを分離する対応がよく見られる。

どれくらい自社ドメインがなりすまされているか、ご存知ですか? - https://eng-blog.iij.ad.jp/archives/3273

STEP 3

知っておいてほしい DMARC

- DMARC レポート
- DMARC ではないもの
- p=reject までの進めかた

どれくらい自社ドメインがなりすまされているか、ご存知ですか? - https://eng-blog.iij.ad.jp/archives/3273

DMARC レポート

配送の透明化に役立つ (受け取り無料)

集計レポート (Aggregate Report)

- DMARC レコードに rua= があれば、UTC の 00:00 頃に 1日 1回、そのメールアドレス宛に送付。
- XML 形式で gz 圧縮の添付ファイル (ZIP で送付する事業者もあり)
- Google、Microsoft、Amazon などが対応。
- 送付は任意。必ず送ってくれるとは限らない。

失敗レポート (Failure Report)

- DMARC レコードに ruf= があれば、認証に失敗したその都度、元メールがまるごと RFC822 形式で添付されてくる。
- DMARC の認証に失敗したとはいえ、プライバシーへの配慮から対応している事業者は少ない。

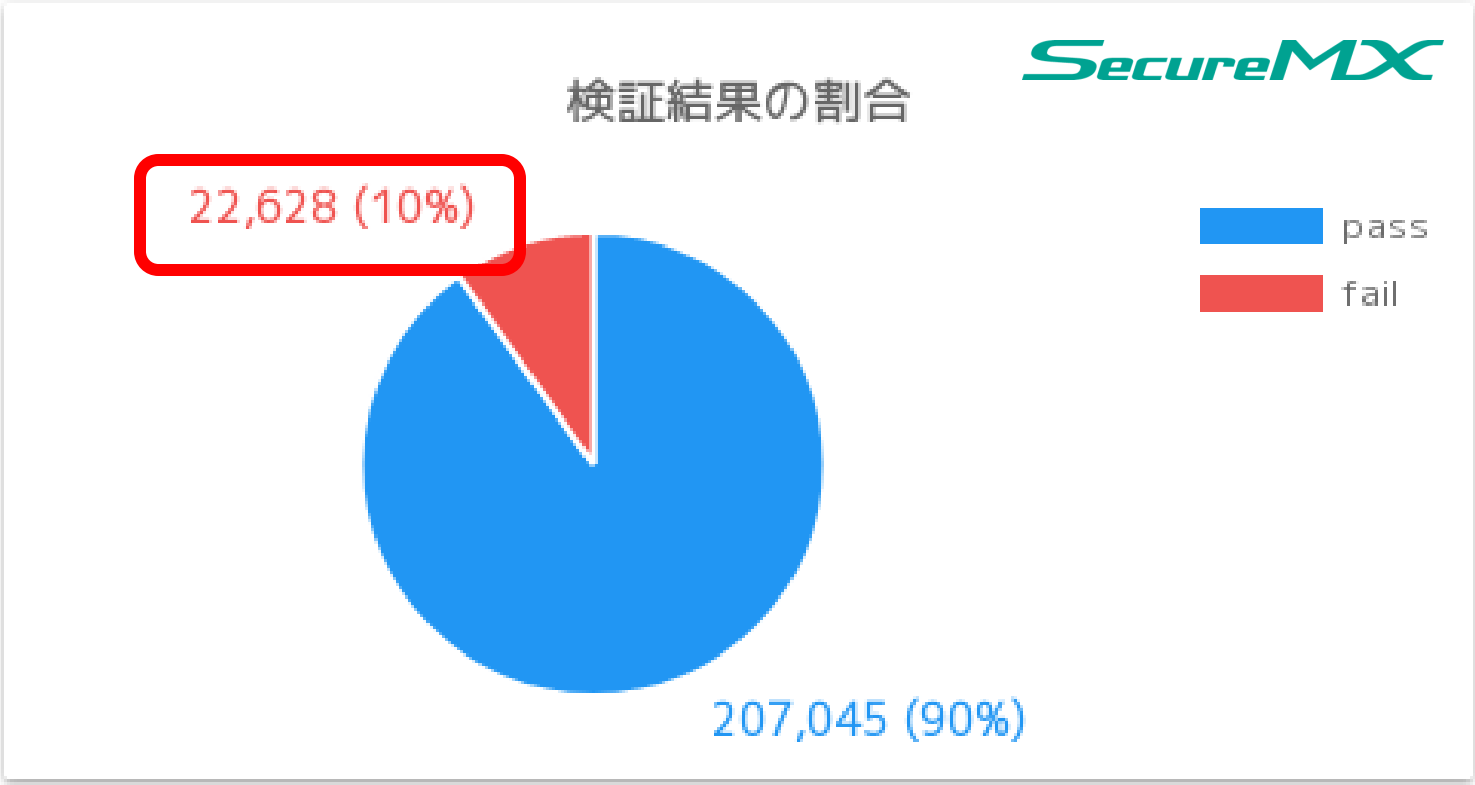
(例)

```
<?xml version="1.0" encoding="UTF-8" ?>
(略)
  <record>
    <row>
      <source_ip>192.0.2.1</source_ip>
      <count>14</count>
      <policy_evaluated>
(略)
    <auth_results>
      <dkim>
        <domain>iij.ad.jp</domain>
        <result>fail</result>
        <selector>20180225.smx</selector>
      </dkim>
      <spf>
        <domain>iij.ad.jp</domain>
        <result>pass</result>
      </spf>
    </auth_results>
  </record>
```

どれくらい自社ドメインがなりすまされているか、ご存知ですか? - https://eng-blog.iij.ad.jp/archives/3273

(参考) iij.ad.jp における DMARC レポートの集計結果

fail したメールは受信拒否されるので、なりすまし価値がなくなる



iij.ad.jp おける DMARC レポートの集計結果 (1か月間)

※ DMARC p=reject はメーリングリスト等の組み合わせで副作用が出るケースがあります

DMARC ではないもの

- **display-name の課題を解決するものではない**

(例)

From: "株式会社インターネットイニシアティブ" <badguy@example.info>

From: "koga@iij.ad.jp" <spammer@example.net>

- **迷惑メールフィルタではない**

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

p=reject までの進めかた

p=none はスタート地点。書くだけで安心しない。千里の道も一歩から。

まずは p=none で
レポート受信
(3か月くらい～是正が終わるまで)

- DMARC は組織ドメインに書けば、全サブドメインのレポートを取得できる。
- 自組織の流通する正規なメールを特定・整理。
- SPF、DKIM の設定状況を確認・是正。

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、見える変化、社内問い合わせはなかった。

p=reject へ

- 思い切って p=reject を宣言。

これから使い始めるドメインは最初から p=reject を書く

STEP 4

メールを使わなくても DMARC

- メールを送らない/受け取らない宣言・Null MX

メールを送らない/受け取らない宣言・Null MX

「このドメイン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 とメーリングリスト

送信ドメイン認証の最後の砦

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

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

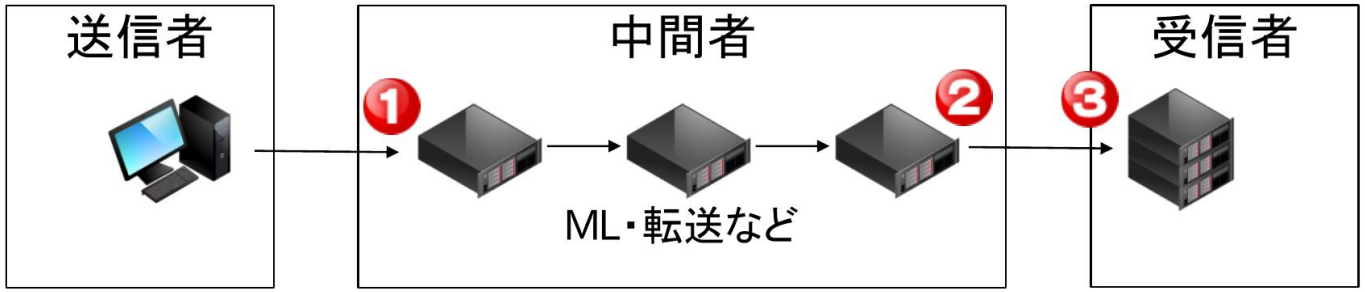
✔ メーリングリストサーバに手を入れなくて良い
DMARC の対応スコープから外せる

✖ 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



- 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

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

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 Mailman 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/

まとめ

今、求められるメールセキュリティ～パスワード付きZIPと
送信ドメイン認証「DMARC」
https://www.iij.ad.jp/dev/report/iir/055/01.html

「悪」の手に掛かる前に対策しましょう

**(1) とにかく DMARC
まずは書きましょう**

**(2) 悪用で被害が出る前に
p=reject の準備を**

IIJ IIR　検索

詳細は IIR vol.55 へ!

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

補足資料

時間の都合で割愛した内容

DKIM の対応優先度が低い理由

どうして DKIM 対応は後回しで良いか

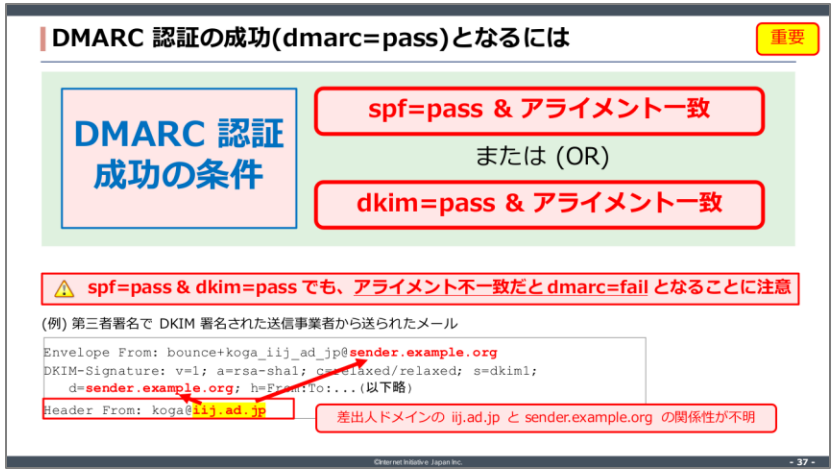
DKIM の対応優先度が低い理由

SPF + DMARC で Header From を守れるようになったから

```
Envelope From: koga@iij.ad.jp
Header From: koga@iij.ad.jp
```

ほとんどの使いかたではアライメント一致

出口サーバも管理されていて SPF も書ける



DKIM 対応が必要なケース

```
Envelope From: bounce+koga_iij_ad_jp@sender.example.org
DKIM-Signature: v=1; a=rsa-sha1; c=relaxed/relaxed; s=dkim1;
   d=iij.ad.jp; h=From:To:...(以下略)
Header From: koga@iij.ad.jp
```

送信事業者に配信を代行している場合、DKIMでしかアライメントの一致ができない!!

SPF よもやま話

SPF でよく聞かれる内容

何をどう評価すればいいか問題

softfail

hardfail

temperror

permerror

neutral

none

softfail / hardfail / temperror / permerror 全部同じでいい

評価基準は

pass か、それ以外か

- pass 以外の結果は認証できていない事実に変わりはない
- 意図的に syntax error を狙った spam も観測
- この機会に SPF の "~all" や "?all" は、"-all" へ変更を!!

DMARC とサブドメイン

サブドメインが大量にあるときの DMARC 対応方針例

サブドメインの対応方針

まずは p=none で
レポート受信

- DMARC は組織ドメインに書けば、全サブドメインのレポートを取得できる。
- 流通しているドメインをここでリストアップする。

「組織ドメイン」と
「サブドメイン」で
ポリシーを分離

- sp= タグを書くと、そのサブドメインに別のポリシーを定義できる。
- 特定サブドメインだけ変えたいときは、そのサブドメインに DMARC レコードを書く。

各々のドメインで
DMARC 対応を
進める

- (例) メーリングリストだけ p=none とし、他はすべて p=reject を目指す。

メール用のサブドメインは、今後新たに作らないのがオススメ。
既存のサブドメインも積極的に廃止するか、正しく管理する。

サブドメインのよくある質問

特定ドメインだけポリシーを変えたいときは?

そのサブドメインに DMARC レコードを書く

(DMARC レコードのルックアップ順序)
1. ヘッダ From ドメインの DMARC レコード (例: _dmarc.bounce.ml.iij.ad.jp)
2. 1. が見つからなければ、組織ドメインの DMARC レコード (例: _dmarc.iij.ad.jp)

サブドメインごとに MTA があって出口が異なる場合は、従来どおり SPF レコードが必要?

必要

DMARC の登場で SPF の仕様が変わったわけではない

DMARC の pct= タグ

DMARC の認証に失敗(fail)したメールのポリシー適用確率

DMARC の pct= タグ

DMARC の認証に失敗(fail)したメールのポリシー適用確率

- 一気にデプロイするのではなく、徐々にポリシーを強化する
- 様子見に使える

```
_dmarc.example.jp.      IN    TXT    "v=DMARC1; p=reject; pct=50"
```

v=DMARC1	example.jp は DMARC に対応
p=reject	DMARC の認証に失敗(fail)したときは受信拒否(reject)してほしい
pct=50	ポリシー(p=)のアクションを適用する確率は 50%

DMARC クイズ (1)

DMARC の認証に失敗(fail)したメールのポリシー適用確率

```
_dmarc.example.jp.      IN    TXT    "v=DMARC1; p=reject; pct=50"
```

DMARC の認証に 10通 fail しました。
10通のうち、5通が reject されるとして、
残りの 5通はどうなるのが RFC 的に正しい挙動でしょう?

(A) なにもしない (p=none として扱う)
(B) 隔離する (p=quarantine として扱う)
(C) 未定義

DMARC クイズ (1)

答え

DMARC の認証に失敗(fail)したメールのポリシー適用確率

```
_dmarc.example.jp.      IN    TXT    "v=DMARC1; p=reject; pct=50"
```

DMARC の認証に 10通 fail しました。
10通のうち、5通が reject されるとして、
残りの 5通はどうなるのが RFC 的に正しい挙動でしょう?

(A) なにもしない (p=none として扱う)

(B) 隔離する (p=quarantine として扱う)

(C) 未定義

DMARC クイズ (2)

DMARC の認証に失敗(fail)したメールのポリシー適用確率

```
_dmarc.example.net.      IN    TXT    "v=DMARC1; p=quarantine; pct=0"
```

DMARC の認証に 10通 fail しました。
どのようにポリシーを適用するのが、RFC 的に正しい挙動でしょう?

(A) なにもしない (p=none として扱う)
(B) 隔離する (p=quarantine として扱う)
(C) 未定義

DMARC クイズ (2)

答え

DMARC の認証に失敗(fail)したメールのポリシー適用確率

```
_dmarc.example.net.      IN    TXT    "v=DMARC1; p=quarantine; pct=0"
```

DMARC の認証に 10通 fail しました。
どのようにポリシーを適用するのが、RFC 的に正しい挙動でしょう?

(A) なにもしない (p=none として扱う)

(B) 隔離する (p=quarantine として扱う)

(C) 未定義

DMARC の pct= タグはややこしい

pct= タグは書かないのがオススメ

- 動きが分かりにくい
- テストをしても結果が想定しづらい

```
_dmarc.example.jp.      IN    TXT    "v=DMARC1; p=reject; pct=50"
```

DMARC(RFC7489) の §6.6.4 Message Sampling にこの動きが書いてある

> If email is subject to the DMARC policy of "quarantine", the Mail Receiver SHOULD quarantine the message. If the email is not subject to the "quarantine" policy (due to the "pct" tag), the Mail Receiver SHOULD apply local message classification as normal.
>
> If email is subject to the DMARC policy of "reject", the Mail Receiver SHOULD reject the message (see Section 10.3). If the email is not subject to the "reject" policy (due to the "pct" tag), the Mail Receiver SHOULD treat the email as though the "quarantine" policy applies.

6.6.4. Message Sampling - https://datatracker.ietf.org/doc/html/rfc7489#section-6.6.4

Q&A

お時間の都合でお話できなかったご質問に回答します (順不同)

DMARC の仕様について

あるドメインに DMARC を設定した場合、そのサブドメインにも影響があるか？

⑩ はい、サブドメインにも適用されます。

⑩ もし、サブドメインに別のポリシーを定義したい場合は 2つの方法があります。p.61 をご覧ください。

TLD に DMARC が設定される可能性はあるか？

- 現時点で、一般的に TLD に DMARC が設定される可能性はないとお考えいただいて差し支えありません。
- gTLD の場合は、記載できる内容が契約書で規定されています。
  https://www.icann.org/en/registry-agreements
- ccTLD の場合は各国の方針次第ですが、例えば、.jp に rua や ruf タグが記載されたら、どのようなことが起こるかを想像してみてください。(特に ruf)

RFC9091 は？

- RFC9091 は、TLD に DMARC レコードを記載できるようにしようという実験的(Experimental) RFC で、すでに .gov や .mil、.gov.uk などで記載が始まっているようです。
- 一方で、仮に .com に ruf が記載されたことを考えてみます。すると、米国の VeriSign 社が .com 全ての情報を収集することが可能になります。これを GDPR が施行されている EU 圏の人々がどのような反応をするでしょうか。筆者はこの RFC の用途はかなり限定的と考えていますが、今後の動向に注視が必要です。

DMARC ポリシー関連について

- **IIJ の DMARC レコードは strict になっているが、理由はあるか?**
  - メールアドレスに利用できるドメインを、厳密に管理するのが目的です。
  - 例えば、strict を指定すれば、勝手にサブドメインでメールアドレスを作れません。
  - 現在 relaxed で運用されている組織も、これ以上に勝手にサブドメインの利用が始まると、管理が困難になりますので、基本的には strict でのアライメント一致を目指すのがオススメです。

- **DMARC 対応しても reject しない限りは受信者に届くので風評被害は減らないのでは? reject 必須?**
  - はい、そうならないために、この場を借りて p=reject を普及させたい考えです ☺
  - みんなが dmarc=fail したメールを reject (受信拒否)するようになれば、悪の組織もそのドメインを騙る価値がなくなっていくでしょう。
  - (参考) Gmail の "No auth, No entry" https://dmarcian.com/no-auth-no-entry/

送信ドメイン認証全般について

参照: p.23, p.37

- **現状 SPF のみ設定しているが、DMARC を設定をすれば、DKIM は不要か？**
  DKIM と DMARC の両方の設定が必須か？
  - SPF のアライメントが一致できる場合は、SPF のみの設定で DMARC レコードを書いても差し支えありません。
  - その場合 DKIM は必須ではありません。

- **.co.jp と .jp の両方を保持している。同じユーザが双方のドメインで受信している場合、送信はどちらかに寄せないと、DMARC の仕組みは使えないか？**
  - 一般的には SPF + DMARC の組み合わせが容易ですので、管理する立場からすれば、どちらかのドメインに統一されるのが、最もラクだと思います。(2つあると二重に管理しなければいけないので)
  - (こんなケースはないと思いますが) 例えば、Envelope From は .co.jp、Header From は .jp のようなメールを送る場合は、.jp 側の DKIM で署名して、DKIM のアライメントを一致させ、DMARC=pass する必要があります。
  - 受信して DMARC によるフィルタリングをしたいだけでしたら、関係ありません。

DMARC レポート関連について

- DMARC のレポートを送るとエラーとなるドメインがかなり有名なドメインでも多い(感想)
  - レポートの送信とフィードバックありがとうございます。
  - 受け取る側もそこそこ苦労があるので気持ちは分かります...