
メールヘッダの見方

情報基盤センター

メールヘッダとは

メールヘッダとは、メールの詳細情報が書かれている部分のことです。
具体的には、メールが配送された経路や時間、経由したサーバーなどが記録されています。

普段皆さんが目にする差出人や送信元アドレスは、メールヘッダのほんの一部であり、送信者によっていかようにも詐称出来ます。
一方で、メールヘッダには、送信者が自由に編集できない部分があり、スパムメールの判定材料になります。

下記はスパムメールの一例です。差出人名が「kitasato-u.ac.jp」となっており、本文もおかしな日本語ではありますが、一見すると本学関係者のようにも見えます。本来「kitasato-u.ac.jp」であるはずの本文中URLアドレスには、よく似た「kitasato-u-acjp」という文字が入っています。

あなたのメールボックスがいっぱいです。
webmail.kitasato-u.ac.jp <aono@speedy.com.ar>
送信日時: 2016/08/09 (火) 8:27 **差出人が北里?**
宛先:

あなたのメールボックスがいっぱいです。
780MB **780MB** **おかしな日本語**
Current size Maximum size

あなたは 10 保留中のメールを持っています。あなたのメールボックスには、もはやメッセージを送信または受信することができます。あなたは、あなたが受け取ると電子メールを送信可能にするためにあなたの電子メールアカウントをアップグレードすることです。アップグレードまたは <http://webmail-kitasato-u-acjp.weebly.com> をクリックするには、ここをクリックしてください **怪しげなURLへの誘導**

実際にこのメールのヘッダを見て、迷惑メールと判断するための方法を次に示します。

メールヘッダの読み解き方

Receivedについて

メールヘッダの情報の中で、特に重要なのがReceivedの情報です。
 Received はメールが送信されてきたサーバーの経路を示します。
 経路は下から上に読んでいきます（基本的に一番下が送信元、一番上が宛先）。
 よって、送信元を確認する場合は、一番下の**Received from**の情報を見ます。
 ※一番下を見てもよく分からない際は、下から二番目、三番目を見ると分かる場合があります。

宛先

Received: from kmvnc.kitasato-u.ac.jp (localhost [127.0.0.1])
 by kmvnc.kitasato-u.ac.jp (deepsmtpd.o 3.7.0)
 with LDelivery for <kinetic@kitasato-u.ac.jp> ;
 Tue, 9 Aug 2016 08:20:59 +0900

Received: from mdi.securemx.jp (210.130.202.103 [210.130.202.103])
 by kmvnc.kitasato-u.ac.jp (deepsmtpd.o 3.7.0)
 with ESMTTP id <OID_1470698254502743_0aono@speedy.com.ar> for <
 <kinetic@kitasato-u.ac.jp>;
 Tue, 9 Aug 2016 08:20:50 +0900

Received:
 by mdi.securemx.jp (mx-mdi1501) id u78NKnw020259;
 Tue, 9 Aug 2016 08:20:50 +0900
 Authentication-Results: mx.securemx.jp; spf=pass smtp.mailfrom=aono@speedy.com.ar; <
 dkim=none; dkim-adsp=none header.from=aono@speedy.com.ar; dmarc=none <
 header.from=aono@speedy.com.ar

Received: from if05-mail-fb08-mia.mta.terra.com (if05-mail-fb08-mia.mta.terra.com <
 [208.84.243.192])
 by mx.securemx.jp (mx-mi1510) id u78NKdmV010462;
 Tue, 9 Aug 2016 08:20:40 +0900

Received: from mail-smtp10-mia.tpn.terra.com (unknown [10.235.200.41])
 by mail-fb08-mia.tpn.terra.com (Postfix)
 with ESMTTP id 60BA882D3968;
 Mon, 8 Aug 2016 23:20:38 +0000 (UTC)
 X-Terra-Karma: -2%
 X-Terra-Hash: c1d21d10ca1f493165f9960e36ea2c27

送信元

Received: from localhost (mail-web14-mia.terra.com [208.84.242.152]) (authenticated <
 user aono!speedy!m) 送信元 送信元IPアドレス
 by mail-smtp10-mia.tpn.terra.com (Postfix)
 with ESMTTP id 40F82C001939;
 Mon, 8 Aug 2016 23:20:36 +0000 (UTC)

この例の場合、「mail-web14-mia.terra.com」が送信元となります。
 ここで、差出人として表示されていた「webmail.kitasato-u.ac.jp」は
 本来の送信者である「aono@speedy.com.ar」によって偽装されたものであり、
 このメールがスパムメールであると判断出来ます。

あなたのメールボックスがいっぱいです。

webmail.kitasato-u.ac.jp <aono@speedy.com.ar>

送信日時: 2016/08/09 (火) 8:27 偽装された差出人名

メールヘッダの送信元の右側写到あるカッコ内の数字が送信元IPアドレスです。
 さらに、Whois情報検索サイトを利用すると送信者情報を調べる事が出来ます。

Whois情報検索サイトの使い方

(1) Whois情報検索サイト (<https://www.cman.jp/network/support/ip.html>)にアクセスします。

(2) 入手した送信元のIPアドレスを貼り付けて下記の通りチェックを入れ、「管理情報照会実行」をクリックします。

Whois情報検索サイトの使い方

- (3) [結果] 項目の中の[Organization]、[Country]の項目を確認します。
(IPアドレスによってCountryが表示されない場合もあります)

NetRange:	208.84.240.0 - 208.84.247.255
CIDR:	208.84.240.0/21 (マスク範囲)
NetName:	TERRA-NETWORKS-USA2
NetHandle:	NET-208-84-240-0-1
Parent:	NET208 (NET-208-0-0-0-0)
NetType:	Direct Allocation
OriginAS:	AS40260
Organization:	Terra Networks Operations Inc. (TNO-2)
RegDate:	2007-11-30
Updated:	2012-02-24
Ref:	https://whois.arin.net/rest/net/NET-208-84-240-0-1
OrgName:	Terra Networks Operations Inc.
OrgId:	TNO-2
Address:	396 Alhambra Circle, Coral Gables
Address:	Suite S700
City:	Miami
StateProv:	FL
PostalCode:	33134
Country:	US → (アメリカ合衆国)
RegDate:	2006-03-24
Updated:	2014-08-04
Ref:	https://whois.arin.net/rest/org/TNO-2

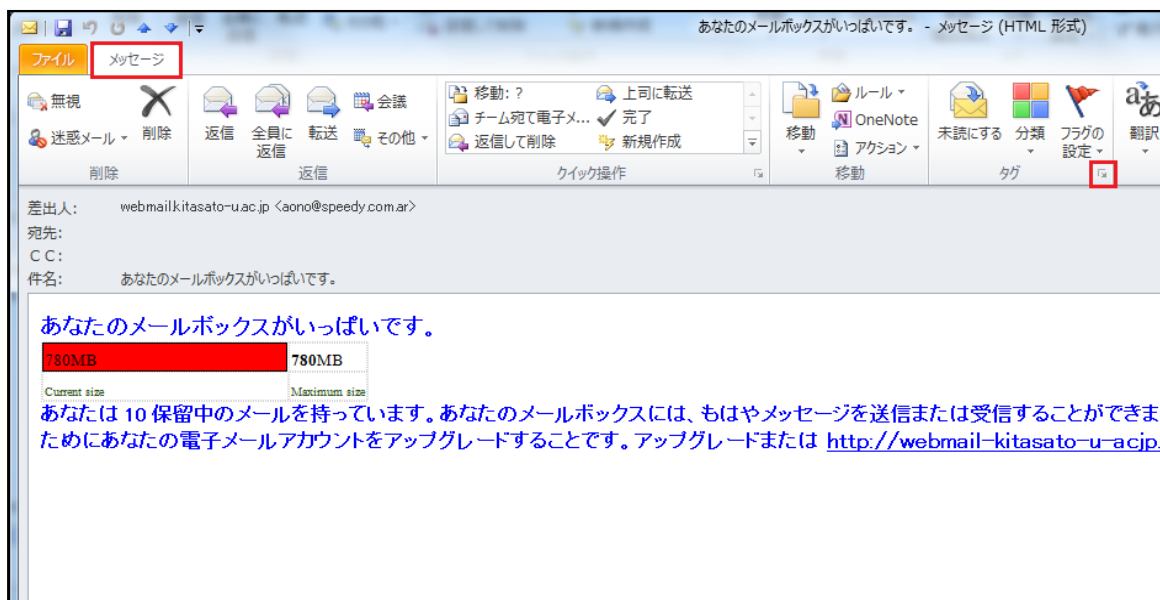
学内ネットワークから送られたメールであれば、通常[Organization]の項目は Kitasato University となります。
さらに、[Country]を見ればアメリカ合衆国のサーバーを経由して送られたことが分かり、このメールがスパムメールであると判断できます。

メールヘッダの読み解き方、Whois情報検索サイトの使い方は以上です。
届いたスパムメールは、そのまま削除するようにしてください。

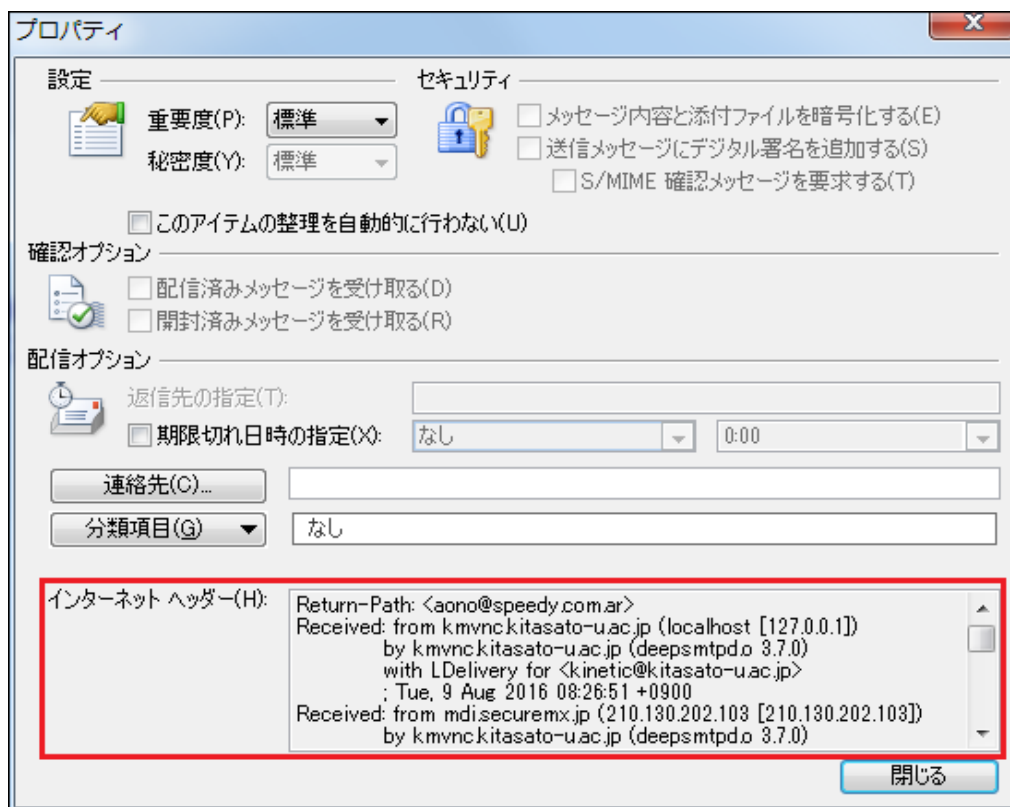
各メーラーでのメールヘッダの表示方法は以下の通りです。

Outlook

- (1) メールをダブルクリックして新しいウィンドウで開き、[メッセージ] タブの [タグ] の右下をクリックします。

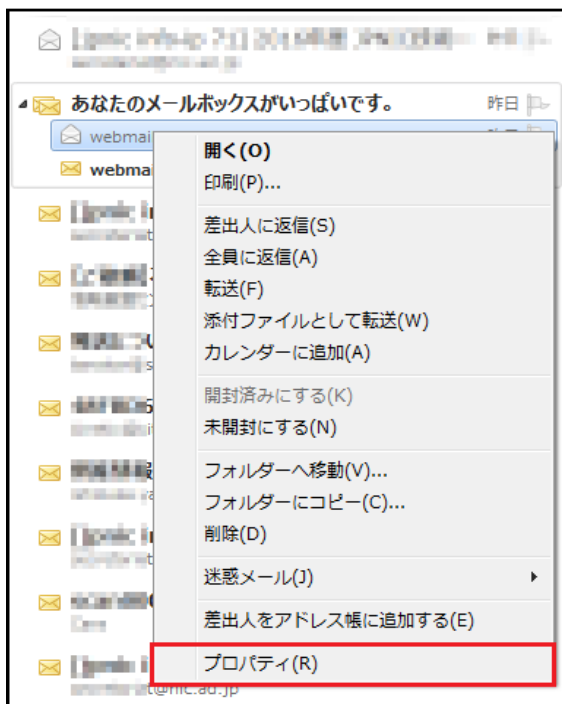


- (2) プロパティが表示されるので、下の項目のインターネットヘッダで参照することが出来ます。



Windows Liveメール

(1) ヘッダを表示させたいメールの上で右クリックをし、 [プロパティ] をクリックします。

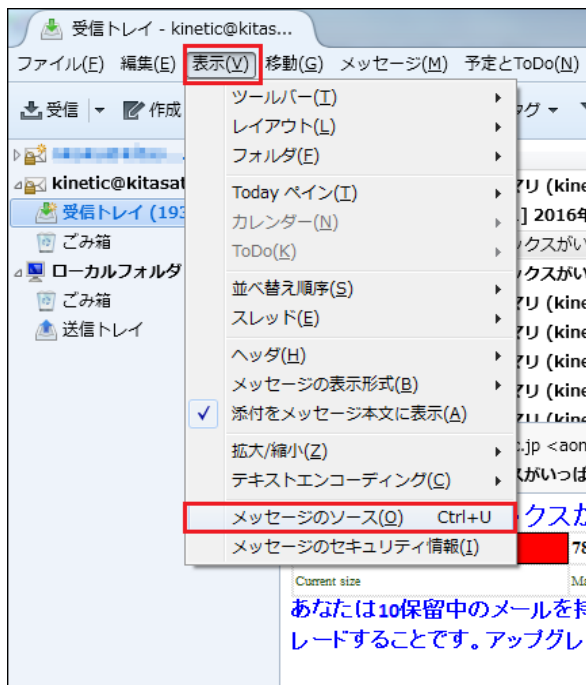


(2) [詳細] タブをクリックするとヘッダを参照できます。
[メッセージのソース] をクリックすると、より大きな画面で見ることができます。

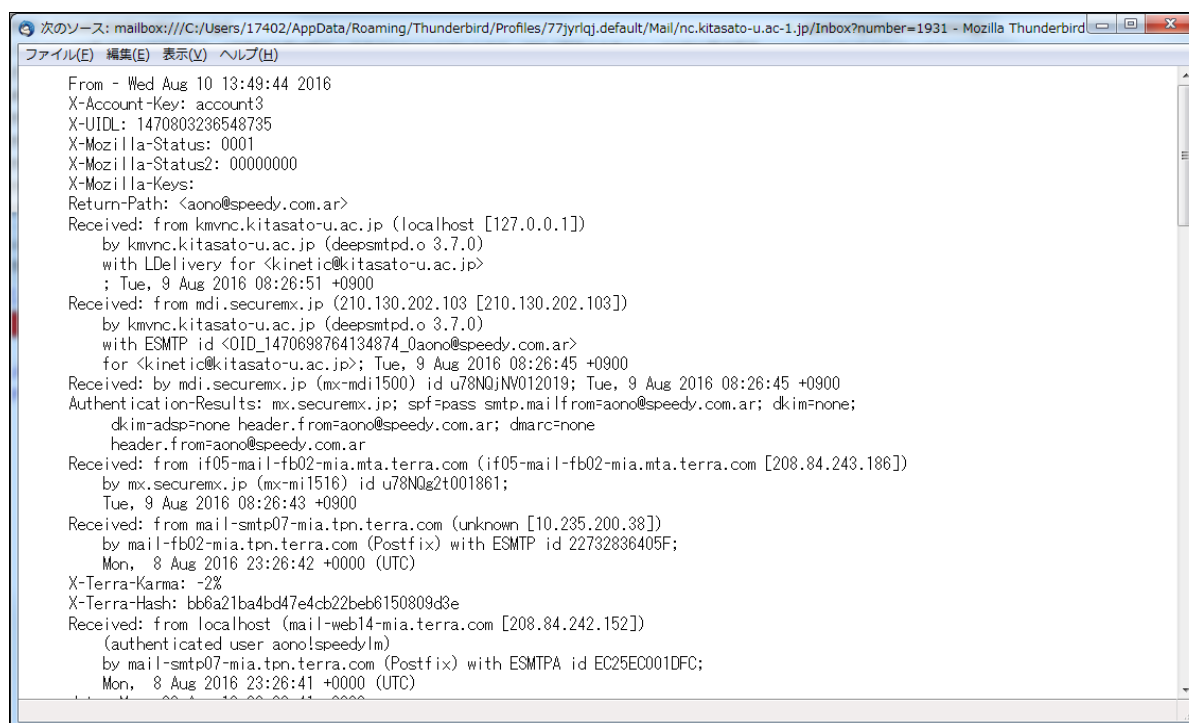


Thunderbird

- (1) メールを表示させた状態で、[表示] タブの [メッセージのソース] をクリックします。
([タブ] が表示されない場合はAltキーを押して表示させてください)



- (2) 新しいウィンドウが開き、ヘッダ情報が表示されます。



Becky

- (1) メールを表示させた状態で、表示部分の下部へカーソルを持っていきます。
[1:t/plain] [0:ヘッダ] が現れたら、[ヘッダ] をクリックします。
(メールに添付ファイルがある場合は最初から[ヘッダ] ボタンが表示されています)



- (2) [ヘッダ] が表示されます。



以上