想定所要時間 50分

Internet Week 2024 / C7
10:00～11:30

IIJ Internet Initiative Japan

# 2024年のメール運用と DMARC (前半)


2024/11/26(火)

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 メールサービス運営課
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部
メールサービス運営課・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
WIDE Project

M3AAWG
Messaging Malware Mobile Anti-Abuse Working Group
M3AAWG

openSUSE
openSUSE (趣味)

# 本題に入る前に

アイスブレイク

# 電子メールのプロトコルができたのはいつ?

- **RFC9000　QUIC: A UDP-Based Multiplexed and Secure Transport**
  https://datatracker.ietf.org/doc/html/rfc9000

# 電子メールのプロトコルができたのはいつ?

2021年

- **RFC9000　QUIC: A UDP-Based Multiplexed and Secure Transport**
  https://datatracker.ietf.org/doc/html/rfc9000

Windows 11

# 電子メールのプロトコルができたのはいつ?

2015年

- **RFC7540　Hypertext Transfer Protocol Version 2 (HTTP/2)**
  https://datatracker.ietf.org/doc/html/rfc7540

Windows 10

2021年

- **RFC9000　QUIC: A UDP-Based Multiplexed and Secure Transport**
  https://datatracker.ietf.org/doc/html/rfc9000

Windows 11

# 電子メールのプロトコルができたのはいつ?

1996年

- **RFC1945　Hypertext Transfer Protocol -- HTTP/1.0**
  https://datatracker.ietf.org/doc/html/rfc1945

2015年

- **RFC7540　Hypertext Transfer Protocol Version 2 (HTTP/2)**
  https://datatracker.ietf.org/doc/html/rfc7540

2021年

- **RFC9000　QUIC: A UDP-Based Multiplexed and Secure Transport**
  https://datatracker.ietf.org/doc/html/rfc9000

Windows 95
Windows 98
Windows 2000
Windows XP
Windows Vista
Windows 7
Windows 8
Windows 10
Windows 11

# 電子メールのプロトコルができたのはいつ?

**1982年**

- **RFC821　SIMPLE MAIL TRANSFER PROTOCOL**
  **https://datatracker.ietf.org/doc/html/rfc821**

MS-DOS 1.25

≈

1996年

- **RFC1945　Hypertext Transfer Protocol -- HTTP/1.0**
  https://datatracker.ietf.org/doc/html/rfc1945

Windows 95
Windows 98
Windows 2000
Windows XP
Windows Vista
Windows 7
Windows 8

2015年

- **RFC7540　Hypertext Transfer Protocol Version 2 (HTTP/2)**
  https://datatracker.ietf.org/doc/html/rfc7540

Windows 10

2021年

- **RFC9000　QUIC: A UDP-Based Multiplexed and Secure Transport**
  https://datatracker.ietf.org/doc/html/rfc9000

Windows 11

# 今日このセッションを聞いて分かること

**電子メールはいわゆる "古き良き時代" に作られた牧歌的なプロトコル**
**「悪」の存在が想定されていなかった**

## イマドキメールの新常識

- 大規模事業者の悩み
- どうしてこうなったのか
- よくある失敗例
- 今やるべきこと

# Google 送信者ガイドライン

Google Sender Guidelines


Google Sender Guidelines
https://support.google.com/a/answer/81126

# Google Sender Guidelines

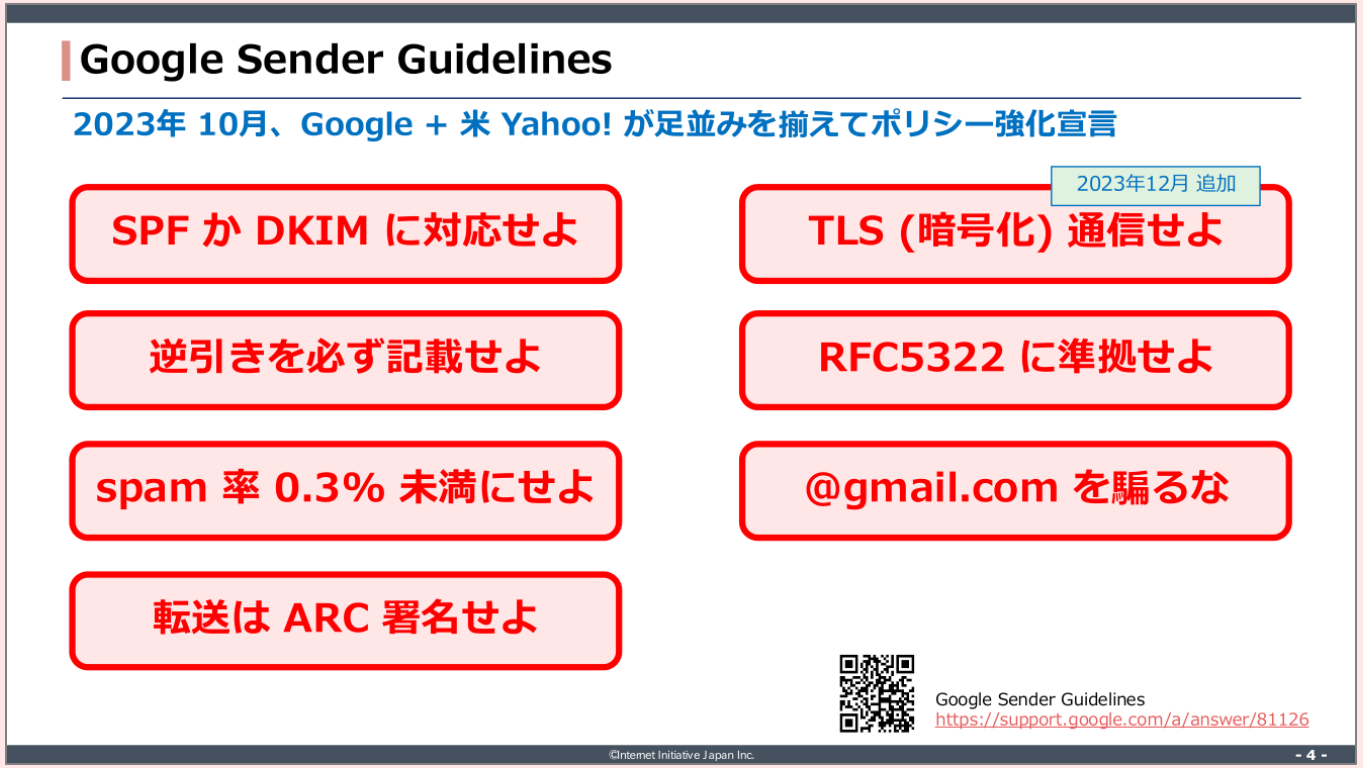
## 2023年 10月、Google + 米 Yahoo! が足並みを揃えてポリシー強化宣言

- SPF か DKIM に対応せよ
- 逆引きを必ず記載せよ
- spam 率 0.3% 未満にせよ
- 転送は ARC 署名せよ
- TLS (暗号化) 通信せよ　（2023年12月 追加）
- RFC5322 に準拠せよ
- @gmail.com を騙るな

Google Sender Guidelines
https://support.google.com/a/answer/81126

# Google Sender Guidelines (5,000通/日 以上送信するドメイン)

## 2023年 10月、Google + 米 Yahoo! が足並みを揃えてポリシー強化宣言




＋

**DMARC対応せよ**

・ドメイン名のなりすましを禁止
・RFC7489 で標準化 (2015年)

**List-Unsubscribe 実装せよ**

・ワンクリックで購読解除できる仕組み
・RFC8058 で標準化 (2017年)

**期限は 2024/01/31 (済)**

Google Sender Guidelines
https://support.google.com/a/answer/81126

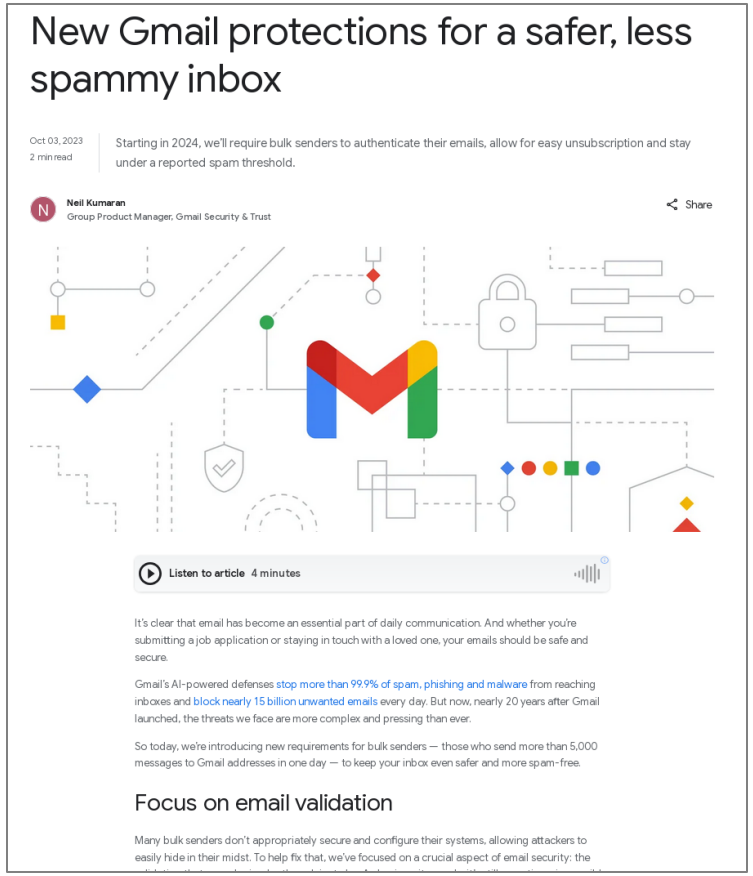
# Google 送信者ガイドラインの背景

米国では「Yahoogle Requirements」と言われています


Google Sender Guidelines
https://support.google.com/a/answer/81126

# Google 送信者ガイドラインの背景

## フィッシングメールとの熾烈な戦いが激化



New Gmail protections for a safer, less spammy inbox

Oct 03, 2023
2 min read

Starting in 2024, we'll require bulk senders to authenticate their emails, allow for easy unsubscription and stay under a reported spam threshold.

Neil Kumaran
Group Product Manager, Gmail Security & Trust

Share

Listen to article 4 minutes

It's clear that email has become an essential part of daily communication. And whether you're submitting a job application or staying in touch with a loved one, your emails should be safe and secure.

Gmail's AI-powered defenses stop more than 99.9% of spam, phishing and malware from reaching inboxes and block nearly 15 billion unwanted emails every day. But now, nearly 20 years after Gmail launched, the threats we face are more complex and pressing than ever.

So today, we're introducing new requirements for bulk senders — those who send more than 5,000 messages to Gmail addresses in one day — to keep your inbox even safer and more spam-free.

Focus on email validation

Many bulk senders don't appropriately secure and configure their systems, allowing attackers to easily hide in their midst. To help fix that, we've focused on a crucial aspect of email security: the

- Google は 毎日**150億通**以上のメールをブロック
- インターネットには時代遅れなシステムが多数あり
  電子メールの全差出人を認証することができていない
- これが攻撃者に付け込まれるスキを与えてしまう

悪を悪と判定することも大事な側面だが
**正しいものを正しい**と判定することも重要

**利用者の保護**

Google The Keyword (公式ブログ)
New Gmail protections for a safer, less spammy inbox
https://blog.google/products/gmail/gmail-security-authentication-spam-protection/

# Google 送信者ガイドラインのスケジュール (済)

## Google が当初発表したタイムラインと時系列

2023年 10月

- **ポリシー強化を発表**
  - 米 Yahoo! も同じ内容で同日に発表
  - この時点では Google Workspace も含まれていた


2023年 12月

- **TLS 通信を利用することを要件に追加**
  - ここで Google Workspace を対象から除外

2024年 2月

- **送信者ガイドラインの施行**
  - Google「迷惑メールフォルダに振り分けられるなど、到達性に悪影響」

2024年 4月

- **送信者ガイドラインに準拠しないメールを一時的なエラー(4xx)で拒否し始める**
  - Google「段階的に行う」

2024年 6月

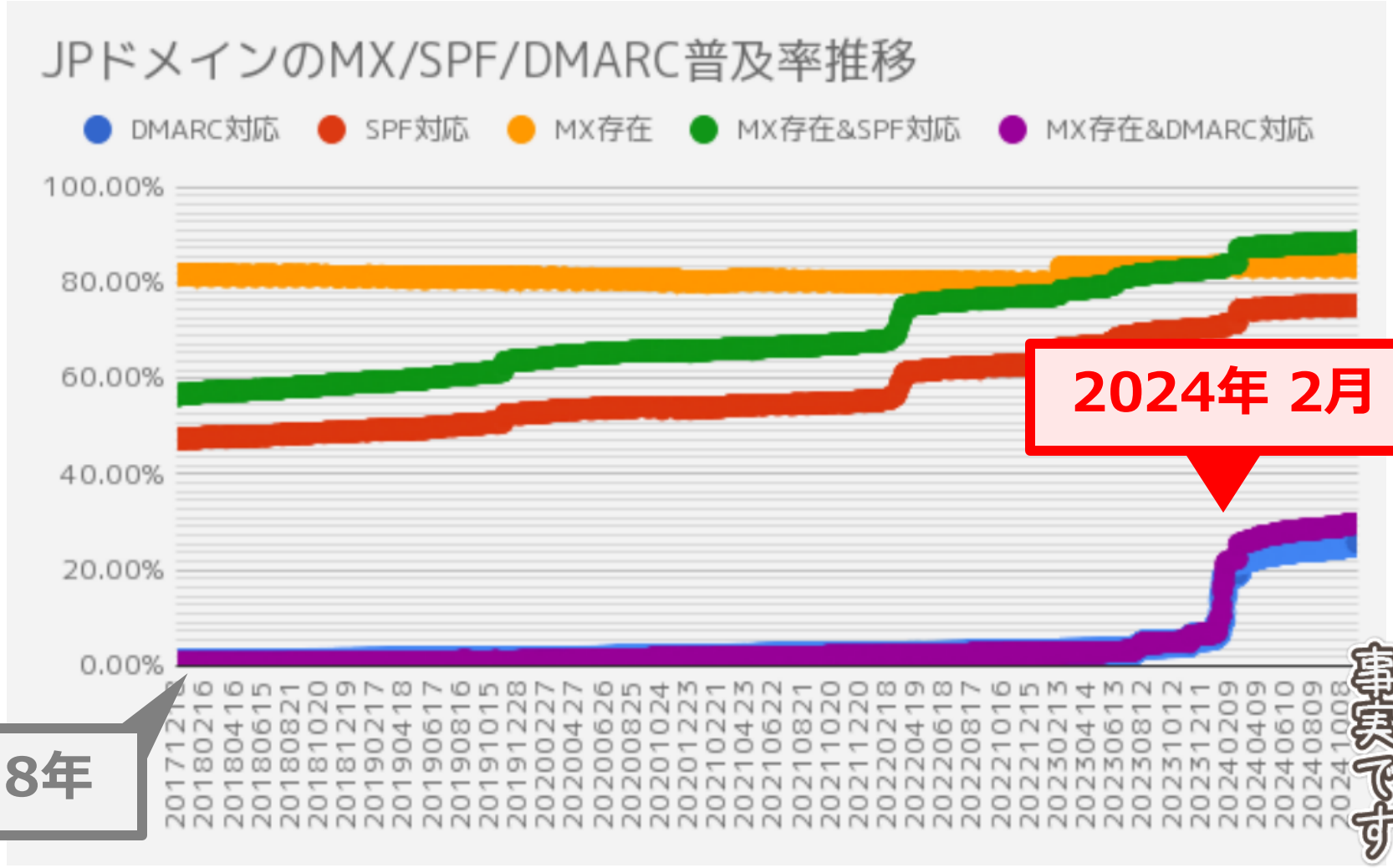
- **ガイドラインに従ったメールの受信拒否を開始**
  - Google「適宜状況を見て判断している」

イマココ

# Google 送信者ガイドラインが与えた影響 (効果)

## 2024年 2月までに急激に DMARC 対応率が増加

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




# 2024年 2月～7月に観測したエラー


## IIJ セキュア MX サービスで観測した Google 宛のエラー数


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

# メール運用管理者に求められる対応

立場によって取るべき対応が微妙に異なるのが
メールの難しいところ

# (例1) 個人でメールサーバを運用している

## 原則全部対応する

- SPF か DKIM に対応せよ
- TLS (暗号化) 通信せよ
- 逆引きを必ず記載せよ
- RFC5322 に準拠せよ
- spam 率 0.3% 未満にせよ
- @gmail.com を騙るな
- 転送は ARC 署名せよ
- DMARC 対応せよ
- List-Unsubscribe 実装せよ
  - メールマガジン等を送信していないなら不要

# (例2) 企業や組織の IT 担当でオンプレミス設備を保有している

## 特に送信ドメイン認証(DMARC)は肝になるため SPF の整理や DKIM 対応は必須

**SPF か DKIM に対応せよ**

**TLS (暗号化) 通信せよ**

**逆引きを必ず記載せよ**

**RFC5322 に準拠せよ**

**spam 率 0.3% 未満にせよ**

**@gmail.com を騙るな**

転送は ARC 署名せよ

メールの転送をしていないなら不要

**DMARC 対応せよ**

5,000通未満の要件に入っていないが実施する

List-Unsubscribe 実装せよ

メールマガジン等を送信していないなら不要

# (例3) メールのクラウドサービスを使っている

## 多くをクラウドサービス事業者が担ってくれるので対応は比較的容易

SPF か DKIM に対応せよ
クラウドサービスのマニュアルを見て対応する

逆引きを必ず記載せよ
クラウドサービス側で対応すべき

**spam 率 0.3% 未満にせよ**

転送は ARC 署名せよ
クラウドサービス側で対応すべき

DMARC 対応せよ
クラウドサービスのマニュアルを見て対応する

TLS (暗号化) 通信せよ
クラウドサービス側で対応すべき

**RFC5322 に準拠せよ**

**@gmail.com を騙るな**

List-Unsubscribe 実装せよ
メールマガジン等を送信していないなら不要

# (例4) オンプレミス設備でメールを大量送信している

## メール送信設備を SIer などに発注している場合は必ず要件(RFP)に含める

**SPF か DKIM に対応せよ**
DKIM の作成者署名が必須

**TLS (暗号化) 通信せよ**

**逆引きを必ず記載せよ**

**RFC5322 に準拠せよ**

**spam 率 0.3% 未満にせよ**
受信者が望まないメールを送ってはいけない

**@gmail.com を騙るな**

転送は ARC 署名せよ
ARC はなくてもよい

**DMARC 対応せよ**

**List-Unsubscribe 実装せよ**
ワンクリックの購読解除は必須要件

# (例5) 広報や人事部など非 IT 部門だが SaaS でメールを送っている

## メールマガジンや人事採用 SaaS を利用しているメールは見落としがちなので注意

**SPF か DKIM に対応せよ**
DKIM の作成者署名が必須

逆引きを必ず記載せよ
SaaS 側で対応すべき

**spam 率 0.3% 未満にせよ**
受信者が望まないメールを送ってはいけない

転送は ARC 署名せよ
ARC はなくてもよい

**DMARC 対応せよ**
DKIM のアライメントが一致しないと
DMARC pass できないので要注意

TLS (暗号化) 通信せよ
SaaS 側で対応すべき

RFC5322 に準拠せよ
SaaS 側で対応すべき

**@gmail.com を騙るな**

**List-Unsubscribe 実装せよ**
ワンクリックの購読解除は必須要件

# メール運用管理者に求められる対応 早見表

| | | SPF か DKIM 対応 | 逆引き記載 | spam rate <0.3% | 転送は ARC 署名 | DMARC 対応 | TLS 対応 | RFC 5322 準拠 | @gmail .com 騙るな | List-Unsubscribe |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 個人でメール設備を運用 | ✅ | ✅ | ✅ | ✅ | ✅ | ✅ | ✅ | ✅ | |
| 2 | 企業でオンプレ設備を保有 | ✅ | ✅ | ✅ | ✅ | ✅ | ✅ | ✅ | ✅ | |
| 3 | クラウドサービス利用 | ✅ | | ✅ | | ✅ | | ✅ | ✅ | |
| 4 | オンプレ設備でメール送信 | ✅ | ✅ | ✅ | | ✅ | ✅ | ✅ | ✅ | ✅ |
| 5 | 非 IT 部門で SaaS 利用 | ✅ | | ✅ | | ✅ | | | ✅ | ✅ |

# メールヘッダの読みかた


RFC5322

# メールヘッダの読みかた 最重要ポイント 3点

## (1) 到着順に下から上　(2) 行頭が空白なら前の行からの続き
## (3) Authentication-Results が送信ドメイン認証の結果


受信者に近い

```
Received: from example.com mta3.example.jp
    by mta4.example.jp with ESMTP id 4AJ0BDme1350   ;
Received: from example.com mta2.example.jp
    by mta3.example.jp with ESMTP id 4AJ0BDD51989   7
Authentication-Results: incoming.example.jp;
      spf=pass smtp.mailfrom=iij-taro@example.jp;
      dkim=pass header.i=@example.jp;
      header.from=iij-taro@example.jp; dmarc=pass
Received: from mta1.example.jp
    by mta2.example.jp with ESMTP id 4AJ0BBPK7128
```

差出人に近い

# 電子メール しくじり先生 実話集

アンチパターンを学んで勘所を掴んでほしい


# (問題 1) この SPF レコードのおかしな点を指摘してください

**SPF か DKIM に対応せよ**

難易度 ★☆☆

```
example.jp.    IN TXT
   "v=spf1 ipv4:192.0.2.0/28  ipv6: 2001:DB8::/124 -all"
```

(実際は一行)

# (正解 1) この SPF レコードのおかしな点を指摘してください

難易度 ★☆☆

## SPF レコードの書式が誤っている

- 設定したら必ず複数の事業者にメールを送信して確認するとよい

```
example.jp.    IN TXT
    "v=spf1 ipv4:192.0.2.0/28  ipv6: 2001:DB8::/124 -all"
    "v=spf1 ip4:192.0.2.0/28 ip6:2001:DB8::/124 -all"
```

(実際は一行)

メカニズム(mechanism) は
ip4: ip6: が正しい ("v" は不要)

メカニズムと値の間に
スペースは入れない

RFC7208 Sender Policy Framework (SPF)
https://datatracker.ietf.org/doc/html/rfc7208

# (問題 2) このSPFレコードのおかしな点を指摘してください

**SPF か DKIM に対応せよ**

難易度 ★☆☆

```
example.jp.    IN TXT    "v=spf1 ip4:192.0.2.0/28 -all"
example.jp.    IN TXT    "v=spf1 include:spf.example.jp -all"
```

# (正解 2) この SPF レコードのおかしな点を指摘してください

難易度 ★☆☆

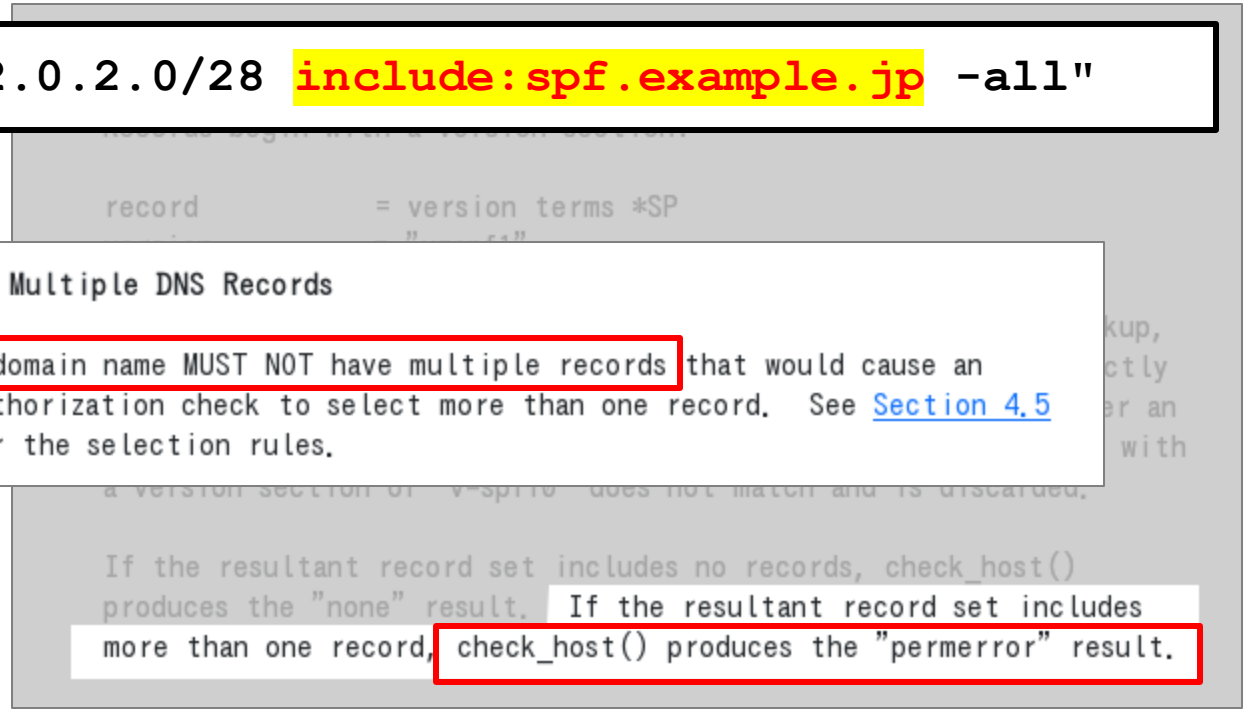
## SPF レコードの書式が誤っている

- 宛先の実装によってはエラーになったりならなかったりするので要注意

```
example.jp.    IN TXT    "v=spf1 ip4:192.0.2.0/28 -all"
~~example.jp.    IN TXT    "v=spf1 include:spf.example.jp -all"~~
```

```
example.jp.    IN TXT    "v=spf1 ip4:192.0.2.0/28 include:spf.example.jp -all"
```

**SPF レコードは必ず一行**
**(2行以上は permerror)**




RFC7208 §3.2 Multiple DNS Records
https://datatracker.ietf.org/doc/html/rfc7208#section-3.2

# (問題 3) このメールヘッダのおかしな点を指摘してください

難易度 ★★☆

**RFC5322 に準拠せよ**

```
To: iij-hanako@example.com
Subject: Internet Week 2024
Date: Tue, 26 Nov 2024 10:20:34 +0900
Content-Type: text/plain; charset="iso-2022-jp"
Content-Transfer-Encoding: 7bit

（本文省略）
```

# (正解 3) このメールヘッダのおかしな点を指摘してください

難易度 ★★☆

## From は RFC5322 で必須のヘッダ

- メーラーで作成してから比較すると分かりやすい

```
From: iij-taro@example.jp
To: iij-hanako@example.com
Subject: Internet Week 2024
Date: Tue, 26 Nov 2024 10:20:3
Content-Type: text/plain; char
Content-Transfer-Encoding: 7bi

（本文省略）
```

| Field | Min number | Max number | Notes |
|---|---|---|---|
| trace | 0 | unlimited | Block prepended - see 3.6.7 |
| resent-date | 0* | unlimited* | One per block, required if other resent fields are present - see 3.6.6 |
| resent-from | 0 | unlimited* | One per block - see 3.6.6 |
| resent-sender | 0* | unlimited* | One per block, MUST occur with multi-address resent-from - see 3.6.6 |
| resent-to | 0 | unlimited* | One per block - see 3.6.6 |
| resent-cc | 0 | unlimited* | One per block - see 3.6.6 |
| resent-bcc | 0 | unlimited* | One per block - see 3.6.6 |
| resent-msg-id | 0 | unlimited* | One per block - see 3.6.6 |
| orig-date | 1 | 1 | |
| from | 1 | 1 | See sender and 3.6.2 |
| sender | 0* | 1 | MUST occur with multi-address from - see 3.6.2 |
| reply-to | 0 | 1 | |

RFC5322 §3.6 Field Definitions
https://datatracker.ietf.org/doc/html/rfc5322#section-3.6

# (問題 4) このメールヘッダのおかしな点を指摘してください

難易度 ★★☆

**RFC5322 に準拠せよ**

```
From: iij-taro@example.jp
To: iij-hanako@example.com
Subject: Internet Week 2024 のお知らせ
Date: Tue, 26 Nov 2024 10:23:45 +0900
Content-Type: text/plain; charset="iso-2022-jp"
Content-Transfer-Encoding: 7bit

（本文省略）
```

# (正解 4) このメールヘッダのおかしな点を指摘してください

難易度 ★★☆

## 非 ASCII 文字は正しくエンコードする

- メール送信プログラムを自作しているケースでよく見かける

```
From: iij-taro@examp
To: iij-hanako@example.com
Subject: Internet Week 2024 のお知らせ
                                    45 +0900
                                    rset="iso-2022-jp"
```

=?UTF-8?B?44Gu44GK55+l44KJ44Gb?=

3.6.5. Informational Fields

The informational fields are all optional. The "Subject:" and "Comments:" fields are unstructured fields as defined in section 2.2.1, and therefore may contain text or folding white space. T "Keywords:" field contains a comma-separated list of one or more words or quoted-strings.

```
subject         =   "Subject:" unstructured CRLF

comments        =   "Comments:" unstructured CRLF
```

2.2.1. Unstructured Header Field Bodies

Some field bodies in this specification are defined simply as "unstructured" (which is specified in section 3.2.5 as any printable US-ASCII characters plus white space characters) with no further restrictions. These are referred to as unstructured field bodies. Semantically, unstructured field bodies are simply to be treated as a single line of characters with no further processing (except for "folding" and "unfolding" as described in section 2.2.3).

RFC5322 §2.2.1 Unstructured Header Field Bodies
https://datatracker.ietf.org/doc/html/rfc5322#section-2.2.1

※ RFC6532 の SMTPUTF8 (SMTP 拡張) に対応している場合は UTF-8 のまま送信できるケースはあるが宛先 MTA の実装依存

# (問題 5) このメールのおかしな点を指摘してください

難易度 ★★★

```
From: iij-taro@example.jp
To: iij-hanako@example.com
Subject: Internet Week 2024 =?UTF-8?B?44Gu44GK55+l44KJ44Gb?=
Date: Tue, 26 Nov 2024 10:26:11 +0900
Content-Type: multipart/alternative; boundary="koko"

--koko
Content-Type: text/plain; charset="us-ascii"

Here is the mail body.

--koko
Content-Type: application/pdf; name="iw2024.pdf"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="iw2024.pdf"

JVBERi0xLjMKMyAwIG9iago8PC9UeXBlI...(省略)
```

# (正解 5) このメールのおかしな点を指摘してください

## Content-Type の宣言が誤っている、MIME を閉じていない

難易度 ★★★

```
From: iij-taro@example
To: iij-hanako@example
Subject: Internet Week
Date: Tue, 26 Nov 2024 10:20:11 +0900
Content-Type: multipart/alternative; boundary="koko"

--koko
Content-Type: tex

Here is the mail

--koko
Content-Type: appl
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="iw2024.pdf"

JVBERi0xLjMK
--koko--
```

**multipart/mixed; が正しい**

(alternative は HTML メールパートなど
本文と同じ内容を別表示できるものに限る)

**改善の余地がある※業務アプリが送信するメールでたまに見る**

(メーラーで見てもいい感じに修復するため気づきづらい)

**MIME は区切り文字のあとに必ず "--" で閉じる**

※ RFC2045～2049 Multipurpose Internet Mail Extensions (MIME)

https://datatracker.ietf.org/doc/html/rfc2045

https://datatracker.ietf.org/doc/html/rfc2046

https://datatracker.ietf.org/doc/html/rfc2047

https://datatracker.ietf.org/doc/html/rfc2048

https://datatracker.ietf.org/doc/html/rfc2049

# バリデーション(検証)方法

電子メール しくじり先生にならないために


# SPF レコード検証ツール

- **yenma -** https://github.com/iij/yenma オススメ
  - IIJ が OSS で公開している milter プログラム、./tools 以下に spfeval コマンドが同梱
  - メールアドレスと IP アドレスを与えて SPF の評価結果・エラーを確認できる

```
$ ./spfeval iij-taro@example.com 192.0.2.1
iij-taro@example.com 192.0.2.1 pass

$ ./spfeval iij-hanako@example.jp 2001:db8::1
info: over 10 mechanisms with dns look up evaluated: sender=example.jp, domain=example.jp
iij-hanako@example.jp 2001:db8::1 permerror
```

- **spf-tools -** https://github.com/spf-tools/spf-tools
  - SPF レコードをルックアップして展開表示できる
  - エラーは報告されない

```
$ ./despf.sh example.net
Getting spf.example.net
ip4:192.0.2.2
ip6:2001:db8::/124
```

- **オンラインで確認できるサイトもある**
  - https://www.naritai.jp/check_spf.html
  - https://mxtoolbox.com/
  - オンラインツールは入力した情報を Web サイトに渡すことになるので注意

# DKIM 署名検証ツール

- **OpenDKIM - http://www.opendkim.org/**
  - The Trusted Domain Project が OSS で公開している DKIM 署名・検証 milter プログラム
  - 署名済みのメールを与えて DKIM の検証結果が確認できる opendkim-testmg が同梱
  - 問題なければ何も報告されない

```
$ opendkim-testmsg < sample.eml
$ echo $?
0

$ opendkim-testmsg < sample2.eml
opendkim-testmsg: dkim_eom(): Bad signature
```

- **dkimverify - https://launchpad.net/dkimpy** オススメ
  - Python の DKIM 実装
  - 署名済みのメールを与えて DKIM の検証結果が確認できる
  - Linux ディストリビューションによってはパッケージがある

```
$ dkimverify < sample.eml
signature ok

$ dkimverify --index 2 < sample2.eml
signature verification failed
```

- **オンラインで確認できるサイトもある**
  - https://www.naritai.jp/notice_check_dmarc.html
  - https://mxtoolbox.com/
  - オンラインツールは入力した情報を Web サイトに渡すことになるので注意

# メールそのものの検証

## 宛先の利用者が使ってそうな複数の MUA (メーラー) で可能な限り確認する

### 無償製品・OSS

- Thunderbird
- Claws Mail (Sylpeed)
- Roundcube (Web メール)
- mutt

### 商用製品

- Outlook
- Becky!

### Web メール

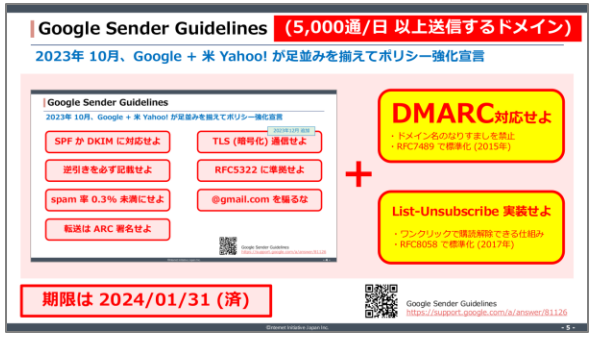
# 前半パートのまとめ

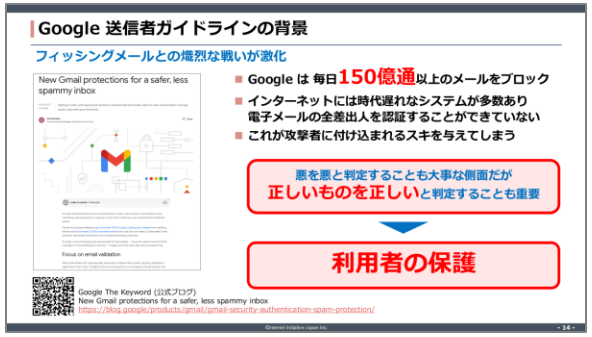
## メールシステムの運用は、送信側の立場と受信側の立場とでマナーや対策が表裏一体

**たかがメール**
**されどメール**

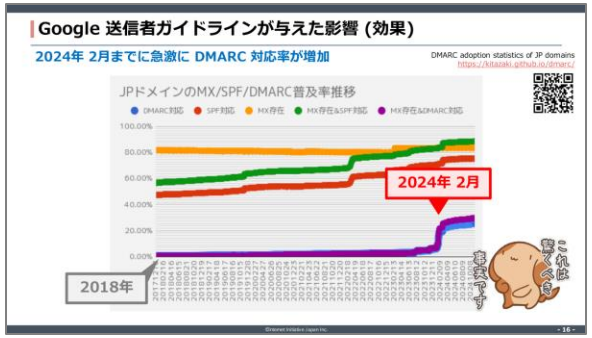
**送信ドメイン認証で**
**しっかり守る**

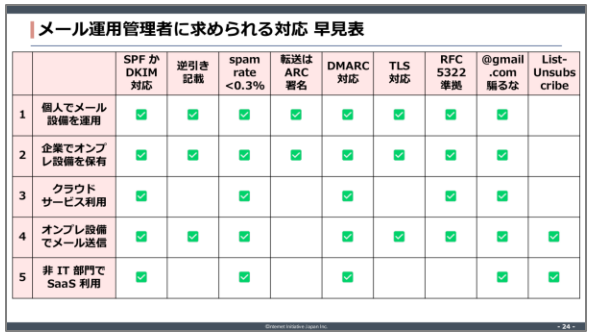
### ■ 正しく届けるためには、まず正しい形で送信




### ■ 悪に付け入れられるスキを与えない



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