



ブランドを守るために必要な送信ドメイン認証

2023/07/21

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(IJ)
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
WIDE Project

M³AAWG
MESSAGING MALWARE MOBILE
ANTI-ABUSE WORKING GROUP
M3AAWG

openSUSE

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



アニメーション制作会社がサイバー攻撃を受けたんだって？

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



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



アニメーション制作会社がサイバー攻撃を受けたんだって？

さいばーこうげき？ ってなに？

子

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



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



アニメーション制作会社がサイバー攻撃を受けたんだって？

サイバーこうげき？ 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



アニメーション制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



アニメーション制作会社がサイバー攻撃を受けたんだって？

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



アニメーション制作会社がサイバー攻撃を受けたんだって？

サイバーこうげき？ 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

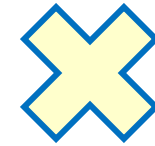
- 誰もが平等
- 資本や立場、政治的な事情で不利な扱いをされたりしない

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)

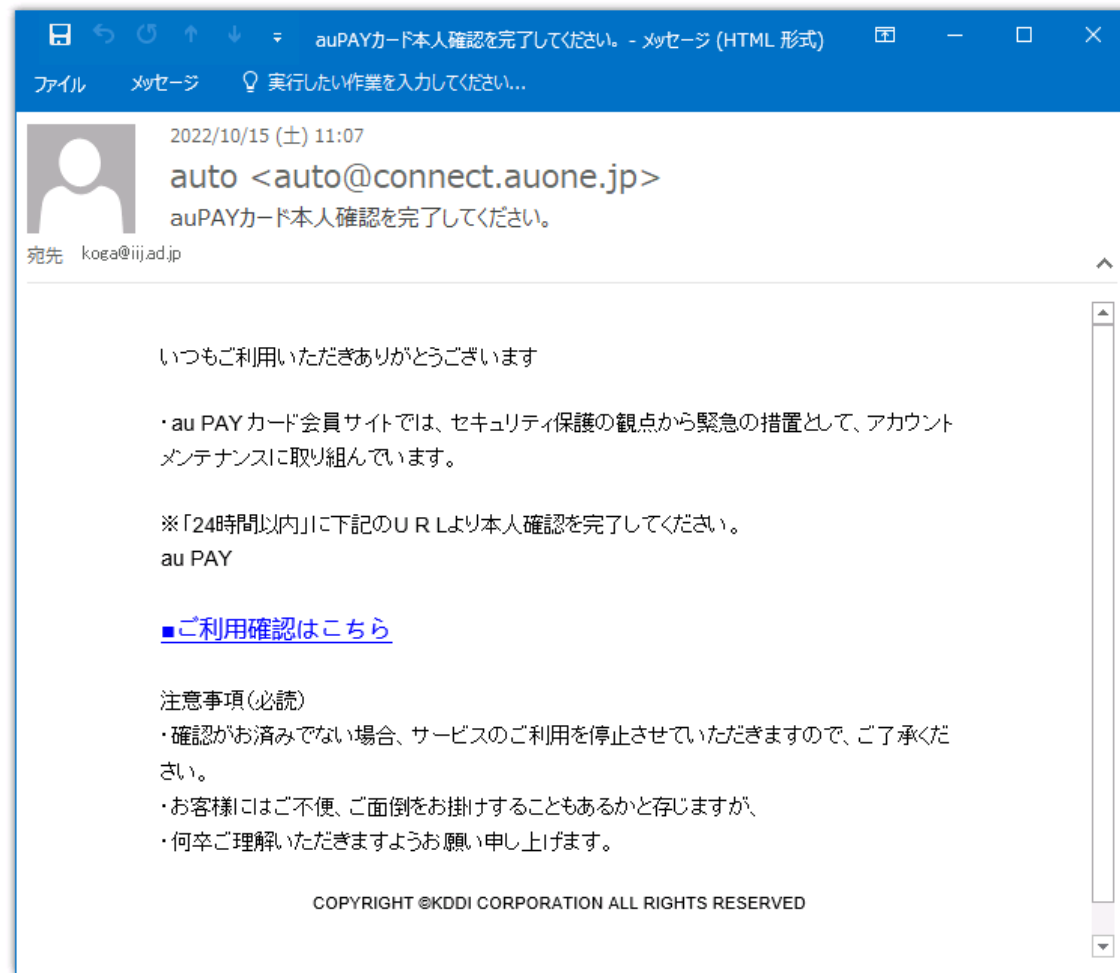
対策をサボると どういう被害が出るのか

サービス利用者側ではなく、提供者側の話をしてします



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



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

「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



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。

「税務署からのお知らせ」等のメールが届いた方へ

- (1) 「税務署からのお知らせ」等のメールとは
- (2) 「税務署からのお知らせ」等のメールの種類

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://〇〇〇〇〇〇・・・・>

(1) 「税務署からのお知らせ」等のメールとは

【令和4年8月26日追記】

以下の赤字部分を追記しました。

e-Taxでは、メールアドレスを登録している方へ、メッセージボックスに情報が格納された場合や、暗証番号の再設定のための秘密の質問と答えなどの登録を受け付けた段階で、登録しているメールアドレスあてに「税務署からのお知らせ」又は「国税庁からのお知らせ」メールを送信しています。

事前にメールに表示する宛名をe-Taxに登録することで、「税務署からのお知らせ」等メールの件名や本文に登録した宛名が表示されます。また、「税務署からのお知らせ」等メールは、以下の送信元から送信されます。

送信元表記 : e-Tax (国税電子申告・納税システム) <info@e-tax.nta.go.jp>

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さい。

- 税務署の連絡先は「[税務署案内](#)」をご覧ください。



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)**



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





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分からない

(例) `example.com.` IN TXT "v=spf1 +all"

```
Envelope From: badguy@example.com  
Header From: Isamu Koga <koga@ij.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

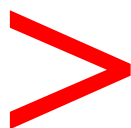
DMARC



ポリシーの話

SPF

絶対やる



DMARC

絶対やる



DKIM

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"
```

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

※ "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 <ul style="list-style-type: none">必ず先頭に書く
p=quarantine	DMARC の認証に失敗(fail)したときは <u>隔離(quarantine)してほしい</u> <ul style="list-style-type: none">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% <ul style="list-style-type: none">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 <ul style="list-style-type: none">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 <ul style="list-style-type: none">宛先は "," で区切って複数指定できる

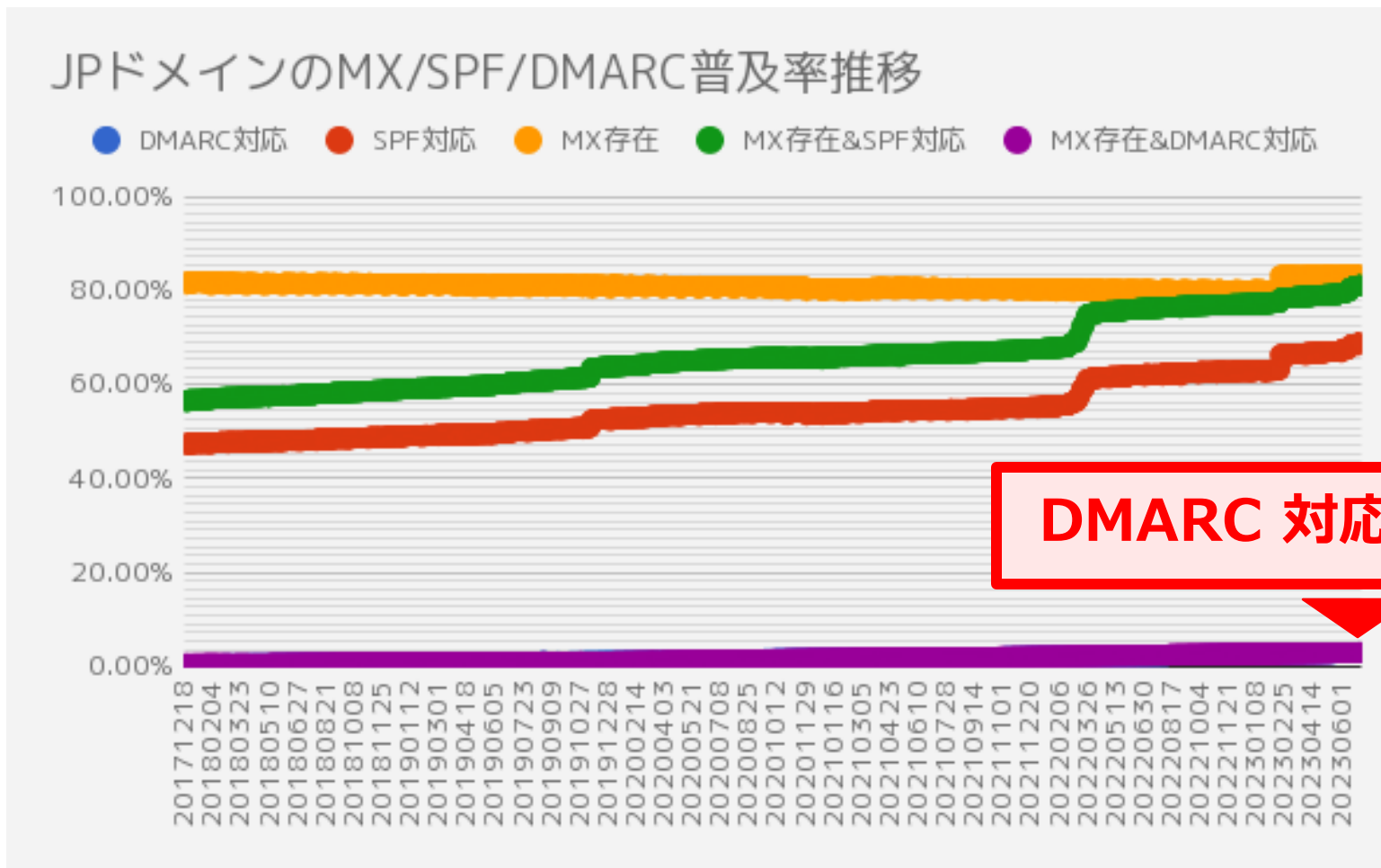
- 受信者のアクションを定義できて
- なりすまし対策もできて
- レポートもタダでもらえる

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 3.03%

※ 2023/07/06 時点



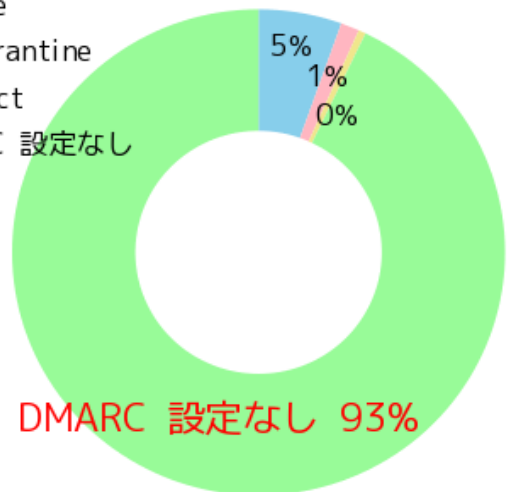
DMARC adoption statistics of JP domains
<https://kitazaki.github.io/dmarc/>

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

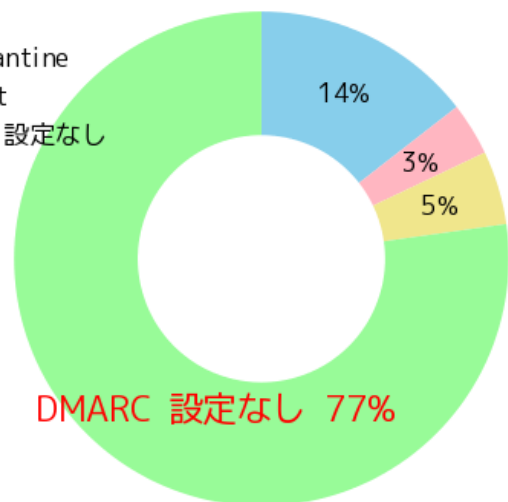
- p=none
- p=quarantine
- p=reject
- DMARC 設定なし



DMARC 設定なし 93%

日本金融機関

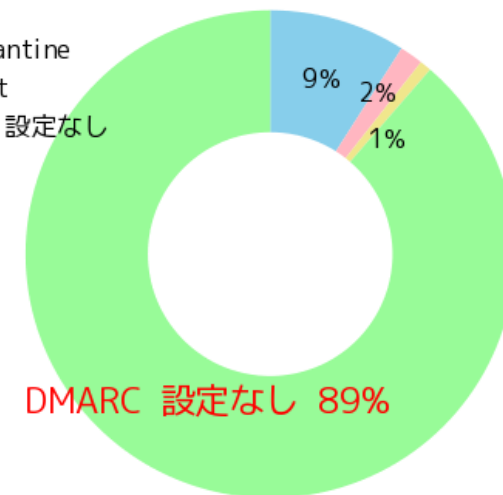
- p=none
- p=quarantine
- p=reject
- DMARC 設定なし



DMARC 設定なし 77%

TOPIX 銘柄企業

- p=none
- p=quarantine
- p=reject
- DMARC 設定なし



DMARC 設定なし 89%

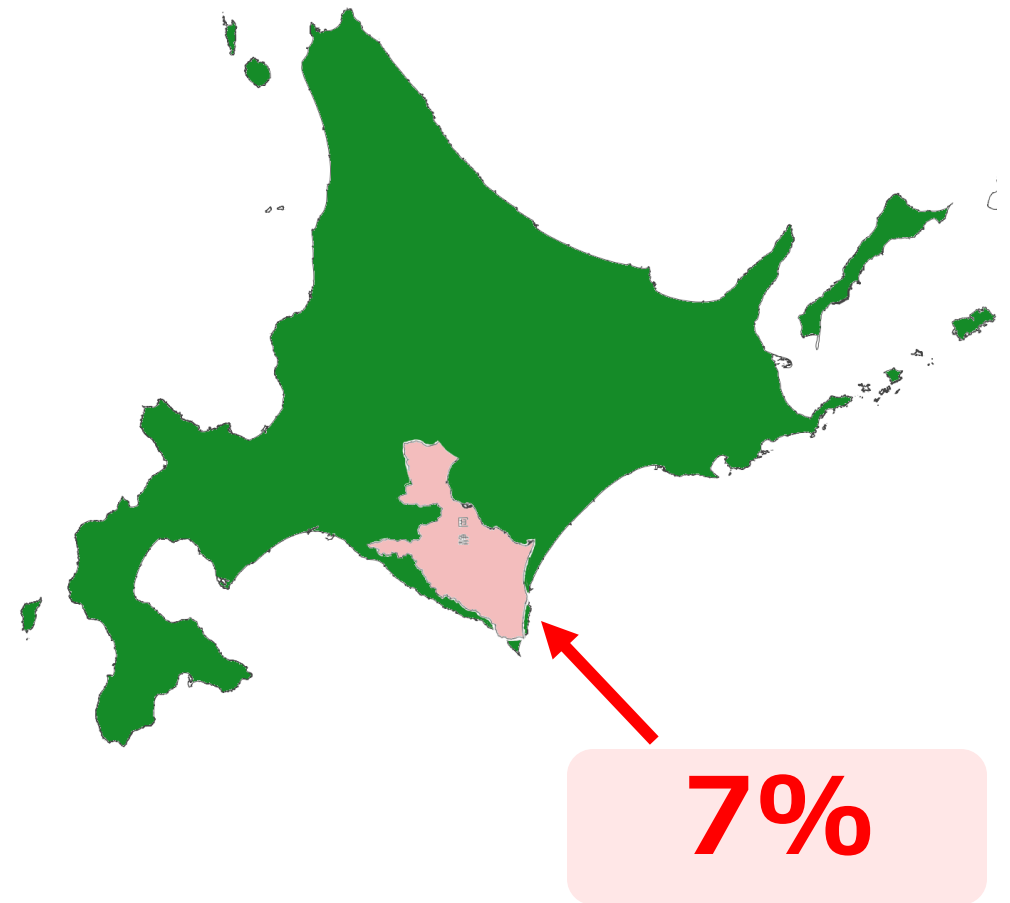
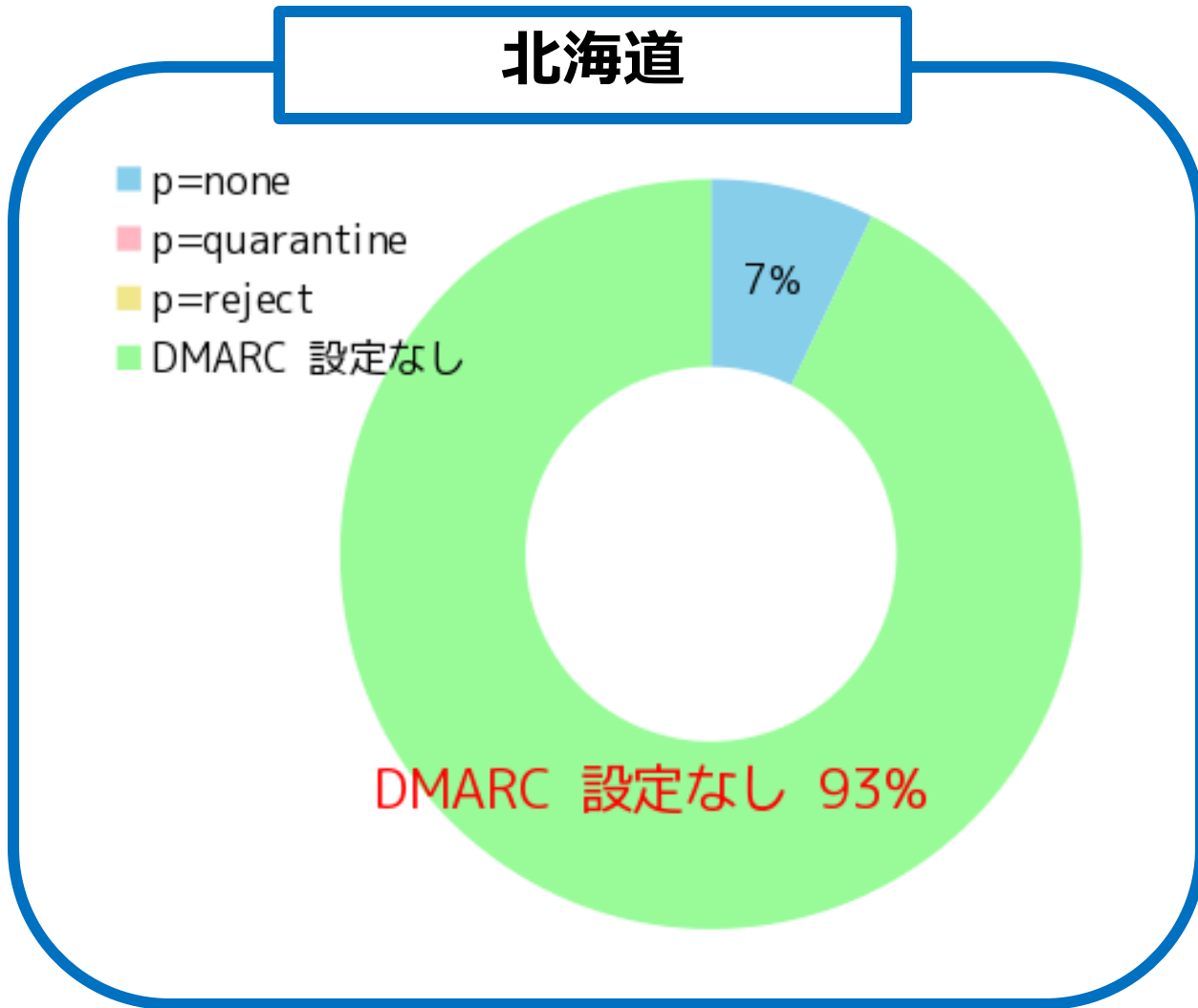


「日本DNSオペレーターズグループ・統計」よりデータ引用
<https://dnsops.jp/stats/>



北海道に本社がある上場企業ドメインの 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



|(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

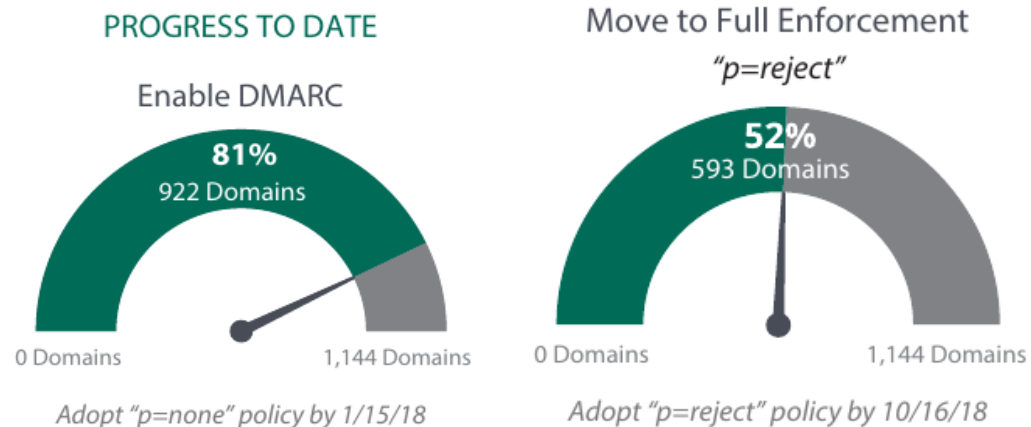
▶ DMARC の普及と、なりすましメールの撲滅に大きく貢献

■ 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、みなさまへお願いに参りました



重要

みなさん、今すぐ

DMARC 書きましよう

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)

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@ ij.ad.jp Header From: koga@ ij.ad.jp	一致	一致
(2) Envelope From: koga@bounce. ij.ad.jp Header From: koga@ ij.ad.jp	不一致	一致



組織ドメイン (Organizational Domain)とは

- ij.ad.jp のような、みんなのものではないもの。
 - .com / .co.jp / .hokkaido.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

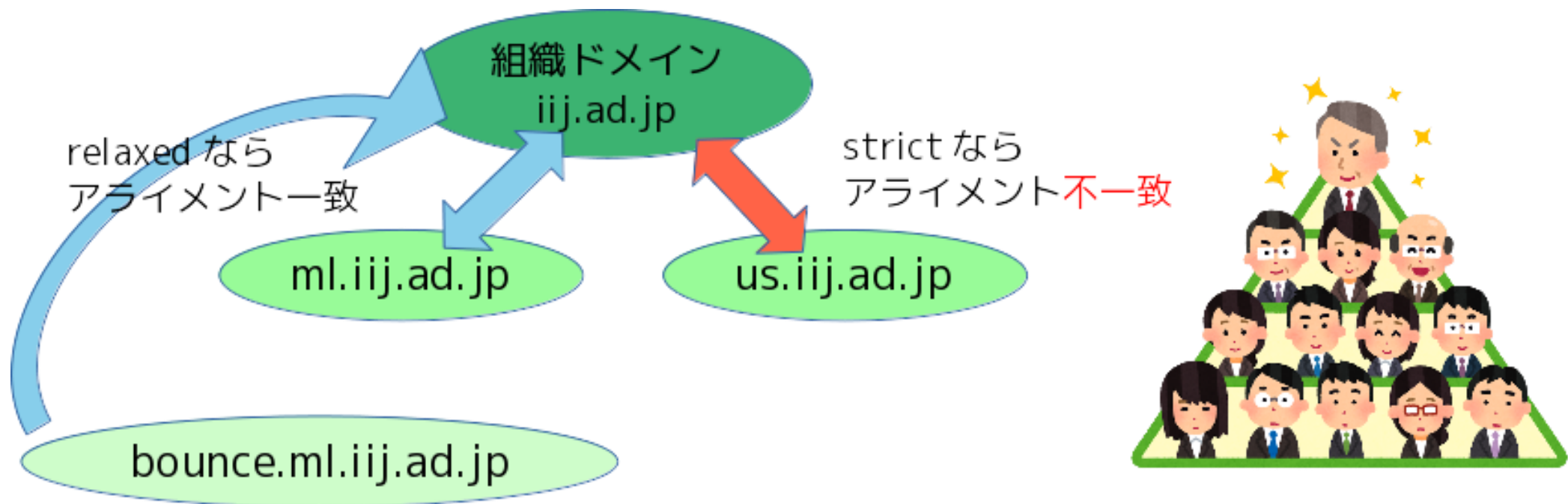
- iij.ad.jp のような、みんなのものではないもの。
 - .com / .co.jp / .hokkaido.jp は、みんなのもの (誰かが .com を独り占めすることはできない)
- みんなのドメインリスト (Public Suffix List)
 - https://publicsuffix.org/list/public_suffix_list.dat (240KB)



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 <u>受信拒否(reject)してほしい</u> <ul style="list-style-type: none">• 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) <ul style="list-style-type: none">• 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) <ul style="list-style-type: none">• 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 <ul style="list-style-type: none">• 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	<ul style="list-style-type: none">「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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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	<ul style="list-style-type: none">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。

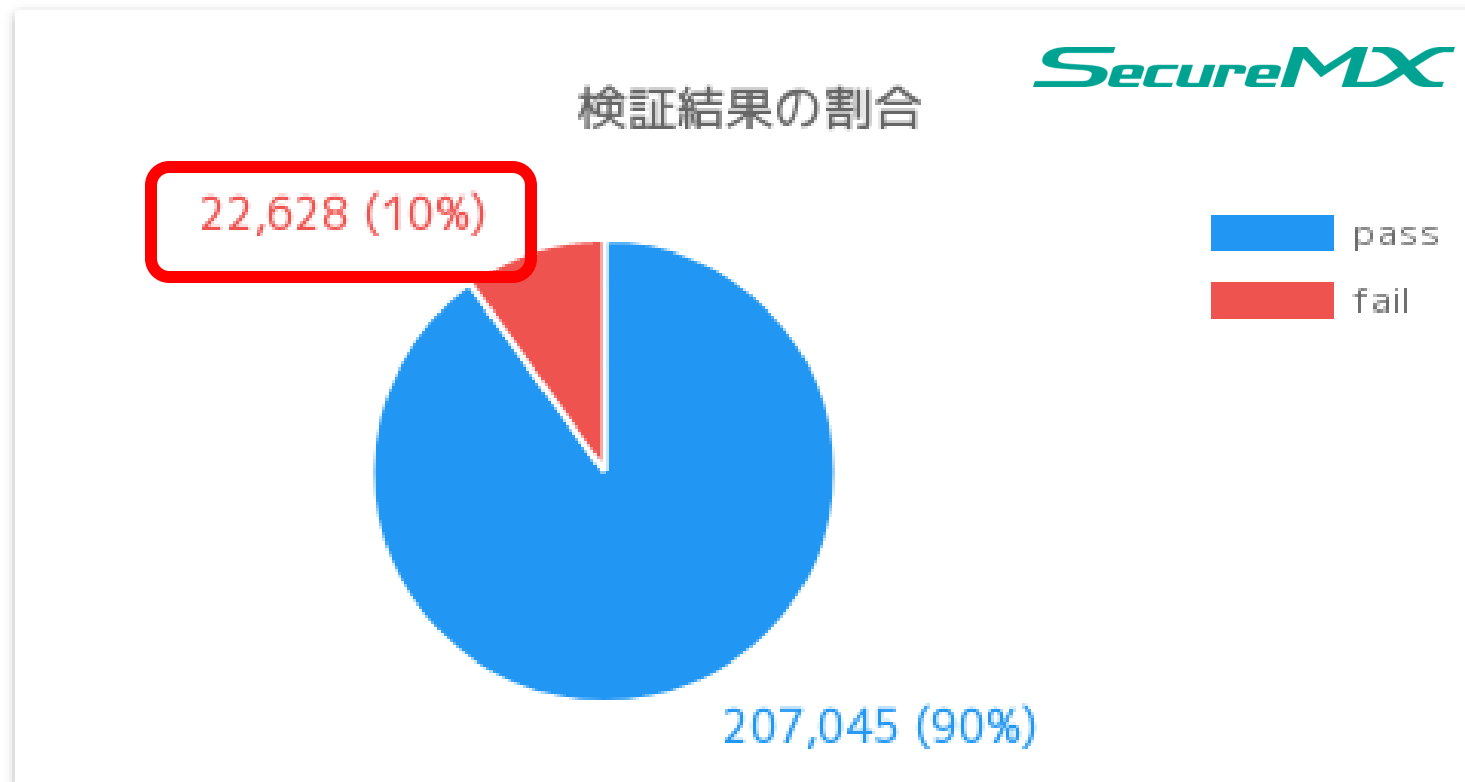
```
(例)
<?xml version="1.0" encoding="UTF-8" ?>
(略)
<record>
  <row>
    <source_ip>192.0.2.1</source_ip>
    <count>14</count>
    <policy_evaluated>
(略)
  <auth_results>
    <dkim>
      <domain>iij.ad.jp</domain>
      <result>fail</result>
      <selector>20180225.smx</selector>
    </dkim>
    <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、なりすます価値がなくなる



iij.ad.jp における 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@ij.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)。
- IJ では、見える変化、社内問い合わせはなかった。

p=reject ^

- 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>

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!



[PR] YouTuber デビューしました

40分の内容を 7分弱に凝縮しました



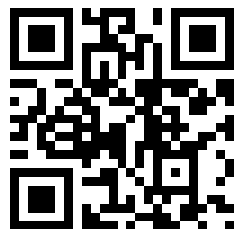
【後編】送信ドメイン認証 DMARC ポリシーの強化

725 回視聴・5 か月前

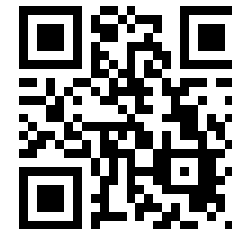


【前編】PPAP 廃止までの流れと IIJ の考える代替策

587 回視聴・5 か月前



<https://youtu.be/3N5G5mP3FxU>



<https://youtu.be/Vg4Oz9SnKCM>

Lead Initiative

日本のインターネットは1992年、IIJとともに始まりました。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はいつも始まりであり、未来です。

Ongoing Innovation

本書には、株式会社インターネットイニシアティブに権利の帰属する秘密情報が含まれています。本書の著作権は、当社に帰属し、日本の著作権法及び国際条約により保護されており、著作権者の事前の書面による許諾がなければ、複製・翻案・公衆送信等できません。IIJ、Internet Initiative Japanは、株式会社インターネットイニシアティブの商標または登録商標です。その他、本書に掲載されている商品名、会社名等は各会社の商号、商標または登録商標です。本文中では™、®マークは表示していません。

©Internet Initiative Japan Inc. All rights reserved. 本サービスの仕様、及び本書に記載されている事柄は、将来予告なしに変更することがあります。