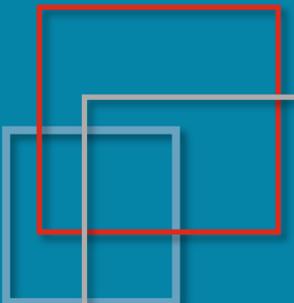


正しいメールを送るためのRFC復習 ～スパマーと間違われないうために～

Vade Japan株式会社

関根 章弘



自己紹介

関根 章弘



- 1995年頃 インターネット接続ブーム時に構築支援を行う要件を満たすために必要に迫られてsendmail.cfをカスタマイズ
- 2000年頃 商用サービス向けの大規模メールシステムの構築に関わる
- 海外のメール製品ベンダに所属し日本のサービスに導入
- 2003年 迷惑メール対策カンファレンスの運営に携わる
- 2019年 Vade Japanに入社、顧客サポートを担当

自己会社紹介

- Vade Japan株式会社（本社はフランス共和国 リール）
- AIエンジンを用いた予測的メール防衛の世界的リーダー
- 全世界で14億を超えるメールボックスを保護
- 日本国内にメール脅威の分析を行う技術チームを保有

本社オフィス外観



セッションの目的

古き良き時代にデザインされたメールシステムは、多くのMTA/MUAが良きに計らってくれているために、なんとなく送っても大部分のメールは問題なく届けられています。しかし、その中にはルール違反でエラーになっても仕方がないようなものも見られます。

しかし、スパムやフィッシングが大量に送られるようになり、最近ではルール違反のメールは受信しないという方針のシステムもあります。

そのような厳格なシステムにブロックされていないようにRFCの内容をチェックします。間違いやすい点を例示して、正しいメールを確認します。

内容

1. メールの基本構造を確認します
2. メールを構成する各パートに対応したRFCの概要を確認します
 - SMTP - 5321
 - Message Format - 5322
 - MIME - 2045, 2046, 2047, 2048, 2049
3. 実際に送信されているメールでベストプラクティス、バッドプラクティスを確認します

※RFCの定義は非常に多岐にわたっています。このセッションでは細かな解釈には踏み込まず、基本的な項目を取り上げます

メールの基本構造



メール関連RFC (1)

メールの構造と対応するRFC

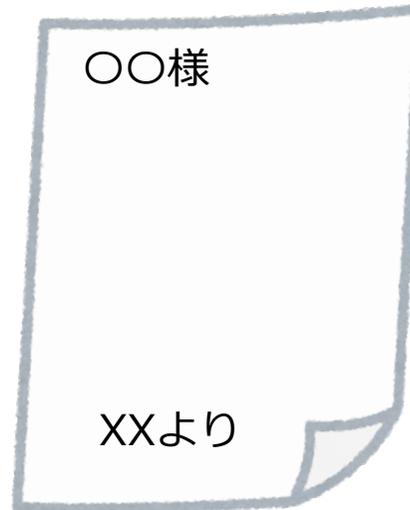
エンベロープ



5321
Simple Mail Transfer Protocol



メール本体



5322 - Internet Message Format
2045, 2046, 2047, 2048, 2049 –
Multipurpose Internet Mail Extensions
(MIME)

メール関連RFC (1)

メールの構造と対応するRFC

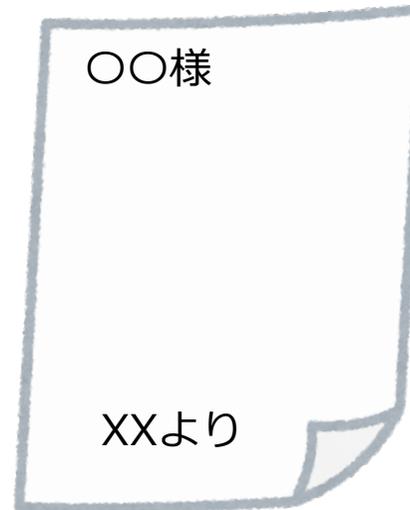
エンベロープ



5321
Simple Mail Transfer Protocol

SPF

メール本体

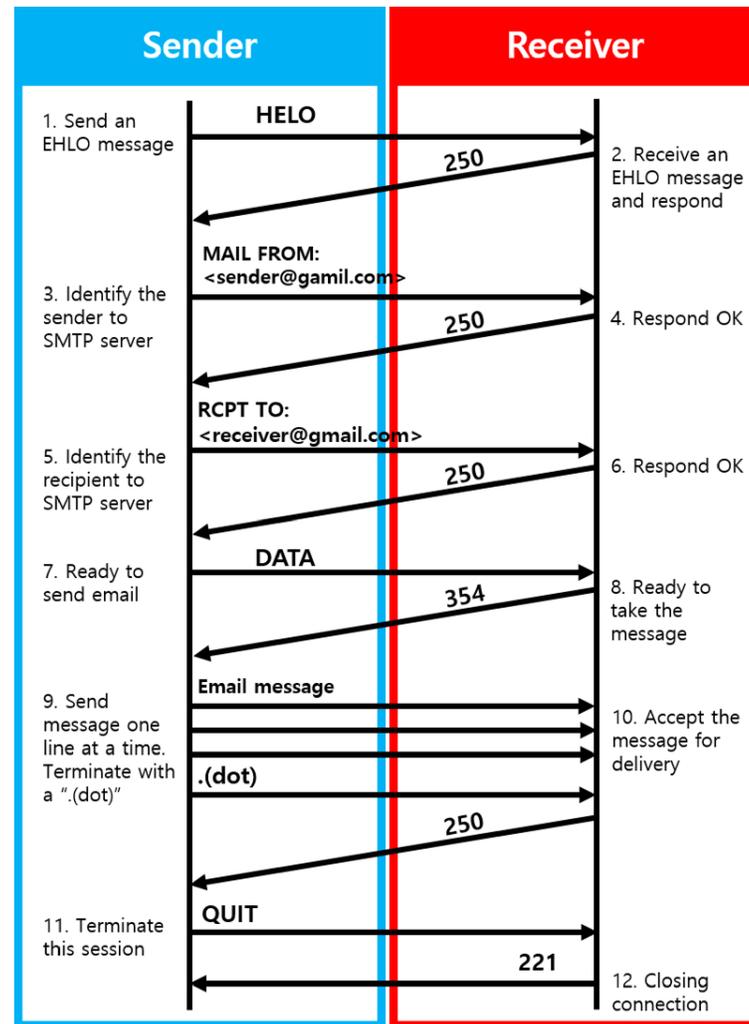


5322 - Internet Message Format
2045, 2046, 2047, 2048, 2049 –
Multipurpose Internet Mail Extensions
(MIME)

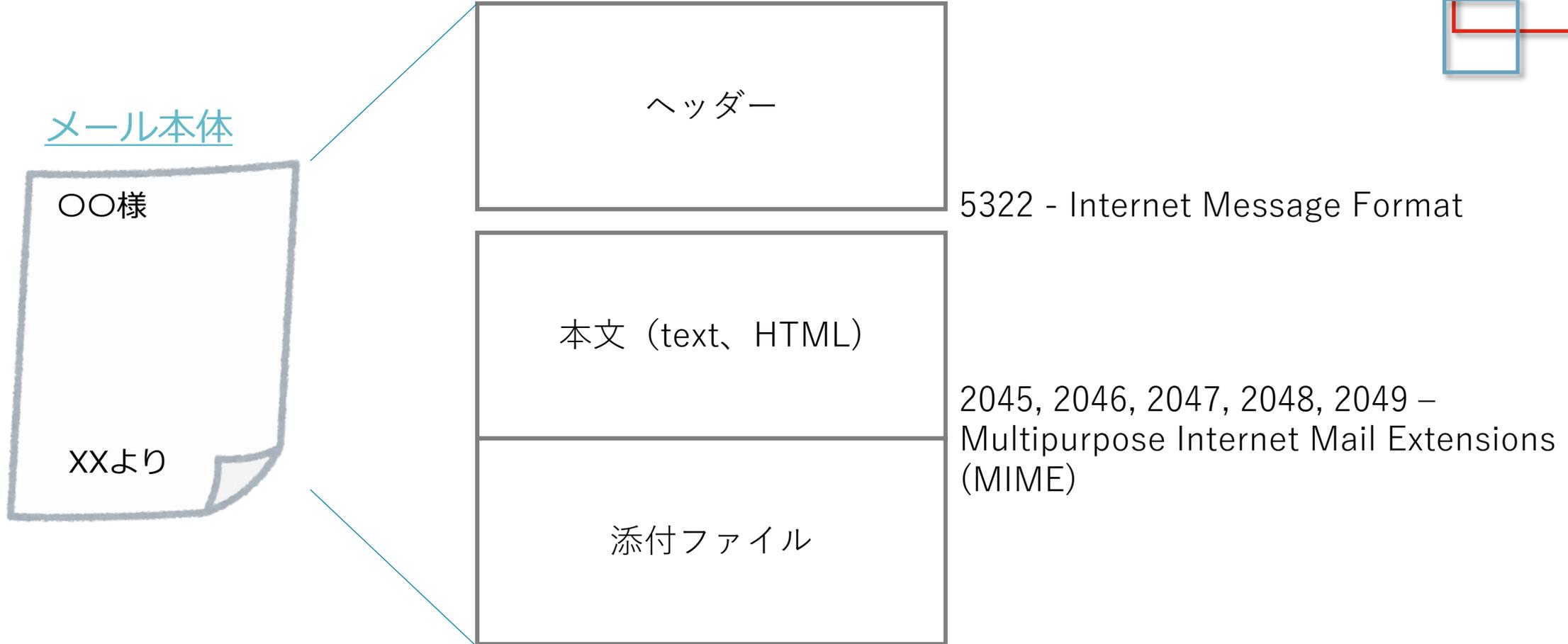
DKIM

RFC5321 Simple Mail Transfer Protocol

- メールを転送する（送る）ための約束事
- クライアント-サーバ間のコマンド/レスポンスを定義しています
- 何度も更新、修正、拡張され、現在は認証、暗号化、バイナリ・データ転送、および国際化された電子メールアドレスのためのさまざまな拡張機能を持つ、拡張可能な構造を持っています



メール関連RFC (2)



RFC5322 Internet Message Format

- メールの形式を定義している
 - ヘッダー、本文の構成
 - アドレス、日付などのフォーマット

- メールの形式

```
message      = (fields / obs-fields)
               [CRLF body]

body         = (*(998text CRLF) 998text) / obs-body

text        = %d1-9 /           ; Characters excluding CR
               %d11 /           ; and LF
               %d12 /
               %d14-127
```

メール(message)はヘッダー(fields)とボディから構成される

ボディに使える文字はCR、LFを除いたASCII文字

ヘッダー

- 必須のヘッダー
 - Date
 - From
 - Message-ID
- 件名や宛先は無くても良い
- 複数書いてはいけないヘッダーがある
 - Gmailは違反したメールをブロック

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	
to	0	1	
cc	0	1	
bcc	0	1	
message-id	0*	1	SHOULD be present - see 3.6.4
in-reply-to	0*	1	SHOULD occur in some replies - see 3.6.4
references	0*	1	SHOULD occur in some replies - see 3.6.4
subject	0	1	
comments	0	unlimited	
keywords	0	unlimited	
optional-field	0	unlimited	

ヘッダー

- 宛先ヘッダー (To/Cc/Bcc)
 - ヘッダーには1つ以上のアドレスを書く (one or more addresses)
 - 複数のアドレスはカンマ区切りで1つのヘッダーに書く
 - ヘッダーは無くても良い(0~1個)
アドレスが無ければヘッダーを付けない

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	
to	0	1	
cc	0	1	
bcc	0	1	
message-id	0*	1	SHOULD be present - see 3.6.4
in-reply-to	0*	1	SHOULD occur in some replies - see 3.6.4
references	0*	1	SHOULD occur in some replies - see 3.6.4
subject	0	1	
comments	0	unlimited	
keywords	0	unlimited	
optional-field	0	unlimited	

ヘッダー

- Message-ID

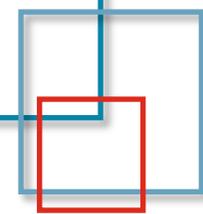
- メッセージに固有の識別子
- リプライ元の特定などに利用
- フォーマットの定義はシンプル
- ただし

The message identifier (msg-id) itself MUST be a globally unique identifier for a message.

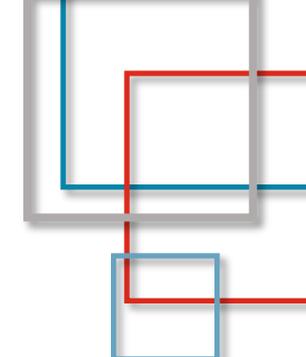
送信者はグローバルに一意的な識別子であることを保証する必要がある

→ @の右側にドメイン名やIPアドレスを入れることが推奨されている

```
message-id      = "Message-ID:" msg-id CRLF
in-reply-to    = "In-Reply-To:" 1*msg-id CRLF
references     = "References:" 1*msg-id CRLF
msg-id         = [CFWS] "<" id-left "@" id-right ">" [CFWS]
id-left        = dot-atom-text / obs-id-left
id-right       = dot-atom-text / no-fold-literal / obs-id-right
no-fold-literal = "[" *dtext "]"
```



RFC2045-2049 MIME



- Multipurpose Internet Mail Extensions
メールで英語(ASCII)以外のコンテンツを扱えるようにするための拡張
- RFC 2045, specifies the various headers used to describe the structure of MIME messages.
- RFC 2046, defines the general structure of the MIME media typing system and defines an initial set of media types.
- RFC 2047, describes extensions to RFC 822 to allow non-US-ASCII text data in Internet mail header fields.
- RFC 2048, specifies various IANA registration procedures for MIME-related facilities.
- RFC 2049, describes MIME conformance criteria as well as providing some illustrative examples of MIME message formats,

RFC2045 MIME Part One

- MIMEヘッダの定義
- メッセージヘッダでMIMEであることを宣言
 - 例 : MIME-Version: 1.0
Content-Type: text/plain; charset="Shift_JIS"
Content-Transfer-Encoding: base64
 - Content-Type: データの説明、テキストやファイル単体か、複数要素か
 - text, image, audio, video, application, message, multipart, 他
 - Content-Transfer-Encoding: エンコーディング（符号化）の種別
 - 7bit, 8bit, binary, quoted-printable, base64

RFC2046 MIME Part Two

- メディアタイプ
- Content-Typeに指定するタイプ、サブタイプの詳細を説明
 - タイプ : text, image, audio, video, application, message, multipart
- 複数要素で構成される場合にはパラメータで区切り文字列を指定します
Content-Type: multipart/alternative; boundary="1fbcea0106f295f9d6ac352fb6584b8e4"

RFC2046 MIME Part Two

```
From: Nathaniel Borenstein <nsb@bellcore.com>
To: Ned Freed <ned@innosoft.com>
Date: Sun, 21 Mar 1993 23:56:48 -0800 (PST)
Subject: Sample message
MIME-Version: 1.0
Content-type: multipart/mixed; boundary=simple boundary
```

This is the preamble. It is to be ignored, though it is a handy place for composition agents to include an explanatory note to non-MIME conformant readers.

--simple boundary

This is implicitly typed plain US-ASCII text. It does NOT end with a linebreak.

--simple boundary

Content-type: text/plain; charset=us-ascii

This is explicitly typed plain US-ASCII text. It DOES end with a linebreak.

--simple boundary--

シンプルなmultipart構成例

- パラメータで区切り文字列を指定します
“simple boundary”
- 先頭に“--”を付けて使用します
- 終端は後ろにも“--”を付けます

※複数階層の複雑な例がRFC2049 Appendix A にあります

RFC2047 MIME Part Three

- メールヘッダーで非ASCII文字を扱う方法
- ヘッダーを変えてしまうと互換性がなくなってしまうため、ヘッダー値(Header Field Body)を印刷可能なASCII文字に変換します
- エンコードされたデータのフォーマットとエンコードの方法が定義されています
- エンコードは2種類
 - "B" encoding - BASE64エンコーディング
データを6bitずつの64進数に分割して、数字、英字と一部の記号64文字で表します。
 - "Q" encoding - Quoted-Printableに類似
8ビットのデータを =XX のような16進数2桁の形式で表します。7ビットの印字可能な文字は変換されません。

RFC2047 MIME Part Three

- 例 (RFC2047 - 8. Examples より)

From: =?US-ASCII?Q?Keith_Moore?= <moore@cs.utk.edu>

To: =?ISO-8859-1?Q?Keld_J=F8rn_Simonsen?= <keld@dkuug.dk>

CC: =?ISO-8859-1?Q?Andr=E9?= Pirard <PIRARD@vm1.ulg.ac.be>

Subject: =?ISO-8859-1?B?SWYgeW91IGNhbiByZWZkIHRoaXMgeW8=?=
=?ISO-8859-2?B?dSB1bmRlcnN0YW5kIHRoZSBleGFtcGxlG=?=

- デコード結果

From: Keith Moore

To: Keld Jørn Simonsen

Cc: André Pirard

Subject: If you can read this you understand the example.

RFC2047 MIME Part Three

日本語への適用例

Subject: サンプル



- Bエンコーディング

Subject: =?UTF-8?B?44K144Oz44OX44OrCg==?=

- Qエンコーディング

Subject: =?UTF-8?Q?=E3=82=B5=E3=83=B3=E3=83=97=E3=83=AB?=

※日本語にはBエンコーディングが効率的なため、一般的に利用されています。

サンプル

バッドプラクティス

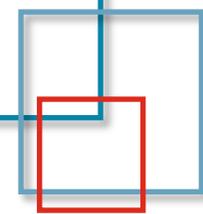
必須ヘッダがない

- Dateがない

```
for <aaaaaaaa@xxxxxxxx.xx.jp>; Thu, 26 Oct 2023 00:07:56 +0900
Received: (from nobody@localhost)
  by cp24-web-asg.1-0246a39c017e97696 (8.14.7/8.14.7/Submit) id 39PF7ueG022651;
  Thu, 26 Oct 2023 00:07:56 +0900.
Message-Id: <202310251507.39PF7ueG022651@cp24-web-asg.1-0246a39c017e97696>
To: aaaaaaaaa@xxxxxxxx.xx.jp
Subject: =?utf-8?B?44CQ44K4440j440L440844K6V0VTV00BruWkj+...?=
From: info@xxxxxxxx-yyyyyyyy.jp
Mime-Version: 1.0
X-Mailer-Unique-Code:
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: base64

44GT44Gu5bqm44Gv44CQ44K4440j440L440844K6V0VTV00BruWkj+S8ke0BvzIwMjMg44Cc56We
44Gh44KD44KT77yG5rWB5pifIOelnTMw5q2z77yB440P440D440U4408440Q440844K5440H4408
```

- Date:とMessage-ID:は忘れずに



ヘッダーのフォーマット不正

メッセージIDがユニークでない

- @以降がプライベートIP

Message-ID: <14893673.102.1693547857043.JavaMail.postfix@192.168.22.246>

- @以降がドメインでない

Message-ID: <6E51BE867EFAC354FC809C3B3EE1AF7B@kmua>

ヘッダーのフォーマット不正

Date: フォーマットは古いRFCと比較して明確に定義されています

- 年は4桁
- タイムゾーンは数字

古いフォーマットの例

Date: 21 Nov 97 09:55:06 GMT

date-time	=	[day-of-week ","] date time [CFWS]
day-of-week	=	([FWS] day-name) / obs-day-of-week
day-name	=	"Mon" / "Tue" / "Wed" / "Thu" / "Fri" / "Sat" / "Sun"
date	=	day month year
day	=	([FWS] 1*2DIGIT FWS) / obs-day
month	=	"Jan" / "Feb" / "Mar" / "Apr" / "May" / "Jun" / "Jul" / "Aug" / "Sep" / "Oct" / "Nov" / "Dec"
year	=	(FWS 4*DIGIT FWS) / obs-year
time	=	time-of-day zone
time-of-day	=	hour ":" minute [":" second]
hour	=	2DIGIT / obs-hour
minute	=	2DIGIT / obs-minute
second	=	2DIGIT / obs-second
zone	=	(FWS ("+" / "-") 4DIGIT) / obs-zone

ヘッダーのフォーマット不正

- From:のメールアドレスに@ドメインがついていない

```
From: <name>  
To: aaaaaaaaa@xxxxxxxx.xx.jp  
Date: Tue, 06 Jun 2023 15:04:23 +0900  
Subject: =?ISO-2022-JP?B?GyRCJUyL0SVIISELJiUkJWsl0TghQk4bKEI=?=  
Message-ID: <a5bfd4f59df570e23c8146cfc2cb55c5@my.domain>  
X-Mailer: dddddddd - Group eMail Vx.y  
X-Priority: 3  
MIME-Version: 1.0  
Content-Type: multipart/mixed;  
  boundary="MIX_VHVllCAwNiBKdW4gMjAyMyAxNTowNDoyMyArMDkwMA=="  
  
This is a multi-part message in MIME format.  
  
--MTX_VHVllCAwNiBKdW4gMiAvMvAxNTowNDoyMvArMDkwMA==
```

mailbox	=	name-addr / addr-spec
name-addr	=	[display-name] angle-addr
angle-addr	=	[CFWS] "<" addr-spec ">" [CFWS] / obs-angle-addr
addr-spec	=	local-part "@" domain

ヘッダーのフォーマット不正

- 宛先 (To/Cc) が空

```
From: <[REDACTED]>  
To: <[REDACTED]>  
Cc:  
Subject: =?iso-2022-jp?B?GyRCIVowMCFb0CtAUTBNTWobKEIgGyRC0C  
Date: Fri, 13 Jan 2023 14:33:51 +0900  
Message-ID: <0930982B56C64334A62A9D0ED056A60A@W102035SD1>  
MIME-Version: 1.0  
Content-Type: text/plain;  
             charset="iso-2022-jp"  
Content-Transfer-Encoding: 7bit
```

```
to           = "To:" address-list CRLF  
cc           = "Cc:" address-list CRLF  
bcc          = "Bcc:" [address-list / CFWS] CRLF
```

ヘッダーのフォーマット不正

- アドレス含めて丸ごとエンコードしてしまっている



📧 IEdhw6tsbGUgTGUgQnJldG9uIDxnLmxlYnJldG9uQGNvb...

2023年5月3日 水曜日 21:57

宛先: 📧 IERVUFVJUyBSw6lteSA8ci5kdXB1aXNAY29vcGV0YmF0LmZyPg==

```
MIME-Version: 1.0
Date: Wed, 3 May 2023 14:57:13 +0200
Content-Language: fr
Message-ID: <db9fd65f-5d21-5f71-2da4-cf14b3454565@coopetbat.fr>
Content-Type: multipart/mixed; boundary="-----0m0EpvzXx0eJjbnDR0qRFgyA"
To: =?UTF-8?B?IERVUFVJUyBSw6lteSA8ci5kdXB1aXNAY29vcGV0YmF0LmZyPg==?=
From: =?UTF-8?B?IEEdhw6tsbGUgTGUgQnJldG9uIDxnLmxlYnJldG9uQGNvb3BldGJhdC5mcj4=??=
Content-Length: 0
-----0m0EpvzXx0eJjbnDR0qRFgyA
```



To: DUPUIS Rémy <r.dupuis@coopetbat.fr>
From: Gaëlle Le Breton <g.lebreton@coopetbat.fr>

mailbox	=	name-addr / addr-spec
name-addr	=	[display-name] angle-addr
angle-addr	=	[CFWS] "<" addr-spec ">" [CFWS] / obs-angle-addr
addr-spec	=	local-part "@" domain

Thank you

