メールヘッダの見方

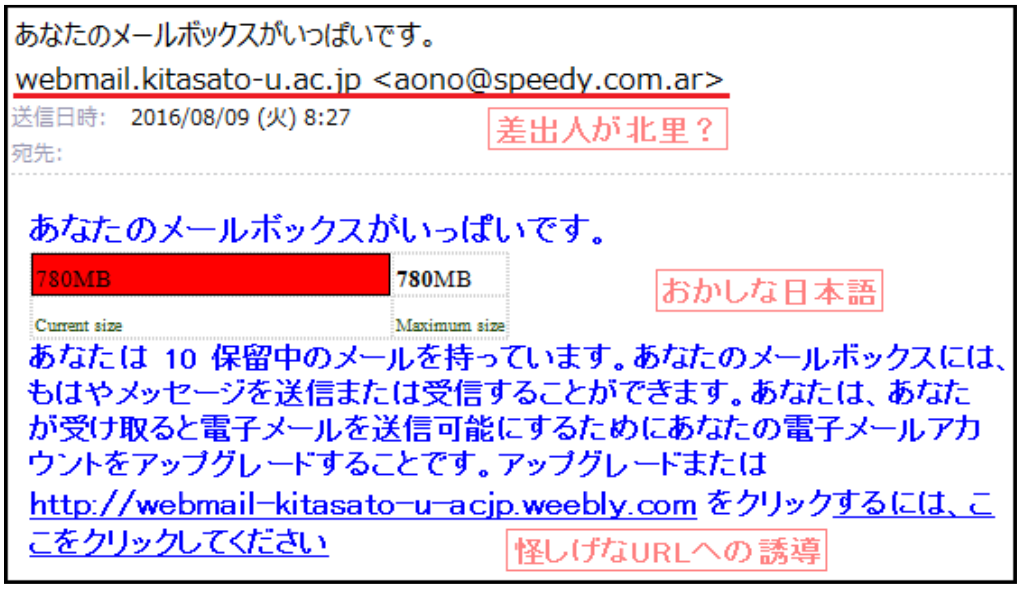
情報基盤センター

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。



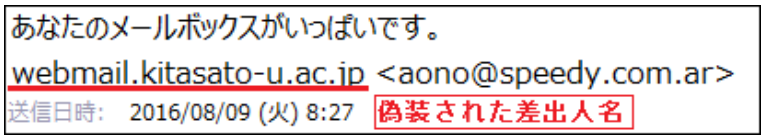
実際にこのメールのヘッダを見て、迷惑メールと判断するための方法を次に示します。

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。

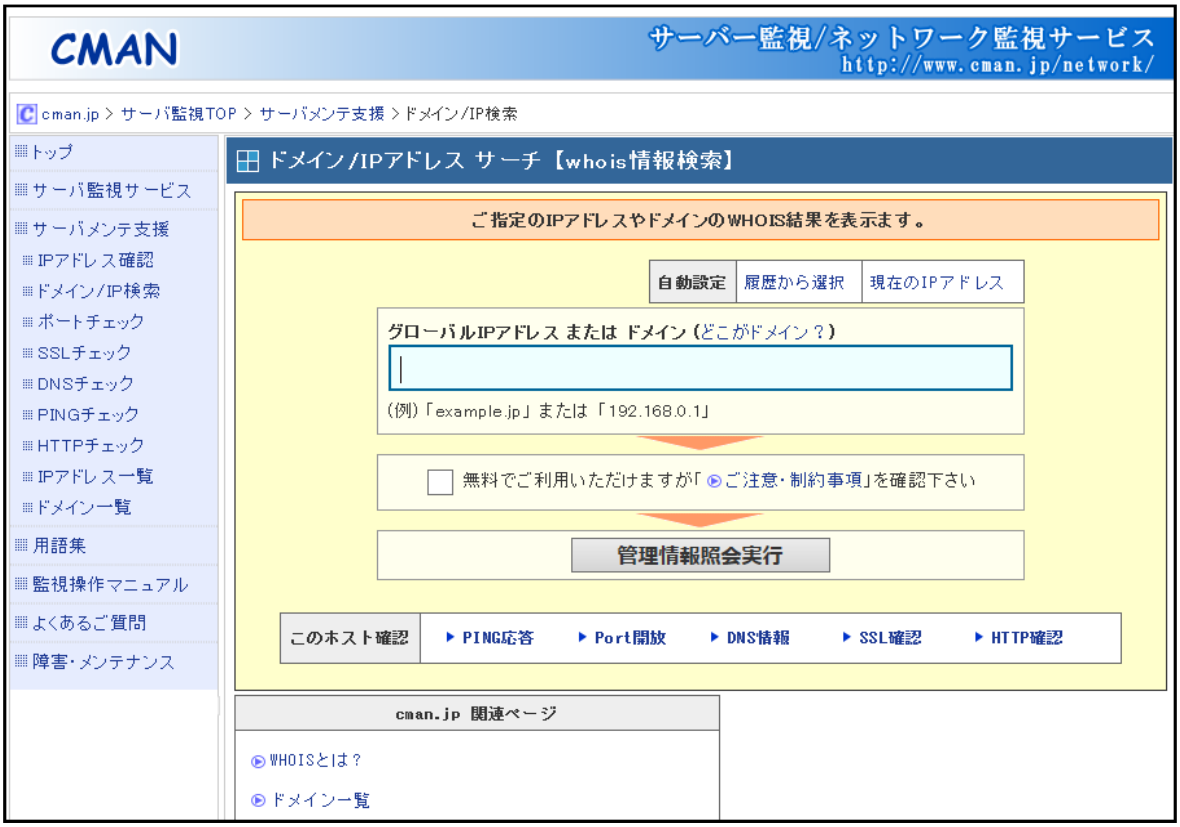
この例の場合、「mail-web14-mia.terra.com」が送信元となります。
ここで、差出人として表示されていた「webmail.kitasato-u.ac.jp」は
本来の送信者である「aono@speedy.com.ar」によって偽装されたものであり、
このメールがスパムメールであると判断出来ます。



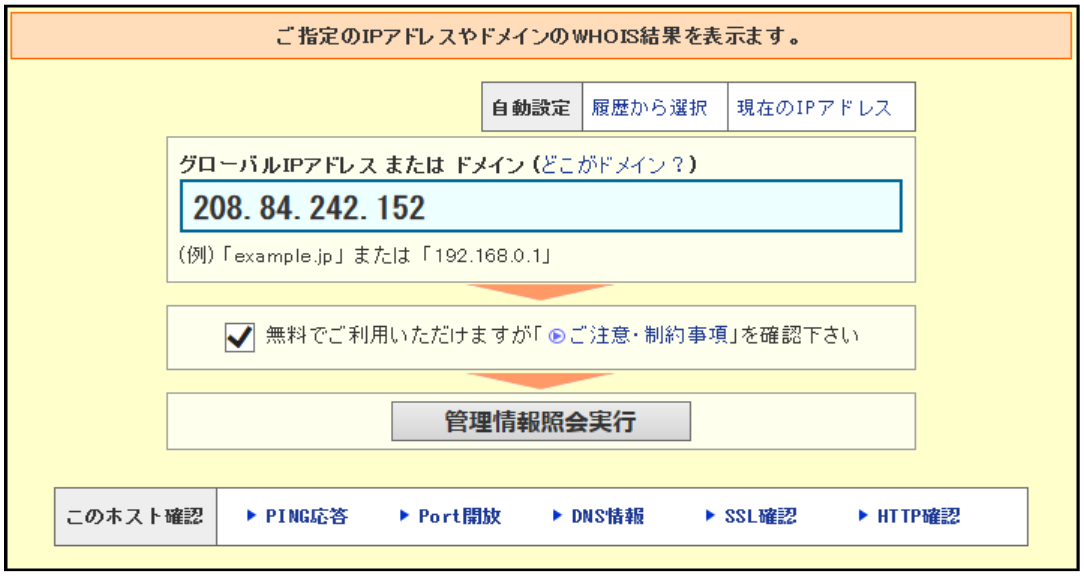
メールヘッダの送信元の右側に書いてあるカッコ内の数字が送信元IPアドレスです。
さらに、Whois情報検索サイトを利用すると送信者情報を調べることが出来ます。

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。

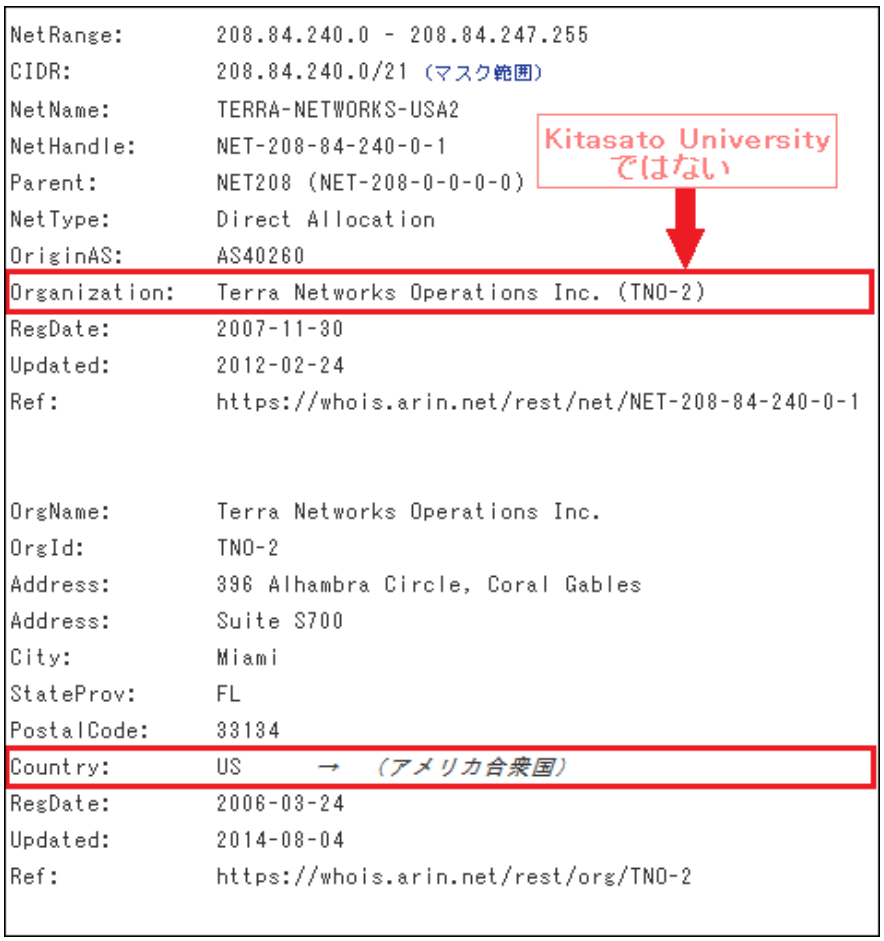


(2)入手した送信元のIPアドレスを貼り付けて下記の通りチェックを入れ、
「管理情報照会実行」をクリックします。



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)



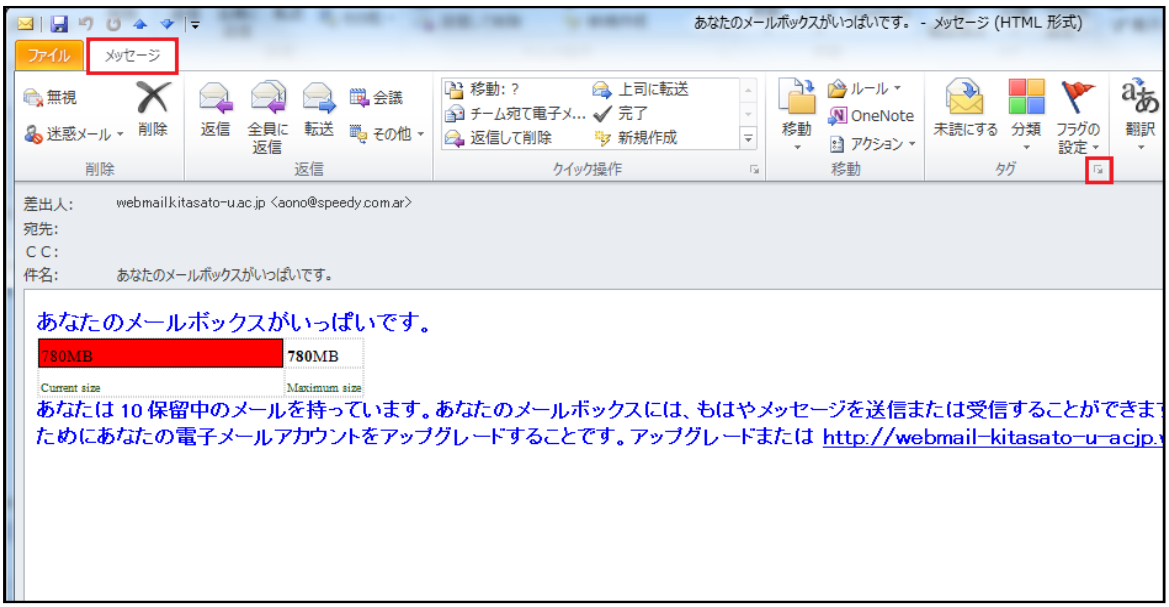
学内ネットワークから送られたメールであれば、通常[Organization]の項目は
Kitasato Universityとなります。
さらに、[Country]を見ればアメリカ合衆国のサーバーを経由して送られたことが分かり、
このメールがスパムメールであると判断できます。

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。

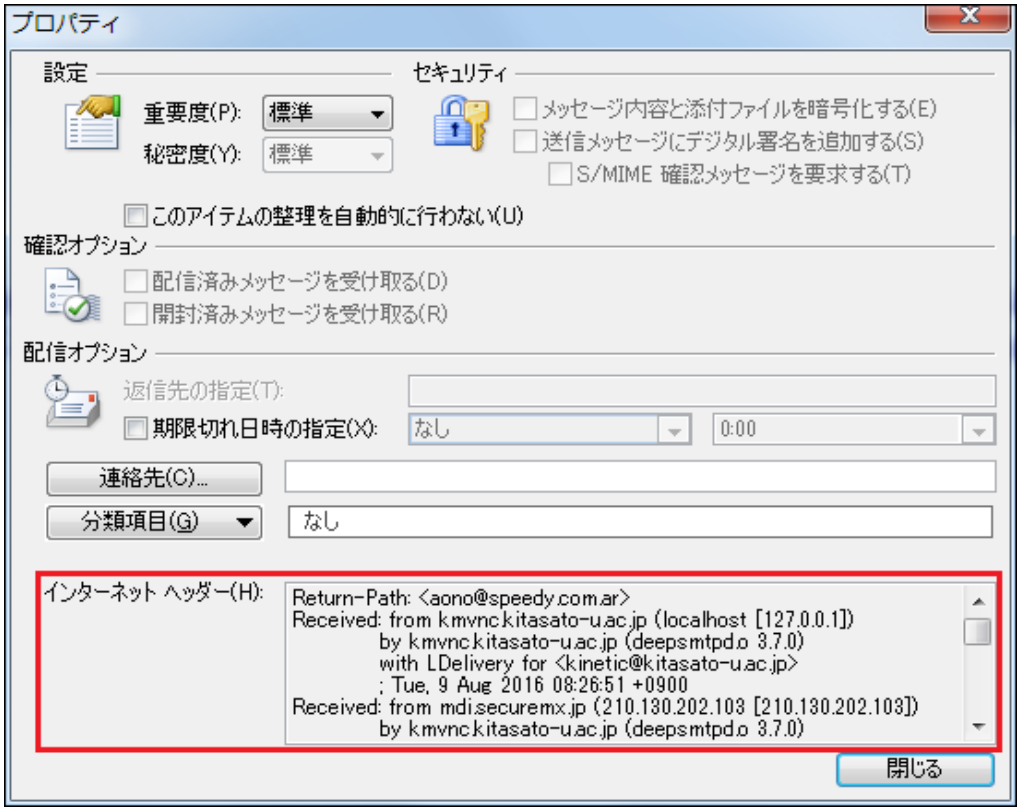
各メーラーでのメールヘッダの表示方法は以下の通りです。

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。

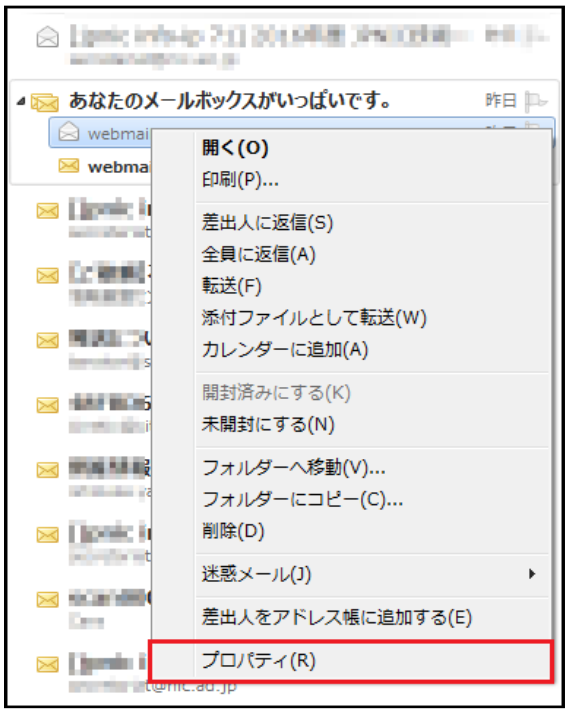


(2)プロパティが表示されるので、下の項目のインターネットヘッダで
参照することが出来ます。

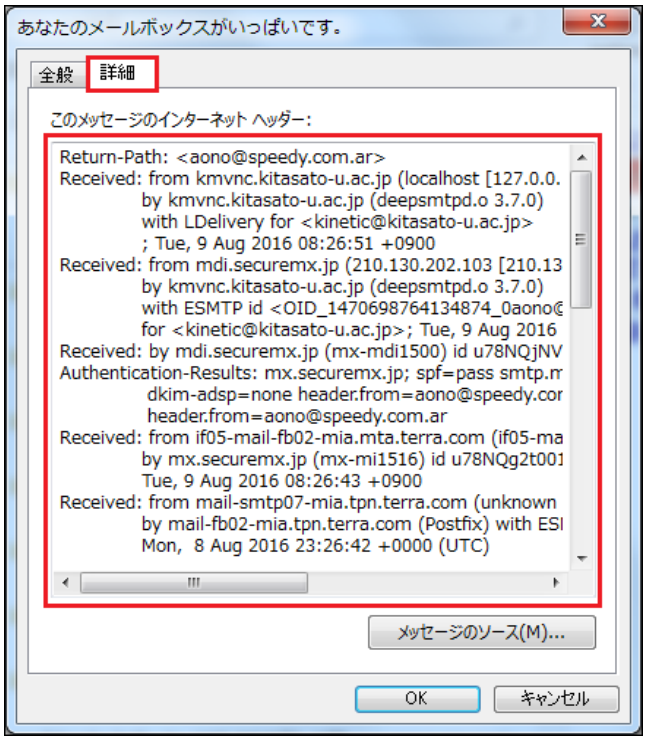


Windows Liveメール

(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。

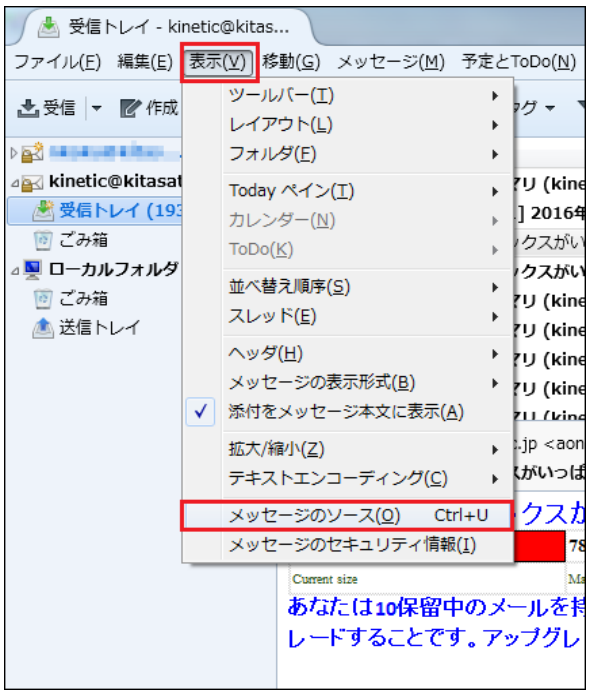


(2)［詳細］タブをクリックするとヘッダを参照できます。
［メッセージのソース］をクリックすると、より大きな画面で見ることができます。

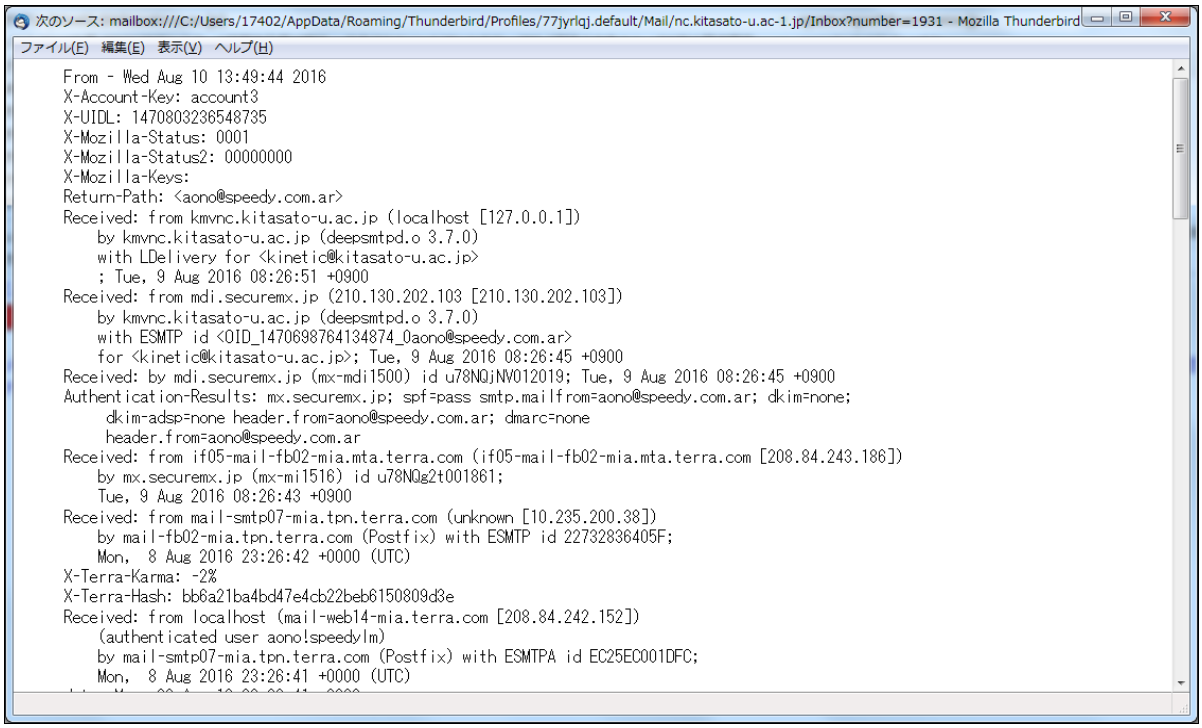


Thunderbird

(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）

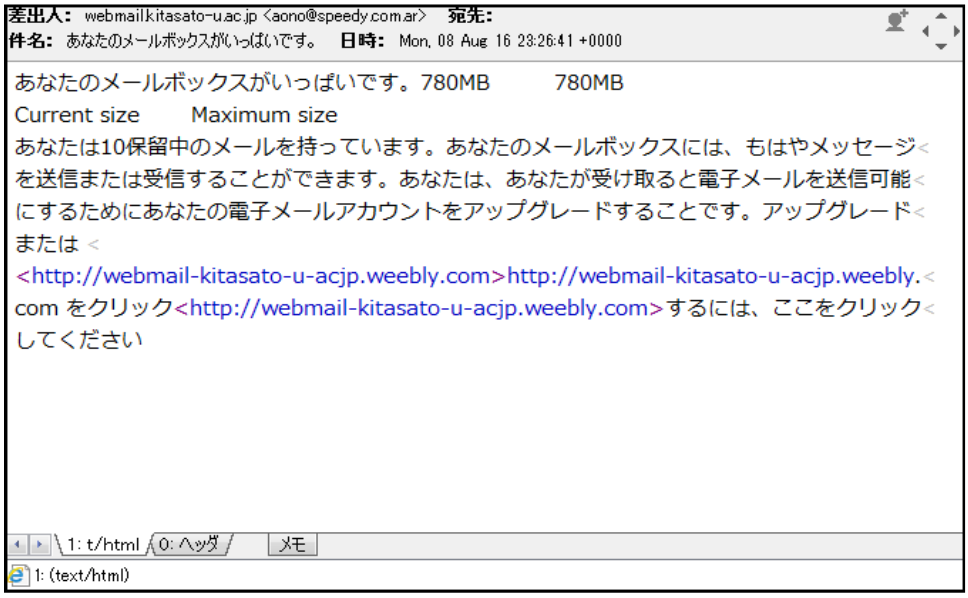


(2)新しいウィンドウが開き、ヘッダ情報が表示されます。

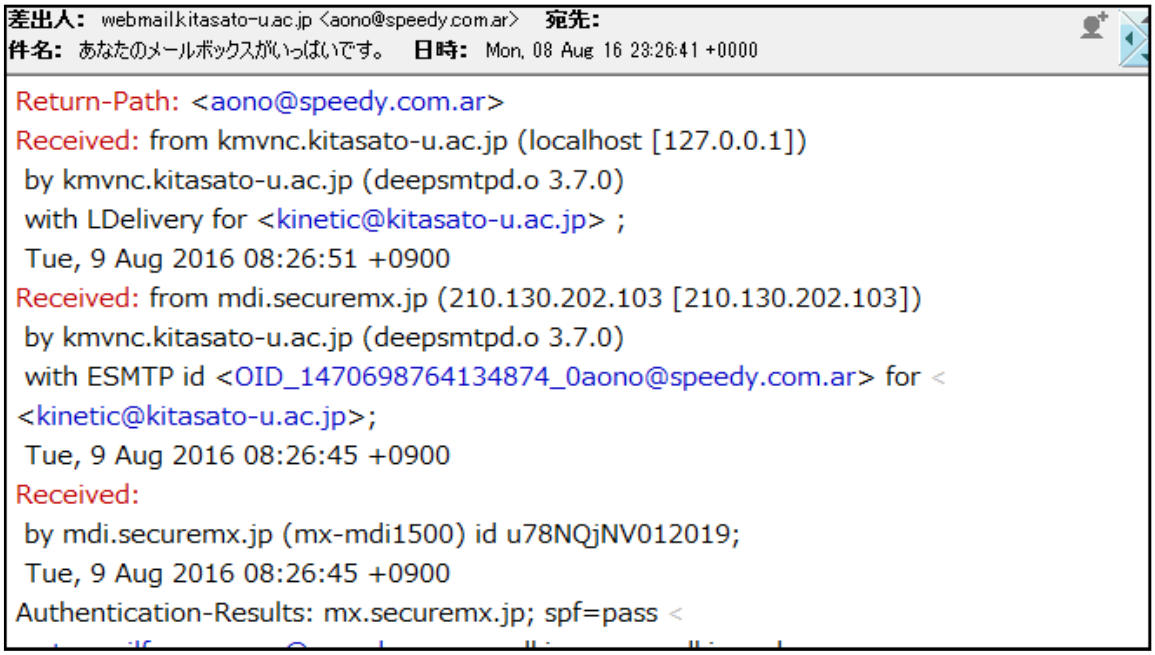


Becky

(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