JPCERT CC®

電子メールソフトのセキュリティ設定について

一般社団法人**JPCERT**コーディネーションセンター

2011 年 **2** 月 **1** 日

JPCERT CC®

目次

JPCERT CC®

本資料は、一般社団法人 JPCERT コーディネーションセンターのウエブサイトにて公開している「電子メールのセキュリティ設定」をPDFファイルにまとめたものです。
最新の情報に関しては、以下の URL を参照してください。

一般社団法人 JPCERT コーディネーションセンター
電子メールソフトのセキュリティ設定について
https://www.jpcert.or.jp/magazine/security/mail/index.html

1 はじめに

インターネットが一般に普及した現在、電子メールはインターネット利用者の大半が使うコミュニケーションツールとなりました。それに伴い迷惑メールが増加し、更にウイルスを配布するような攻撃にもしばしば利用されるようになってきました。

加えて近年では、今までの迷惑メールのような無差別な配布ではなく、特定少数を標的とした標的型メール攻撃と呼ばれる攻撃も散見されるようになってきています。

標的型メール攻撃において攻撃者は、企業情報、個人の Web ページや ブログ、メーリングリスト等から特定の個人情報等を入手し、知り得た情報をもとに標的とされた特定の組織向けにメール文面などをカスタマイズし、その会社の幹部社員などからの社内文書や、組織が関連している分野の資料を装ったメールを作成します。

攻撃者は、標的となったユーザがつい開いてしまうような電子メールを送付することによって、ユーザにメールに添付した文書ファイルなどを開かせ、そこに仕込んだウイルスを感染させることによって、情報を窃取したり、利用者の PC を乗っ取ったりするといった手法を用いるものが多く見られます。

このように電子メールが攻撃に利用される背景としては、電子メールには偽造されたり、内容を改ざんすることが比較的容易にできてしまう規格上の問題があります。このような問題を解決するための技術やサービスが提供されていますが、そもそもこのような事実が広く知られていないことから、対策が浸透していない状況にあります。

電子メールが広く利用されていることから、電子メールの偽造、改ざんといった問題や、迷惑メールへの対策が必要なことは言うまでもありません。特に、送信者の偽造や内容の改ざんは、電子メールを用いたコミュニケーションの根本的な信頼性にかかわる問題と言えます。

この問題に対処するために、例えば PKI や PGP を用いた電子署名を利用するなどのユーザ側での対策や、SMTP 認証を利用したサービス提供者側での対策などがあります。できる限りこれらの対策をとり、不正な電子メールに騙されないようにすることが重要です。

しかしながら、電子署名は導入の難しさからか比較的敬遠されやすく、また、あまり一般的でもないため、この対策を採用している組織は非常に少ないのが現実です。

このような現状の中で、ユーザとして「何に注意をして」、「どのように設定すればよいのか」を知ることは非常に重要です。 特に標的型メール攻撃は、突き詰めれば個人の傾向を理解した上での攻撃手法であることから、システムだけで完全に保護することはできません。 従って、電子メールの利用者側でも自分の身を護るために対策を行っていくことが重要です。

以上のような状況から、JPCERT/CC では電子メールの利用者が自分の身を護るための最低限の設定や確認事項を調査し、公開することにいたしました。

本文書を参考にして、皆さんが電子メールを用いた詐欺や攻撃を受ける可能性を少しでも減らすことができればと願っております。

2　本文書がカバーする電子メールソフト

本文書では以下の電子メールソフトを取り上げました。

電子メールソフト	バージョン
Apple Mail.app	3.5 (930.3)
Becky! Internet Mail	2.50.01
Microsoft Outlook Express	6.00.2900.5512 (xpsp.080413-2105)
Microsoft Outlook 2003	(11.8217.8221) SP3
Microsoft Outlook 2007	(12.0.6316.5000) SP1 MSO (12.0.6320.500)
Microsoft Windows Live Mail	2008 (Build 12.0.1606)
Mozilla Thunderbird	3.1.6
Gmail	-
Yahoo! メール	-

これらの電子メールソフトは、一般的に利用されており、特に Microsoft Outlook Express/Microsoft Windows Live Mail/Apple Mail.app は OS に標準で添付されているため、利用者が多い電子メールソフトとなっています。

※各電子メールソフトの手順中に使用している画像には、一部上記と異なるバージョンで取得した画像が含まれています。
その場合の該当箇所には、画像を取得した電子メールソフトのバージョン情報を記載しています。

3　電子メールソフトの設定に関する説明

電子メールソフトは利用者が頻繁に利用するものであるため、各電子メールソフトには様々な機能が実装されています。

ここでは、安全に電子メールを利用するための必要最低限の機能に関して簡単に説明を行います。

3.1　受信メール一覧で表示される情報の拡張

電子メールを取り扱うにあたり、受信したメール一覧の表示項目には、最低限以下を表示するべきです。

- 送信者の電子メールアドレス (From)
- 受信者の電子メールアドレス (To)
- 表題 (Subject)
- 送信日時 (Date)

これらの項目は、自分に届いた電子メールが迷惑メールや攻撃メールであるかどうかを判断する上で、基礎となる情報です。これらの情報を詐称する事も可能ですが、まずはこれらの情報を確認することが電子メールを安全に使用するための第一歩となります。

「受信メール一覧で表示される情報の拡張」に関する各電子メールソフトの設定については、4 章の各電子メールソフトの項を参照してください。

3.2　送信者のアドレス表示

電子メールには本文の他に、「送信者」、「受信者」、「配送経路」等を含む、ヘッダと呼ばれる項目があります。

一般に、電子メールを利用する上で送信者の情報を確認することは重要です。

攻撃を目的とした電子メールでは、送信者情報を詐称することが多いため、送信者を確認したから安全とは言えませんが、攻撃を検知するための一助となることは間違いありません。

また、現在の電子メール規格では、送信者のメールアドレスの他に、「表示名」(display name)と呼ばれる付加情報を追加することができます。 多くの場合、表示名には本名やニックネームなどが使われていますが、表示名は送信者が任意で設定できることが出来るため、送信者を確認する際にこの「表示名」に頼り切ると、送信者の詐称を受けやすくなるという意味で両刃の剣と言えます。

送信者情報が詐称されている可能性を踏まえた上で、確認してください。

「送信者のアドレス表示」に関する各電子メールソフトの設定については、4 章の各電子メールソフトの項を参照してください。

3.3 S/MIME 及び PGP 対応

電子メールは通常、暗号化や電子署名を行わずにやりとりされています。これは、電子メールを何らかの方法で、不正に受信し、内容を読んだり（盗聴）、書き換えたりする（改竄）することが可能であると言うことを意味し、盗聴による個人情報の窃取や、改ざんによる攻撃などが比較的簡単に行えてしまいます。

IETF では、このような状況に対応するために、S/MIME(RFC5750, RFC5751)及び、MIME の PGP 対応(RFC2015, RFC3156, RFC4880)に関する規格を制定しています。

S/MIME は PKI を利用した電子証明書を用いる手法で、公的個人認証基盤(いわゆる住基ネット)等で配られている個人証明書や、様々な証明書発行機関によって発行された個人証明書を利用して電子メールの暗号化や電子署名を行うことができます。

今回調査した電子メールソフトは、Becky!を除き全ての電子メールソフトがインストール直後から S/MIME を利用できます。また、Becky!も標準で添付されている Plug-In をインストールすることで S/MIME に対応できます。

一方、PGP 対応については、いずれの電子メールソフトでも標準では利用できません。実際には Windows Live Mail 以外の電子メールソフトは、Plug-In を導入することで PGP に対応できますが、本文書では取り扱いません。

本文書では、S/MIME、PGP 対応のどちらを採用すべきかに関しては論じませんが、電子メールを通じた被害を減らすためには、電子署名や暗号化を活用することが重要であると考えています。

「S/MIME 及び PGP 対応」に関する各電子メールソフトの設定については、4 章の各電子メールソフトの項を参照してください。

3.4 迷惑メールフィルタ機能

迷惑メールの増加に伴い、一部の電子メールソフトでは、迷惑メール対策のためのフィルタ機能が組み込まれています。

この迷惑メールフィルタ機能は、受信した電子メールをふるいにかけ、迷惑メールを分離する機能です。

昨今、流通する電子メールの大半が迷惑メールであるとの報告があり、大量の迷惑メールを受信することによる作業効率の低下が問題となっています。迷惑メールフィルタ機能を利用することで、迷惑メールの処理時間の低減が期待出来ます。

なお、迷惑メールフィルタ機能は、迷惑メールを「完全に」分離してくれるわけではなく、迷惑メールと疑わしいと判定された電子メールを分離するものです。 従って、利用の際には、

- 迷惑メールではない電子メールが迷惑メールに分類されてしまう
- 迷惑メールが認識されない

という状況が発生することを認識した上で使用する必要があります。

「迷惑メールフィルタ機能」に関する各電子メールソフトの設定については、4 章の各電子メールソフトの項を参照してください。

3.5 HTML メールの取り扱い

3.5.1 HTML メールとは

HTML メールとは、電子メールの本文が HTML（Hyper-text Markup Language）で記述された電子メールです。「HTML 形式のメール」とも呼ばれます。

HTML メールは、HTML の特徴である多彩な表現力を使用して、文字に装飾を施したり、文章に図や写真などの画像を組み込んだりすることが出来ます。HTML メールは、クリスマスカードやバースデーメールなどの個人間の社交的なコミュニケーションのために利用される他、企業からの広告案内や商品通知などにおいて、積極的に利用されています。

3.5.2 HTML メールを表示する仕組み

電子メールソフトは、一般的に HTML メールを表示するために HTML レンダリングエンジンを実装しています。電子メールソフトは、受信した電子メールのヘッダを解析し、HTML メールと判定した場合に HTML レンダリングエンジンを使用して HTML で記述された内容に従い、メールの内容を表示します。

主な HTML レンダリングエンジンと、各エンジンを搭載している Web ブラウザや電子メールを次に掲げます。

- Trident(MSHTML)：Internet Explorer、Outlook など
- Webkit：Safari、Apple Mail など
- Gecko：Firefox、Thunderbird など

例えば、Gecko と呼ばれる HTML レンダリングエンジンは、Web ブラウザである Firefox にも、電子メールソフトである Thunderbird にも、共通して使用されています。したがって、HTML レンダリングエンジンに起因する Web ブラウザの脆弱性が発見された場合、脆弱性の影響を受ける範囲は、同系の電子メールソフトにまで広がる可能性があります。

3.5.3 HTML メールの危険性

HTML メールには、以下のような問題があります。

一つは、これまでに電子メールソフトの HTML 表示機能に多数の脆弱性が見つかっていることです。

これまで、電子メールソフトの HTML メール表示関連処理には多くの脆弱性が発見されてきました。メールを閲覧するだけで PC がウイルスなどに感染してしまうため、HTML メールの表示（プレビュー）に関する脆弱性は特に危険度が高いのです。攻撃者が送信した HTML メールを閲覧したユーザの PC がウイルスに感染したという事例も過去に発生しています。

もう一つは、リンクが偽装されやすいことです。

HTML では、悪意をもった発信者が、もっともらしく見える表示に対して、まったく無関係なリンク先を対応付けることが出来ます。このため、HTML メール上では銀行の URL だと信じてクリックした受信者が、実際には攻撃者が用意したフィッシングサイトに誘導される可能性が高まります。

また、直接的な危険性ではありませんが、HTML メールを表示する際に Web サーバへのアクセスが生ずる場合（画像の読み込みなど）には、ユーザがメールを開いた事を Web サーバの運用者が確認出来るため、電子メール・アカウントが利用されていることや、ユーザの行動がトラッキングされてしまう可能性もあります。

<リンク偽装の事例>
以下の事例では、フィッシング対策協議会の URL が表示されているが、実際にクリックしたときにジャンプする先は、JPCERT/CC の Web サイトとなっています。

フィッシング対策協議会のサイトはこちら。
http://www.antiphishing.jp/

3.5.4 HTML メールの取り扱い

このように HTML メールは攻撃手段として使用される可能性があります。セキュリティを重視するのであれば HTML メールの受け取りは控えたほうがよいでしょう。 HTML メールを受け取った場合にも、以下のように電子メールソフトを設定して HTML メールとしての表示を抑制しておくことで、攻撃されるリスクを減らすことができます。

1) 電子メールソフトで HTML メールをプレビューしないようにする。

2) 電子メールソフトで HTML メールを送信しないようにする。

各電子メールソフトの設定は、以下を参考に実施してください。

もし、HTML メールを使用する場合は、その危険性を理解した上で、電子メールソフトのみならず OS、Web ブラウザの修正プログラムを適宜更新した上で利用してください。

3.6 添付ファイルの取り扱い

3.6.1 添付ファイルとは

添付ファイルとは、電子メールの本文に添付して送受信されるファイルです。

電子メールは、単体のテキスト・メッセージだけの送受信を前提として設計され、画像データや音声データなどのバイナリデータはテキストに変換して本文中に埋め込まない限り、電子メールで送受信することができませんでした。

電子メールの利用が拡大するのに伴い、そうした不便さを解消するため、1 つの電子メールのメッセージを複数の要素から構成できるような拡張が定義され、構成要素がバイナリデータである場合には、

BASE64 や uuencode、Quoted Printable などといった方式に従って文字データに変換（エンコード）および復元（デコード）する方法が採用されて、画像やドキュメントファイルなど様々なファイルを手軽に送受信することができるようになりました。

3.6.2 添付ファイルの危険性

電子メールの添付ファイルは便利な機能ですが、ウイルスなどマルウエアの感染経路の一つともなっています。スパムメールにマルウエアが添付されている場合もあります。発信元に知人のアドレスが記載された電子メールのように見えても、第三者が知人のアドレスを騙って発信した可能性や、知人の PC がウイルスに感染していて添付ファイルも汚染されている可能性が否定できません。

添付ファイルにウイルスが含まれている場合、添付ファイルを開くことは、ウイルスが起動する契機を与えることになるため、添付ファイルの取り扱いには注意が必要です。

ウイルス等のマルウエアは、.exe や .scr などの実行形式ファイルだけでなく、Adobe Reader/Acrobat や Microsoft Office のデータ形式のファイルに埋め込まれていて、それらのアプリケーションの脆弱性を悪用して感染させようとする可能性があります。

また、安全なファイル形式とされている .txt などに拡張子を偽装した（電子メールソフトが認識する実際の拡張子とは異なる拡張子のように見せかけた）ファイル名が攻撃に利用されたケースもあります。

3.6.3 添付ファイルの取り扱い

添付ファイルをもつ電子メールを受け取った場合は、次の点に注意することが重要です。

- 知らない相手からの添付ファイルを開かない、もしくはメールを削除する

  知らない相手からの電子メールに添付されたファイルの安全性を確認することは容易ではありません。不審なメールにはウイルスが添付されていることが多いため、不用意に添付ファイルを開かないことが望まれます。

- 知り合いからの添付ファイルも不用意に開かないようにする

  電子メールの差出人は詐称することが可能であることやウイルス感染により意図せずメールが送信されている場合があるため、差出人が知り合いであっても、添付ファイルは不用意に開かず、メール本文や添付ファイル名を確認の上、少しでも不審に感じた場合は、添付ファイルを開く前に送信者に確認することが望まれます。

- ウイルス対策ソフトを最新の状態に保つ

  添付ファイルに既知のウイルスが含まれていた場合、ウイルス対策ソフトの定義ファイルが最新の状態であれば、誤って添付ファイルを開いてしまった場合でも感染を防げる可能性があります。このため、常に定義ファイルを最新の状態に保つことが望まれます。

- 使用している OS やアプリケーションを常に最新の状態に保つ

添付ファイルに含まれるウイルスには、OS やアプリケーションの脆弱性を利用して感染を広げるものがあります。パッチなどが公開された既知の脆弱性を利用したウイルスの場合、基本的には OS やアプリケーションを最新の状態することで感染を防ぐことが可能です。このため、OS やアプリケーションは常に最新の状態に保つことが望まれます。

3.6.4 送信メールの形式

現在、様々な形式で電子メールを送付することが可能となっています。(例として、HTML、リッチテキスト等)

しかし、HTML メールの取り扱いで説明したとおり、この種の拡張されたメール形式は、場合によって攻撃に利用されることがあります。従って、受信者によってはこの種の電子メールに対し「受け取らない」・「読まずに捨てる」という扱いをする可能性があります。

ですから、特別なことがない限り、HTML メールやリッチテキストメールは送らないことが望ましいと言えます。

「送信メールの形式」に関する各電子メールソフトの設定については、4 章の各電子メールソフトの項を参照してください。

3.6.5 開封確認機能

もともとの電子メールの規格では、電子メールを送信した後、受信者が配送された電子メールを読んだことを確認する術がありませんでした。 しかし、電子メールがビジネスなどでも利用されるようになり、受信者が電子メールを開封した事を確認したいという要望が増えたため、受信者が電子メールを開封したことを通知する開封確認機能が追加されました。

しかし、この開封確認機能は、「メールを読んだ（開封した）」という情報だけでなく、どこで読んだかなどの情報が漏洩してしまう可能性があり、セキュリティ的にはリスクを伴う物でもあります。

以上の理由により、どうしても必要な人を除いて、この機能は利用しないことが（現時点では）望ましいと考えられます。

「開封確認機能」に関する各電子メールソフトの設定については、4 章の各電子メールソフトの項を参照してください。

4　代表的な電子メールソフトの設定方法

4.1　Mail.app の設定

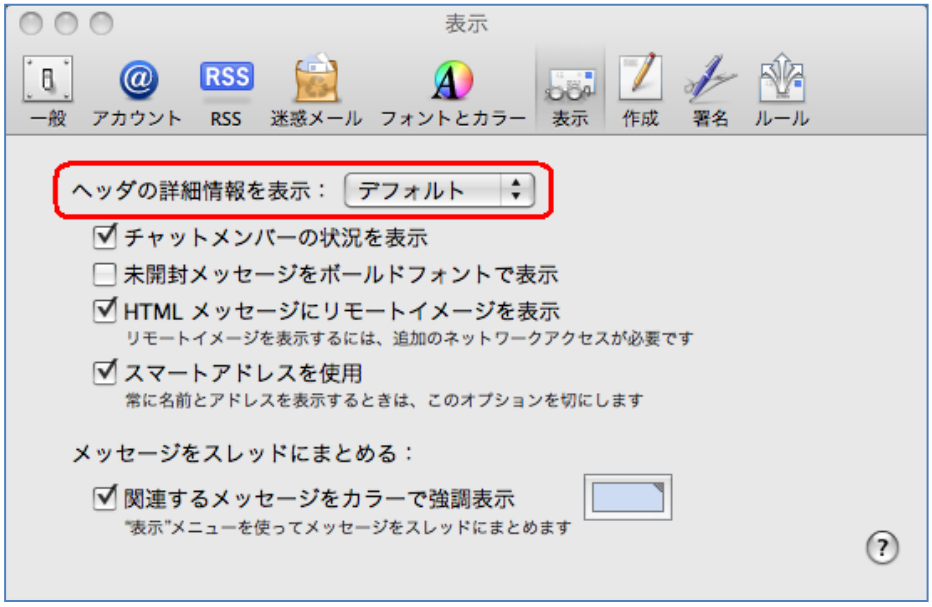
4.1.1　各設定

Apple Mail.app は、全ての設定を「環境設定」から行う事ができます。
「環境設定」ウインドウは、以下の操作により開くことが可能です。

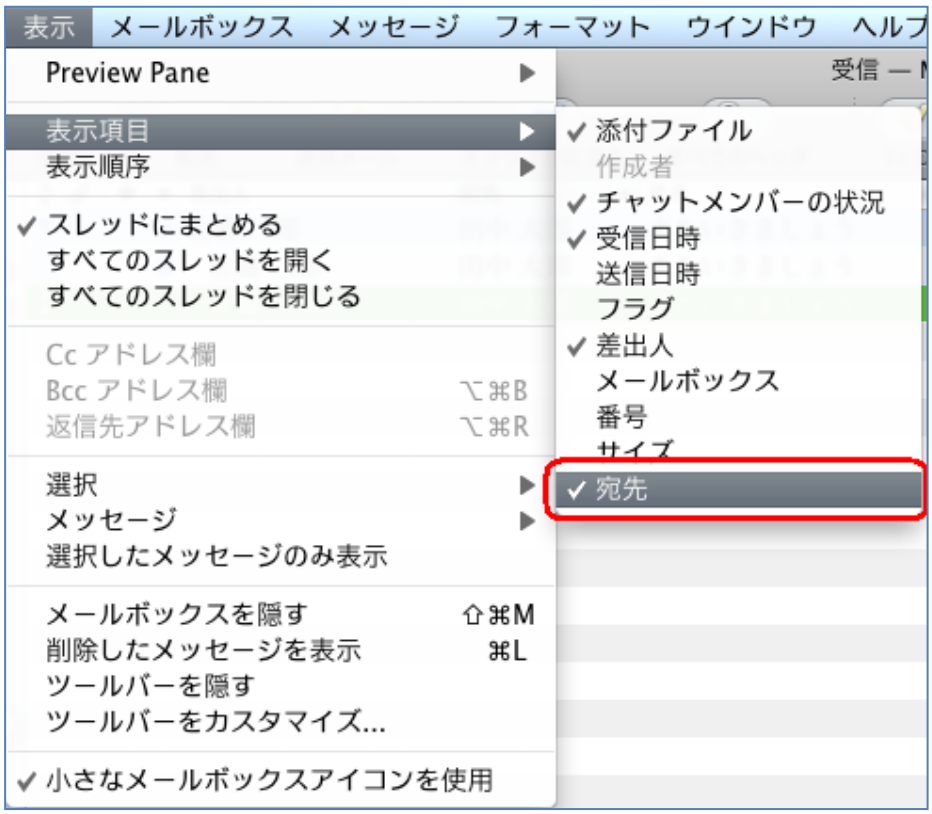
- Mail.app が起動かつ選択状態にある場合、最上部のメニューバーの「Mail」をクリックし、環境設定を選択する。

受信メール一覧で表示される情報の拡張

- 「環境設定」ウインドウから「表示」を選択し、「ヘッダの詳細表示」プルダウンメニューが「デフォルト」であることを確認する。



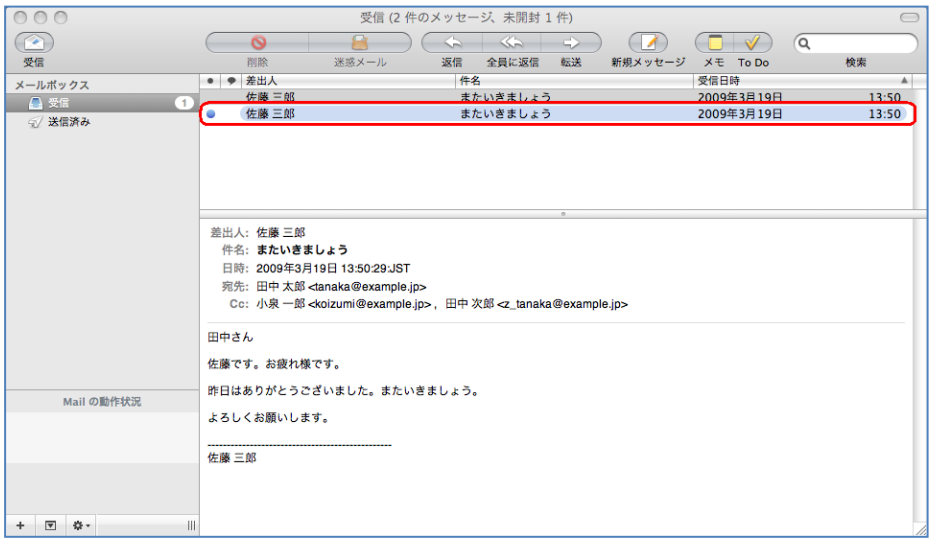
- Mail.app のメニューバーから「表示」を選択し、「表示項目」の「宛先」を有効にする。



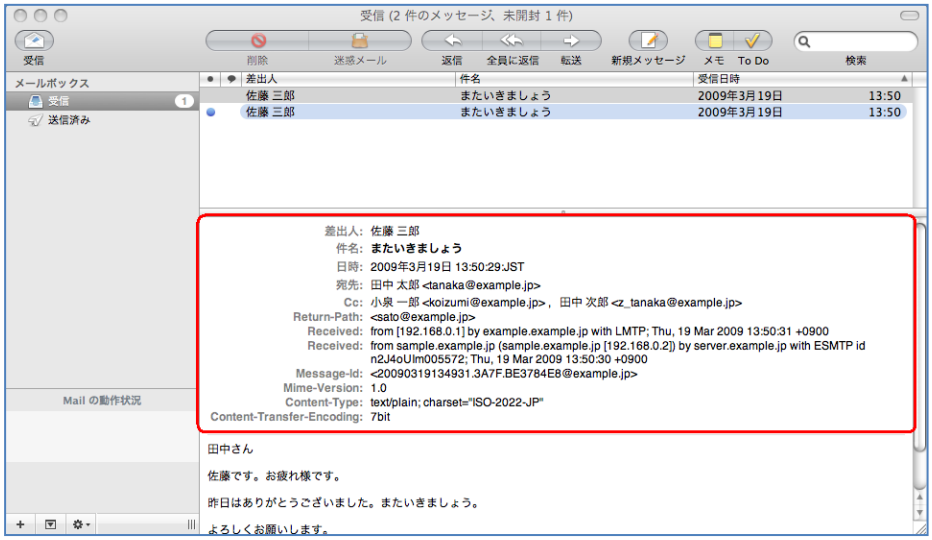
※この画像は Apple Mail.app 4.2(1077) で取得しています。

メールヘッダ情報の確認方法

- メールを選択する。

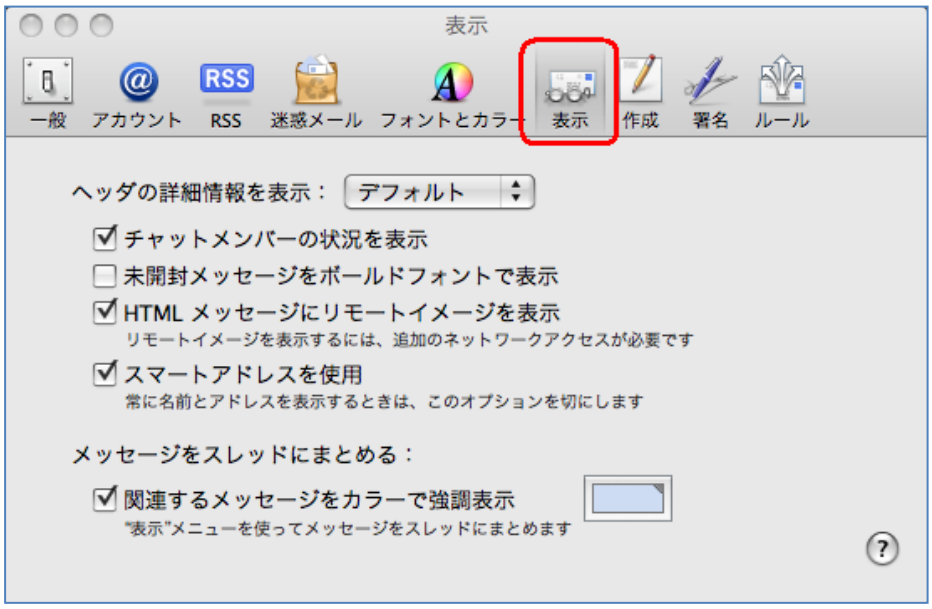


- メニューバーの「表示」から「メッセージ」を選択し、「全てのヘッダ」を選択する。

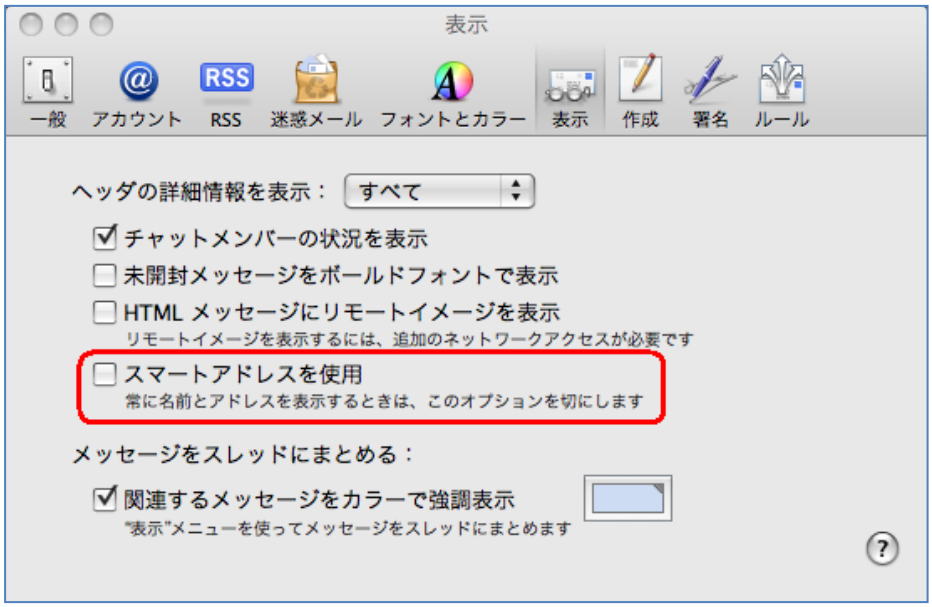


メールアドレスの表示形式の設定

- 「環境設定」ウインドウから「表示」を選択する。

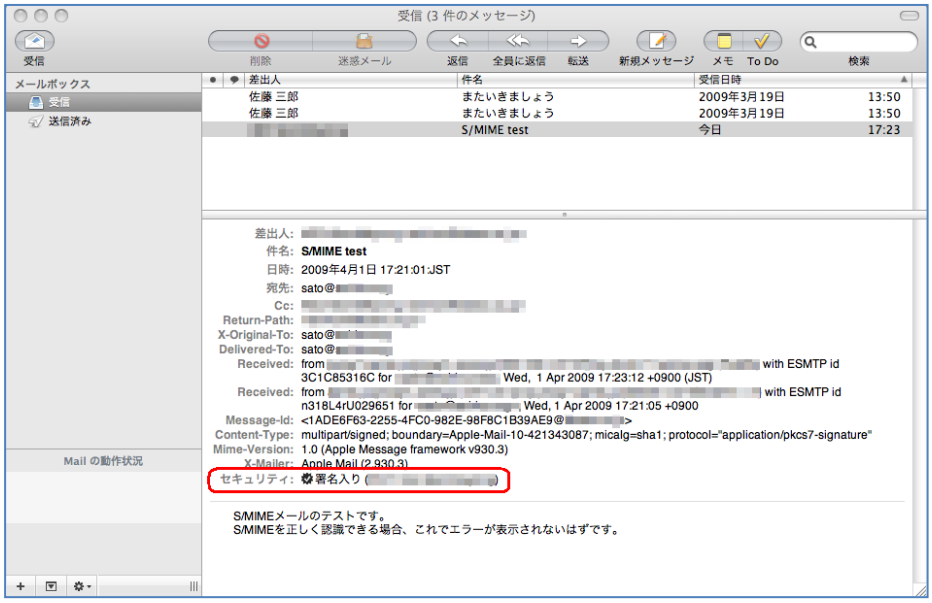


- 「スマートアドレスを使用」のチェックを外す。

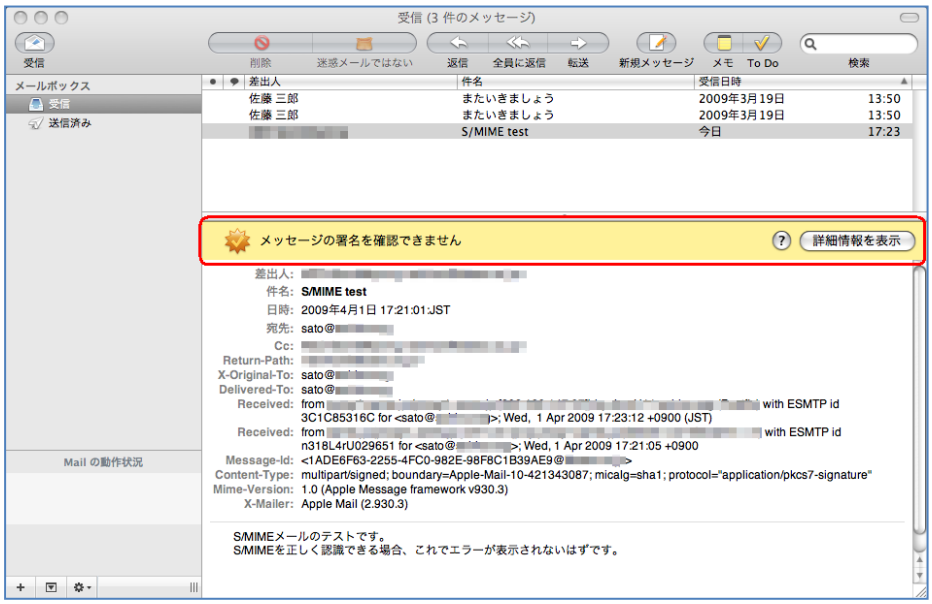


S/MIME による署名メールの表示例

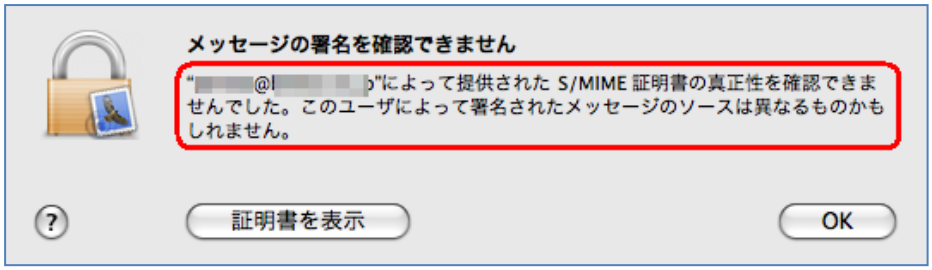
- S/MIME で署名されたメッセージが問題なく検証された場合
  メールヘッダ部分に「セキュリティ: 署名入り」と表示される。



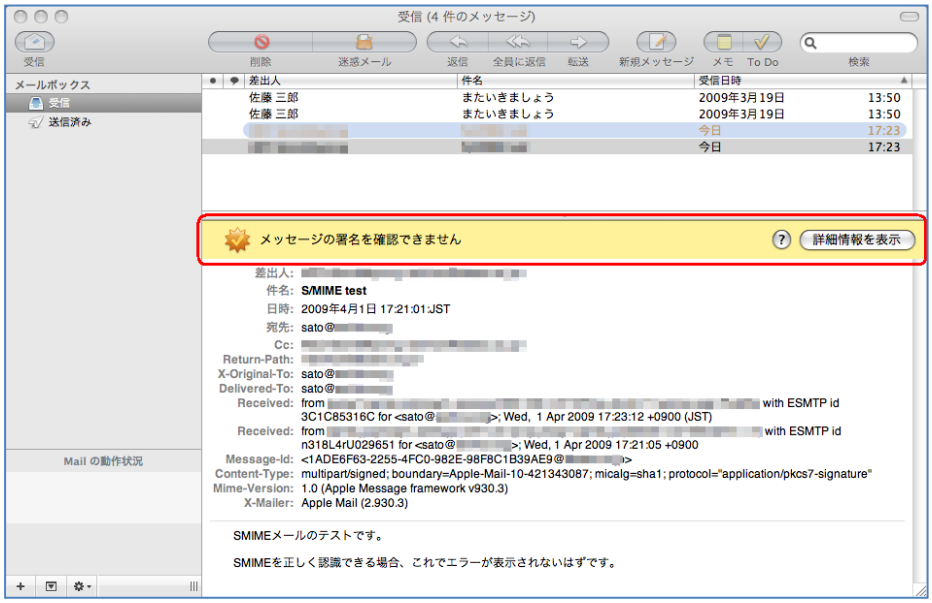
- S/MIME で署名されたメッセージの証明書が検証できない場合
  メール本文の最上部に、「メッセージの署名を確認できません」と表示される。



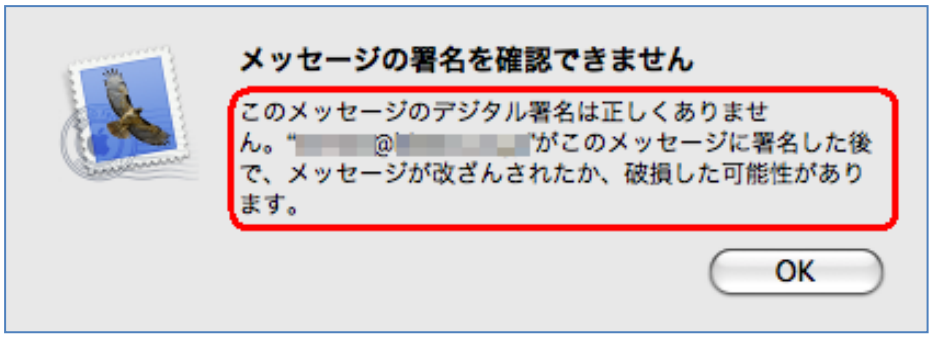
- 証明書を検証出来ない場合、「詳細情報を表示」ボタンを押すと、「メッセージの署名が確認できません」と表示され、証明書の真正性が確認できないことが表示される。



- S/MIME で署名されたメッセージが改ざんされている場合
メール本文の最上部に、「メッセージの署名を確認できません」と表示される。



- メッセージが改ざんされている場合、「詳細情報を表示」ボタンを押すと、「メッセージの署名が確認できません」と表示され、デジタル署名が正しくないことが表示される。

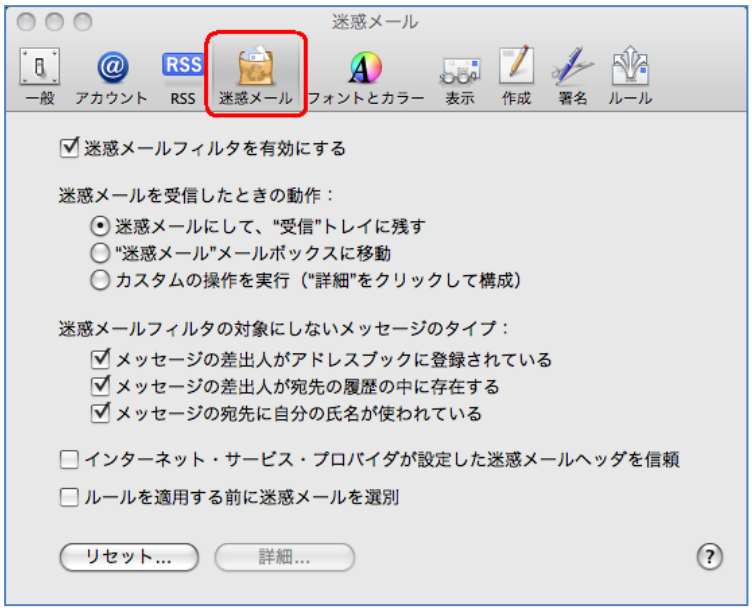


PGP 対応

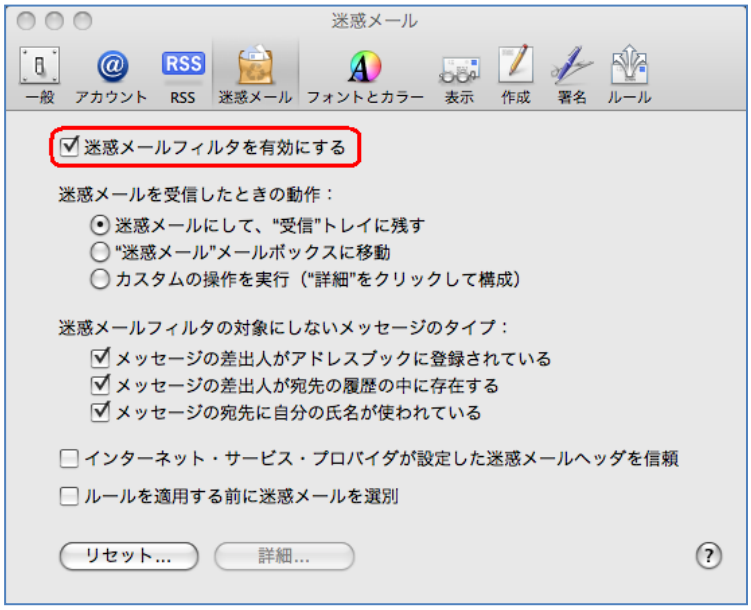
Apple Mail.app は、標準で PGP をサポートしていません。

迷惑メールフィルタの設定

- 「環境設定」ウインドウを開き、「迷惑メール」を選択する。

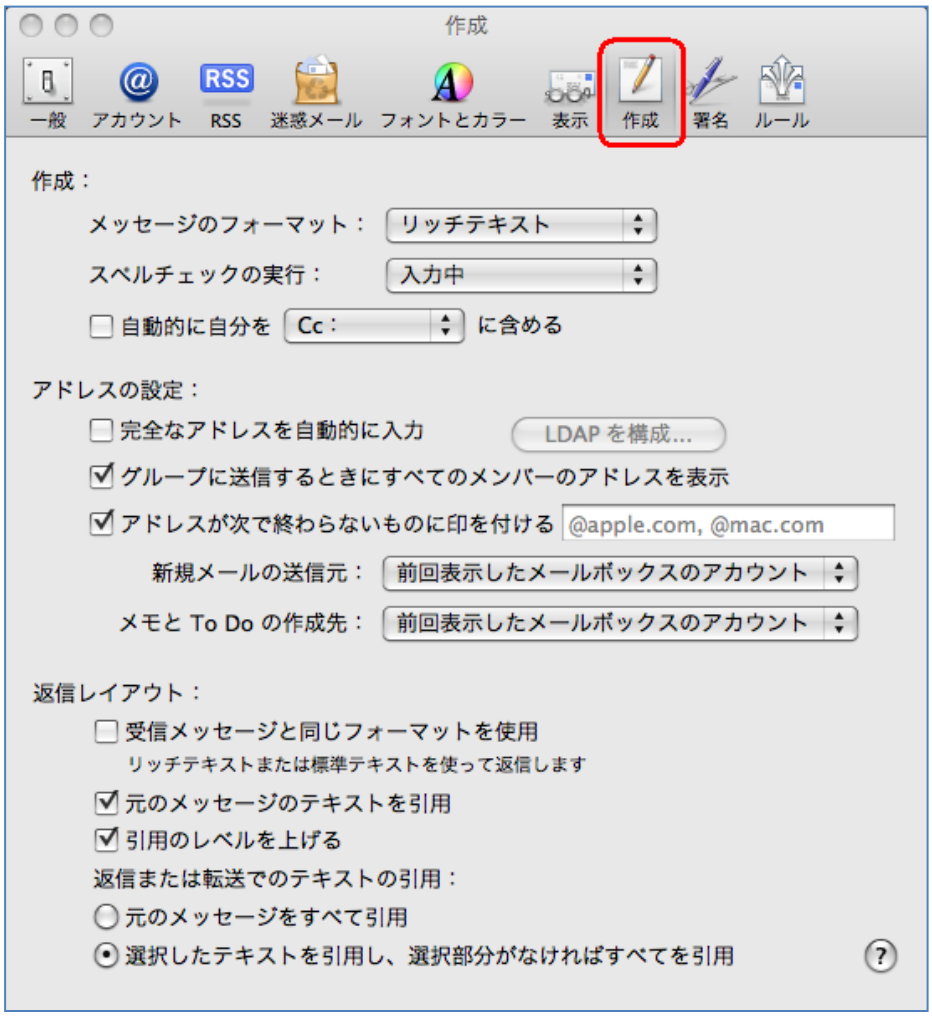


- 「迷惑メールフィルタを有効にする」がチェックされていることを確認する。
※なお、本稿では触れませんが、「迷惑メールを受信したときの動作」で「カスタムの操作を実行」にチェックすると、「詳細ボタン」から迷惑メールに関する動作を細かく設定することができます。

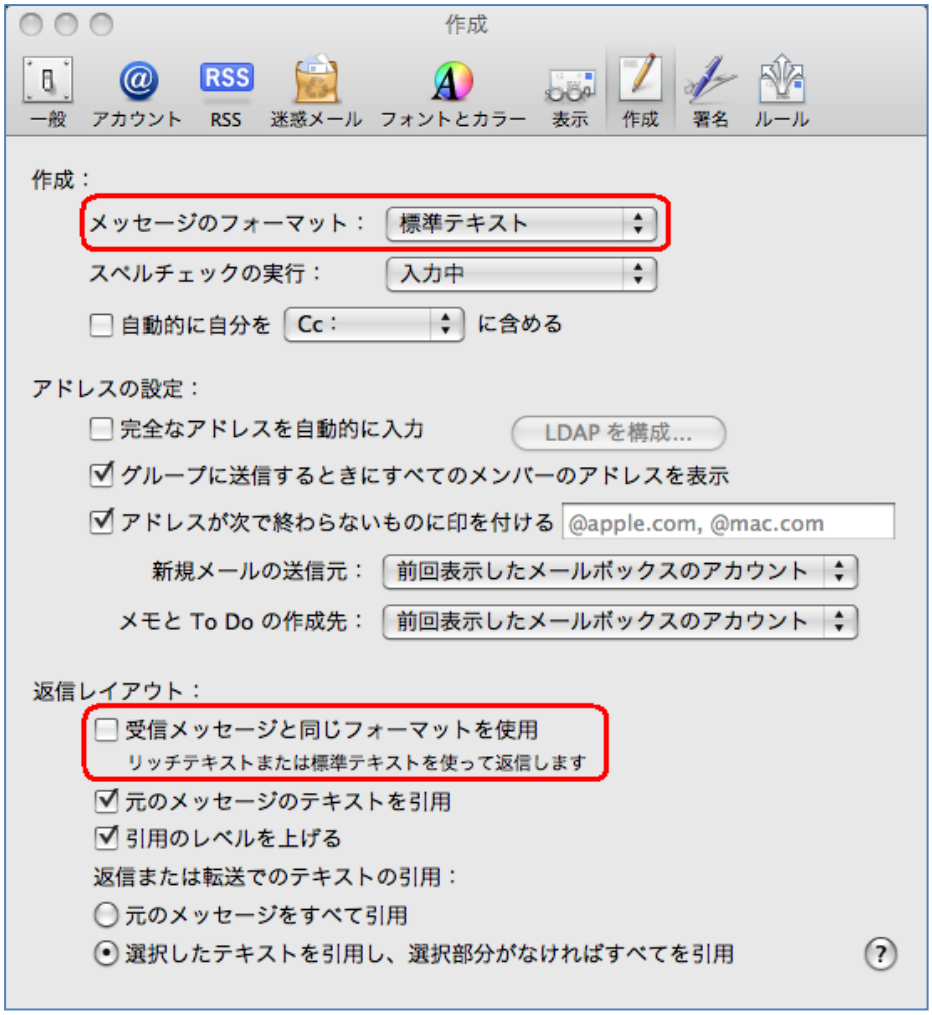


メール送信フォーマットに関する設定

- 「環境設定」ウインドウを開き、「作成」を選択する。

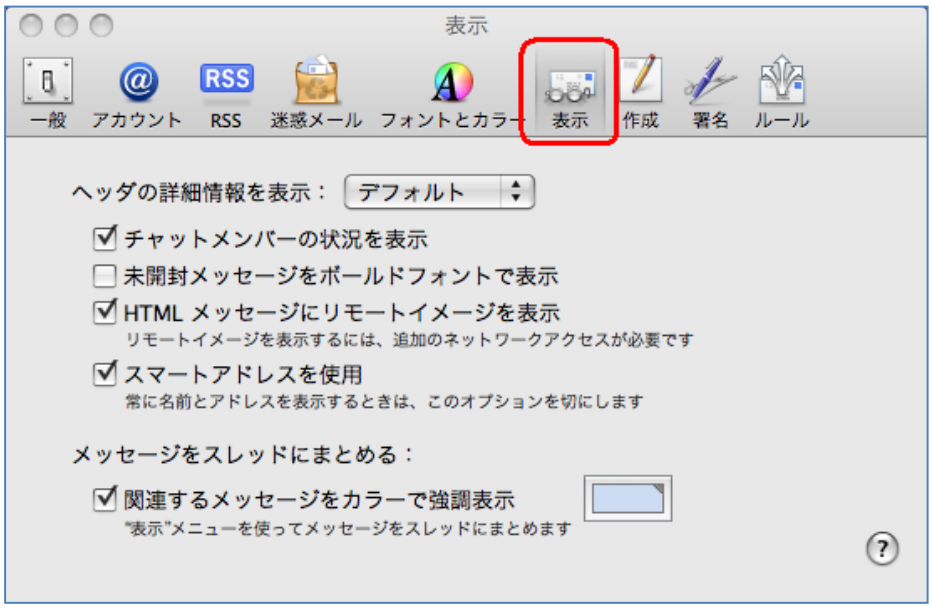


- 「メッセージのフォーマット」プルダウンメニューから「標準テキスト」を選択し、「送信レイアウト」内の「受信メッセージと同じフォーマットを使用」のチェックを外す。

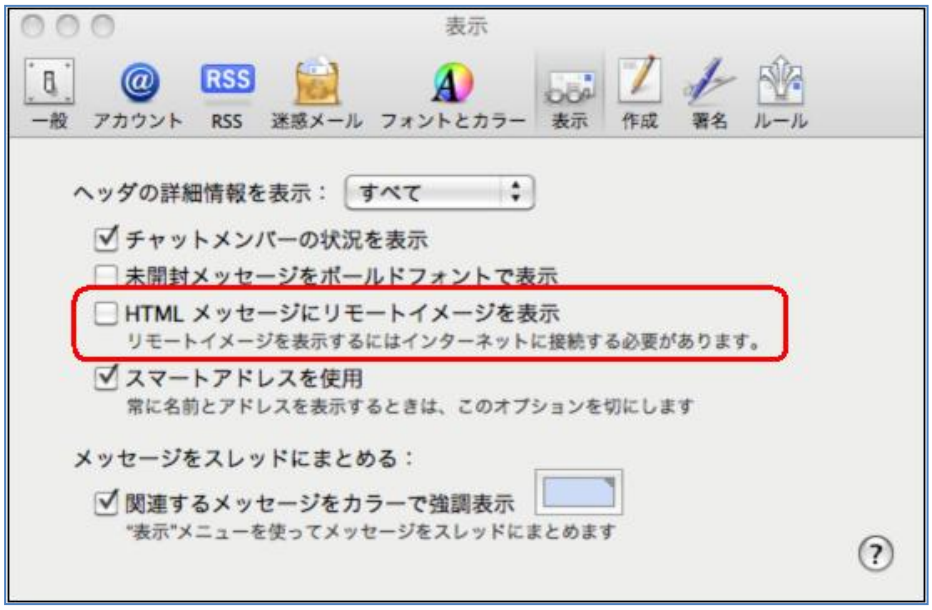


HTML メールの表示に関する設定

- 「環境設定」ウインドウを開き、「表示」を選択する。



- 「HTML メッセージにリモートイメージを表示」のチェックを外す。



開封確認機能に関する設定

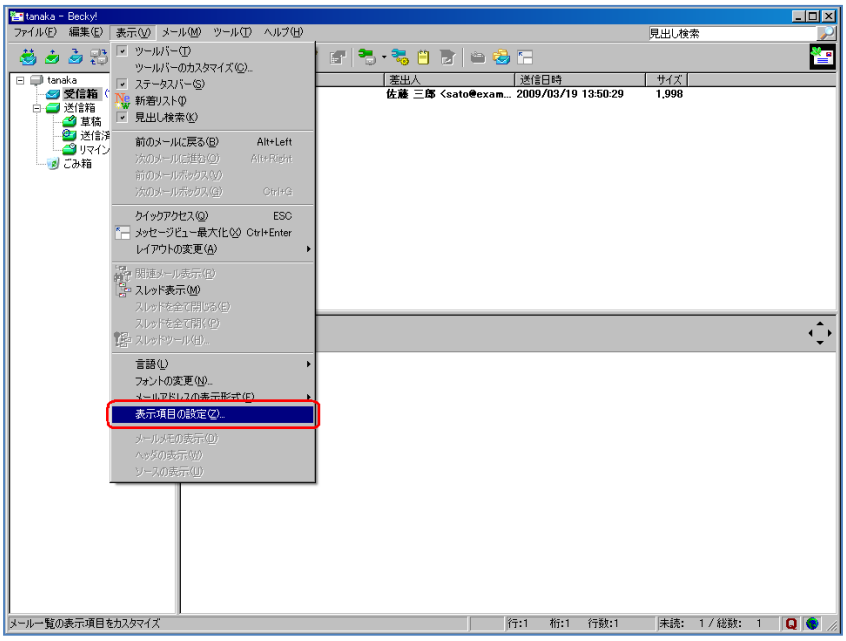
Apple Mail.app は、開封確認機能を持っていないため、設定はありません。

4.2 Becky!の設定

4.2.1 各設定

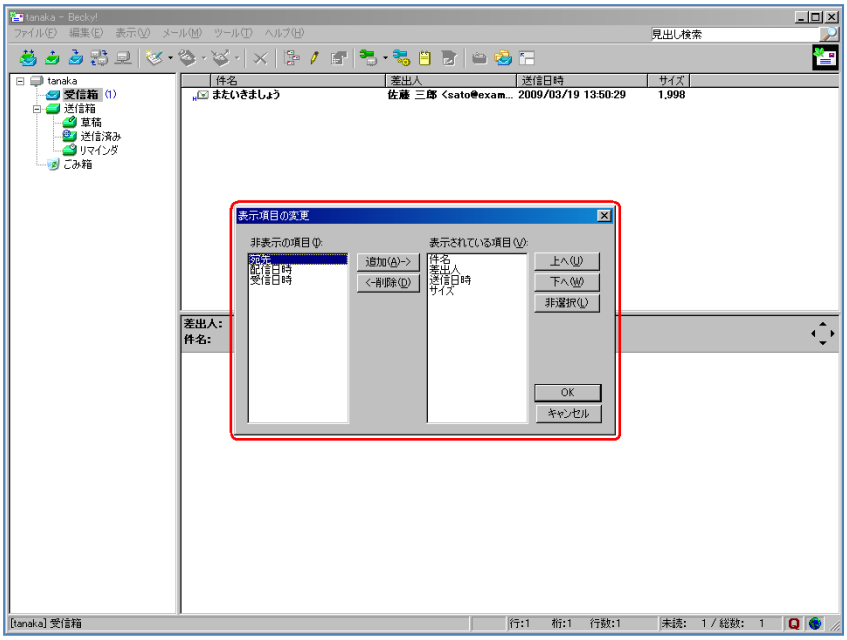
受信メール一覧で表示される情報の拡張

- メニューの「表示」から「表示項目の設定」を選択する。



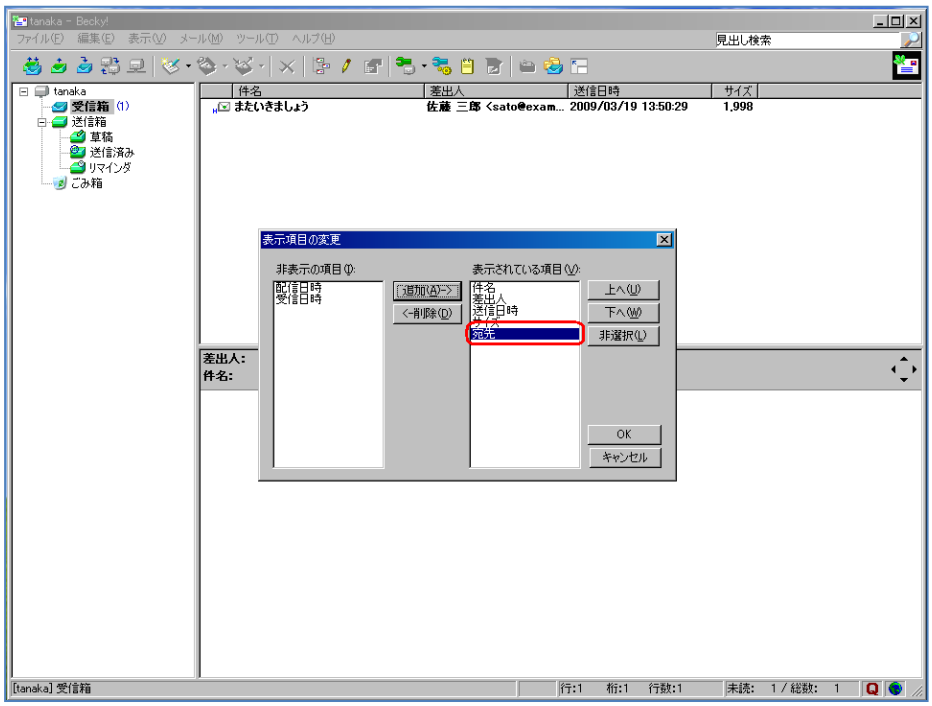
※この画像は Becky! Internet Mail 2.52.02 [ja] で取得しています。

- 「表示項目の変更」ウインドウが表示される。



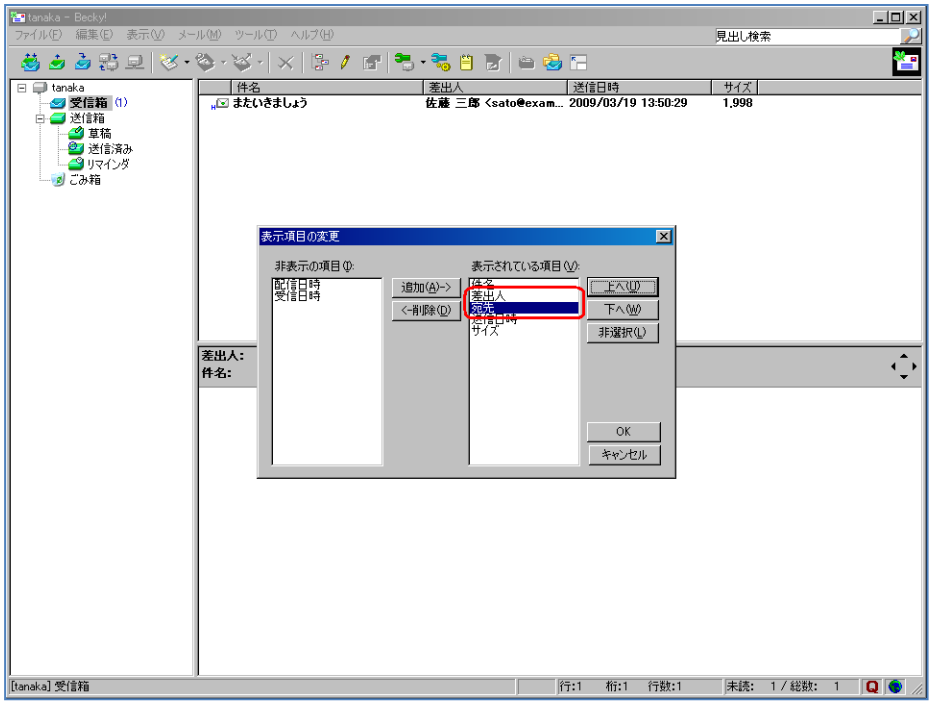
※この画像は Becky! Internet Mail 2.52.02 [ja] で取得しています。

- 表示項目の「宛先」を追加する。



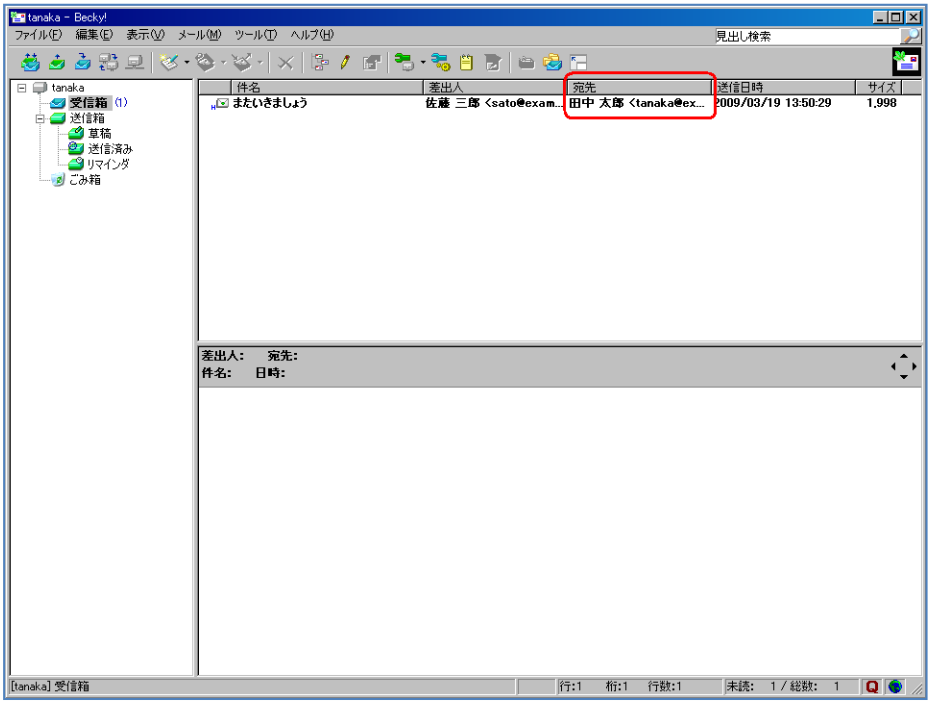
※この画像は Becky! Internet Mail 2.52.02 [ja] で取得しています。

- 表示されている項目の「差出人」の下部に「宛先」を移動する。



※この画像は Becky! Internet Mail 2.52.02 [ja] で取得しています。

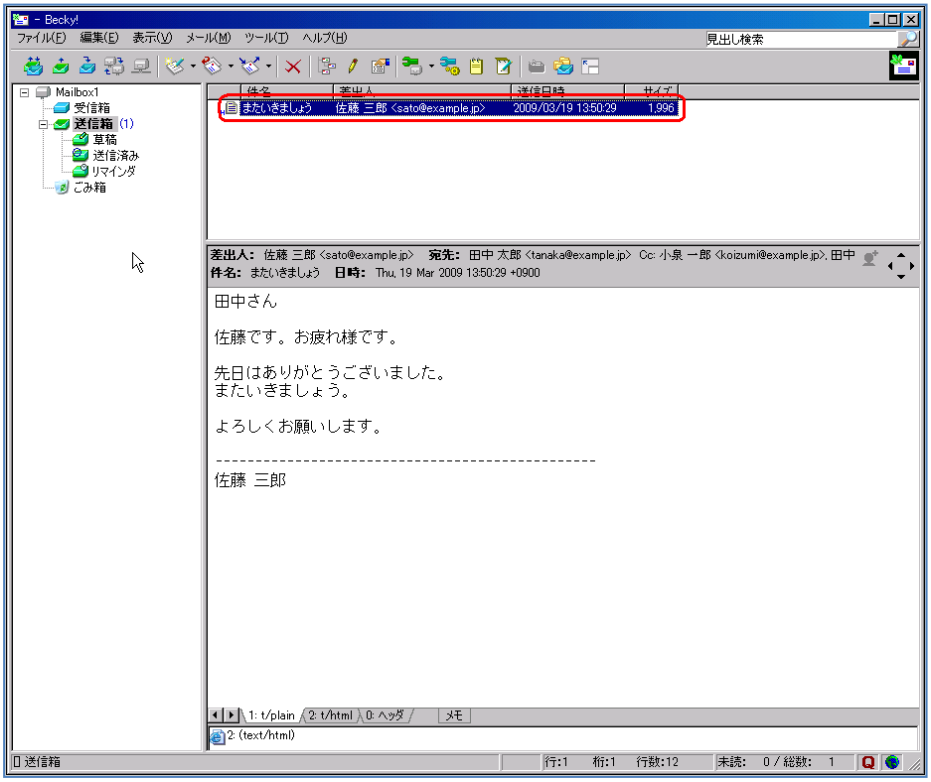
- 表示項目に「宛先」が追加される。



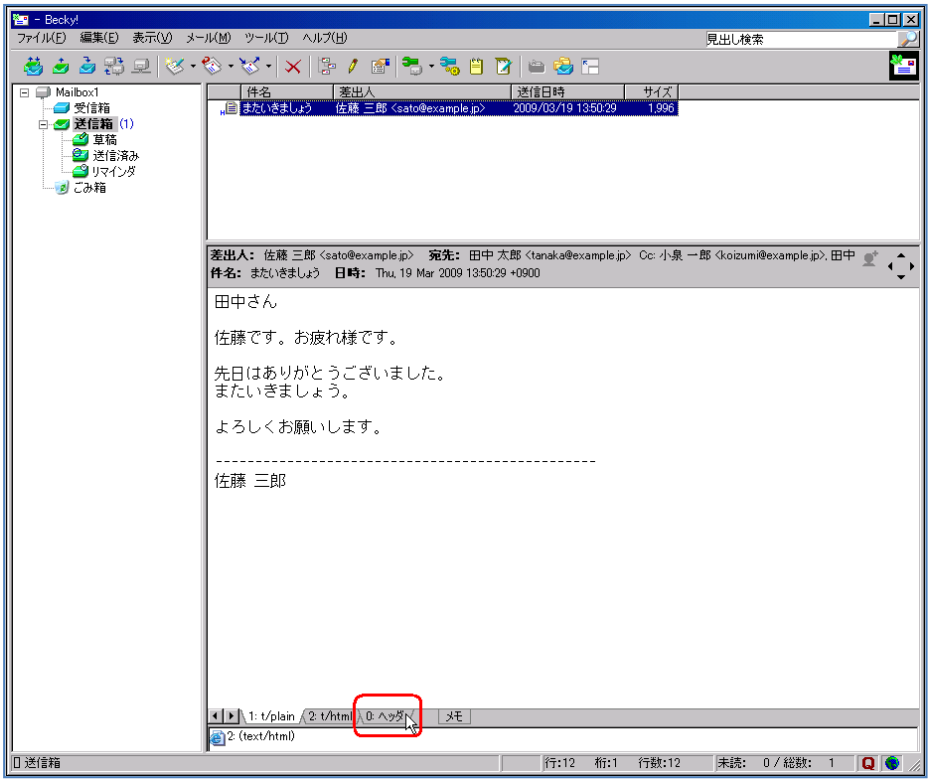
※この画像は Becky! Internet Mail 2.52.02 [ja] で取得しています。

メールヘッダ情報の確認方法

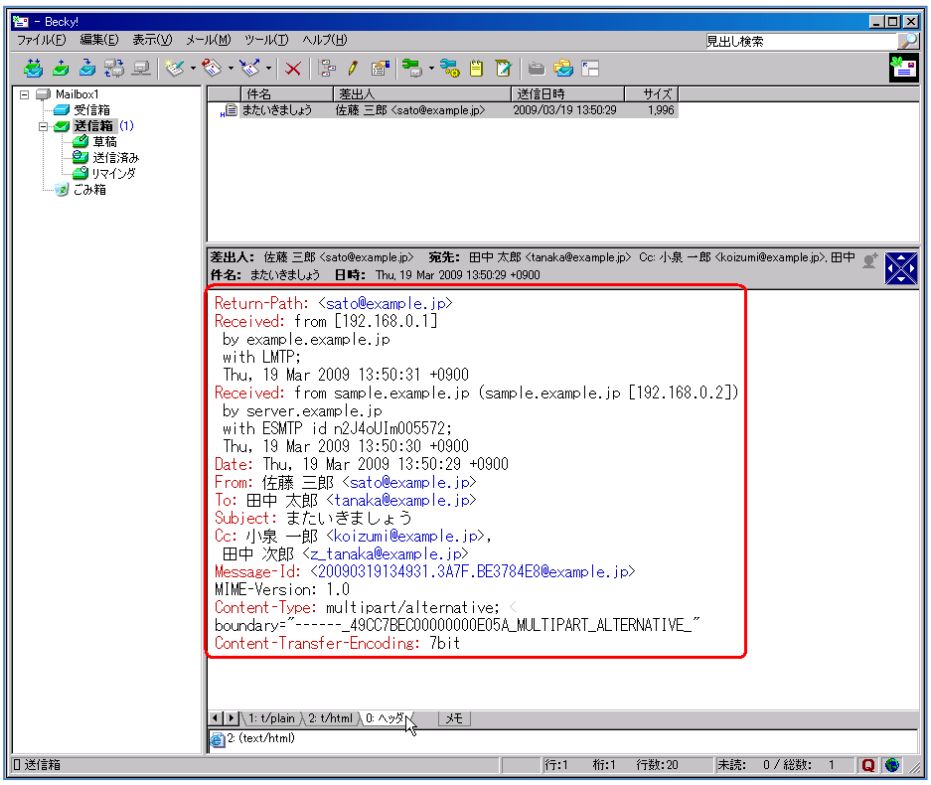
- メールを選択する。



- メール本文下部の「ヘッダ」タブを選択する。

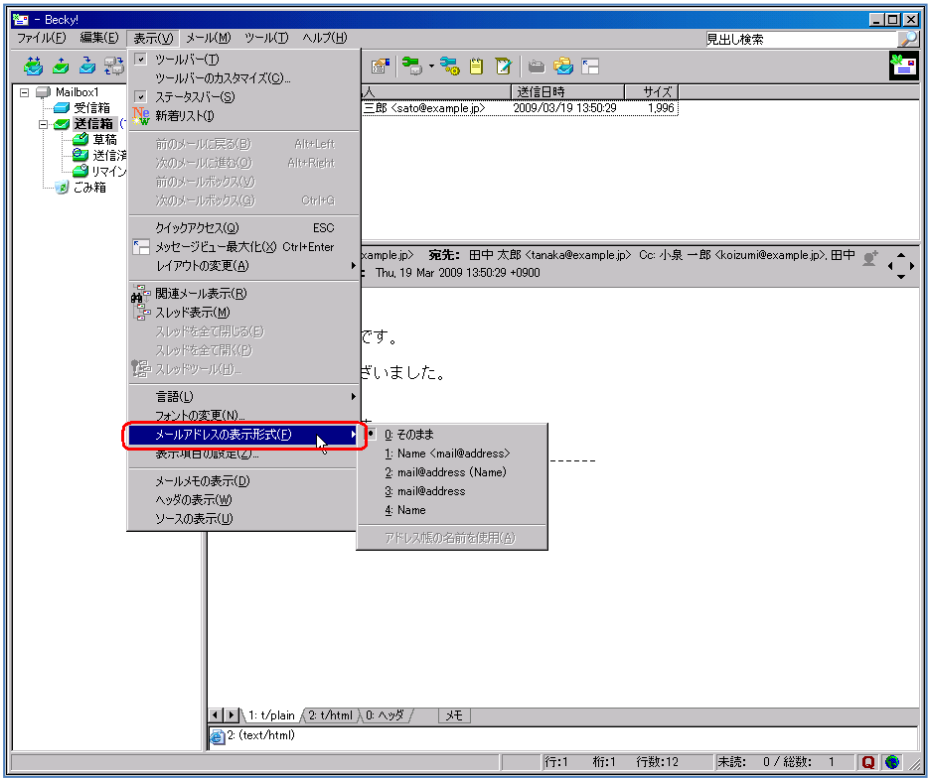


- メールのヘッダ情報が表示される。

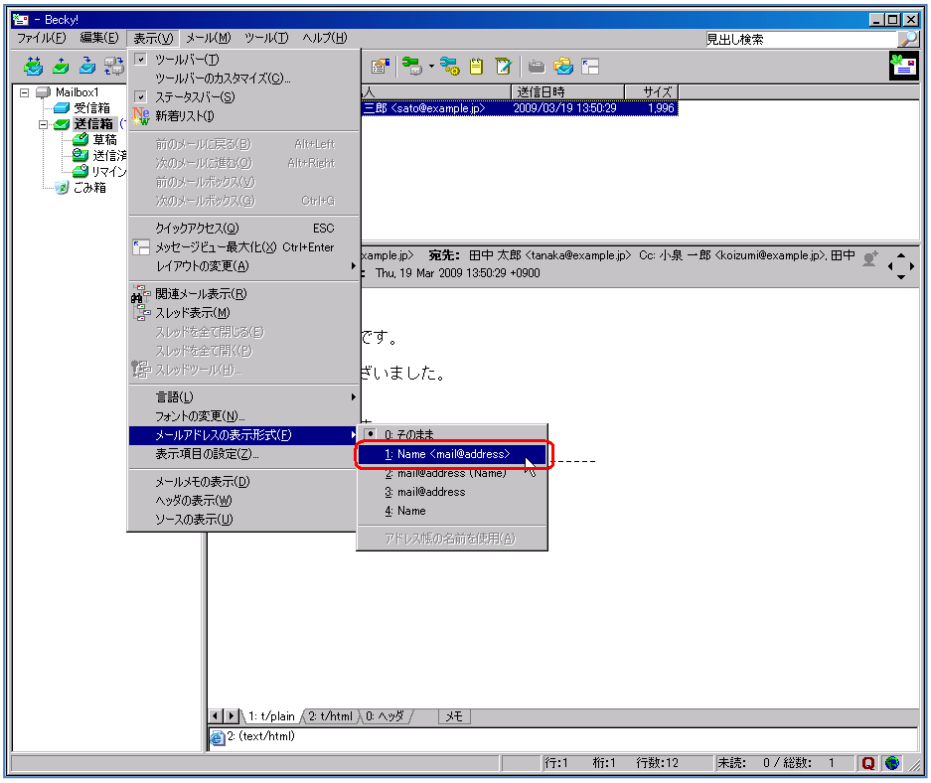


メールアドレスの表示形式の設定

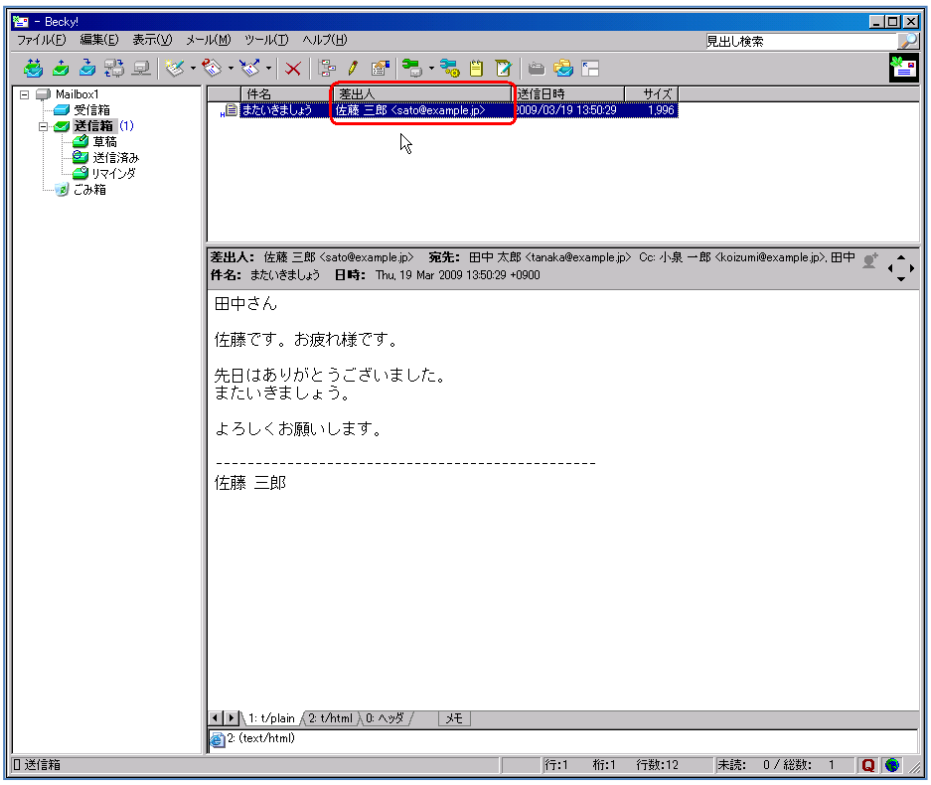
- メニューの「表示」から「メールアドレスの表示形式」を選択する。



- 「Name <mail@address>」、または、「mail@address (Name)」を選択する。



- メールの差出人情報が「表示名＋メールアドレス」の形になる。



S/MIME による署名メールの表示例

Becky!は、標準で S/MIME をサポートしていません。
なお、RimArts 社のウェブページから、S/MIME 対応 Plug-In が配布されているので、必要な方は入手してインストールしてください。

PGP 対応

Becky!は、標準で PGP をサポートしていません。

迷惑メールフィルタの設定

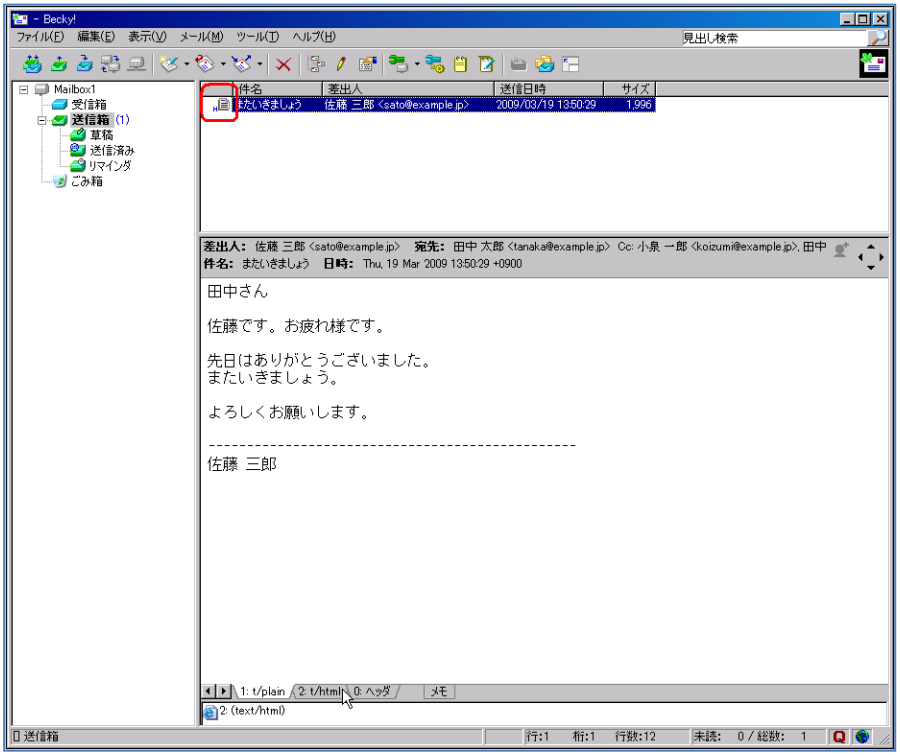
Becky!は、標準で迷惑メールフィルタをサポートしていません。

メール送信フォーマットに関する設定

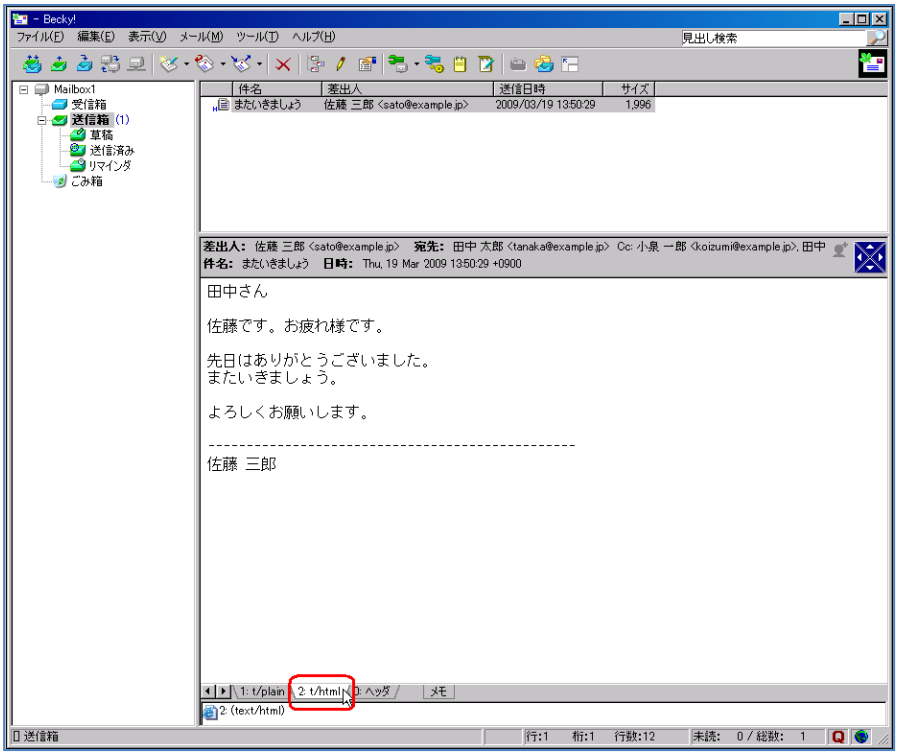
Becky!は、標準でテキスト形式のメールを作成するようになっています。特別な設定は必要ありません。

HTML メールの表示に関する設定

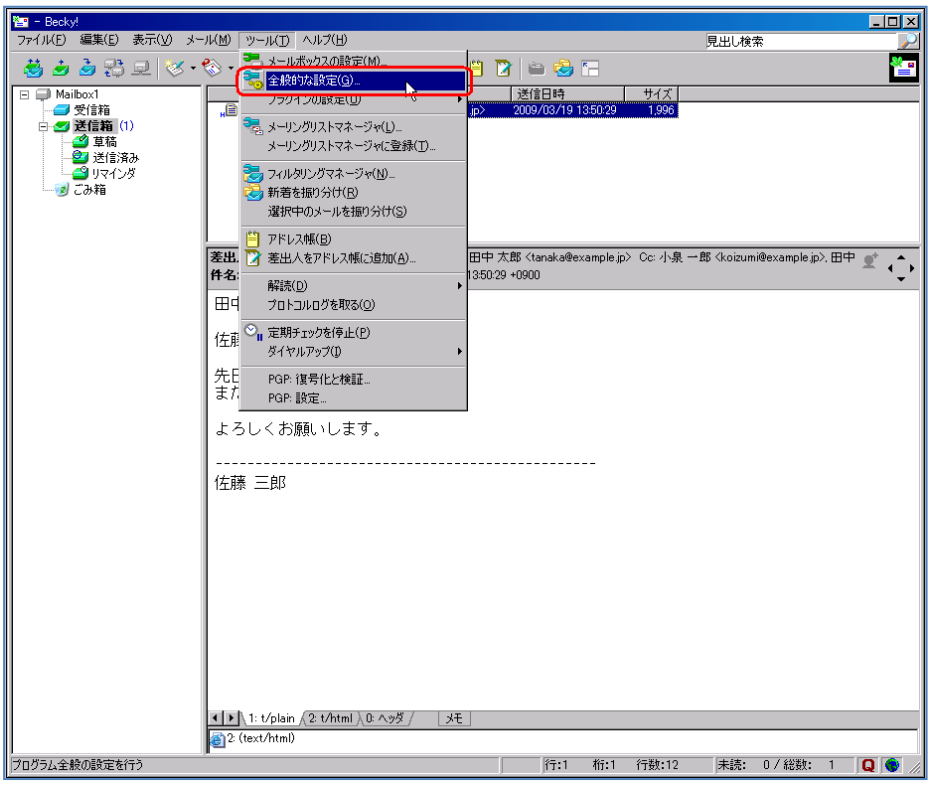
- HTML メールを受信した場合、件名の左側のメールアイコンに「H」の文字が付加される。



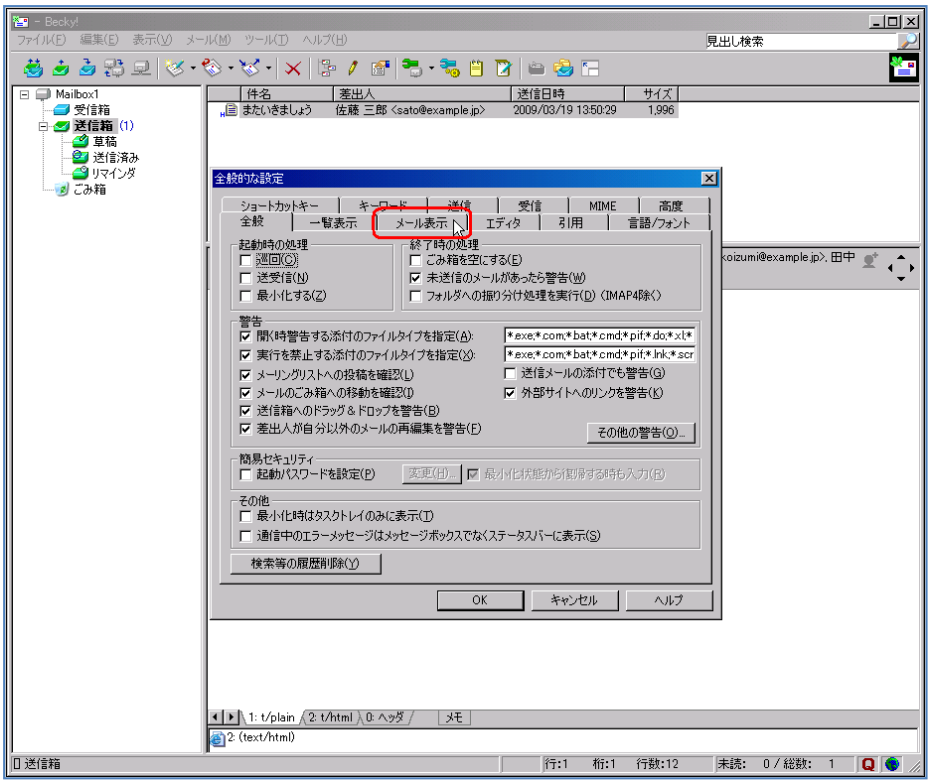
- メール本文下部の「t/html」タブを選択すると、HTML メールを表示する。



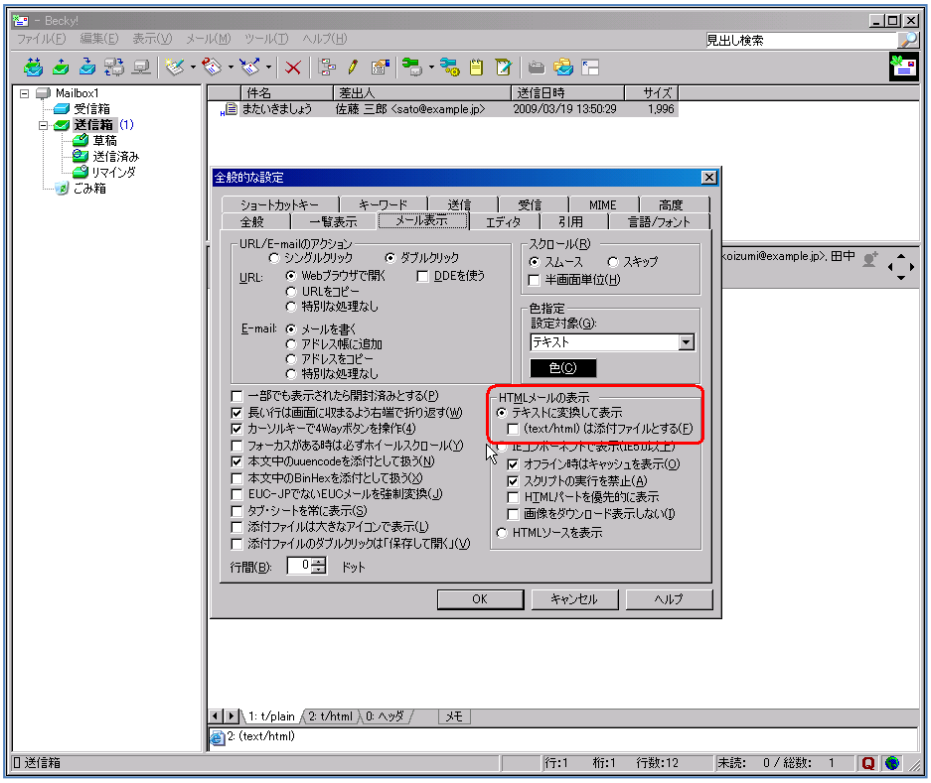
- メニューの「ツール」から「全般的な設定」を選択する。



- 「全般的な設定」ウインドウから「メール表示」タブを選択する。

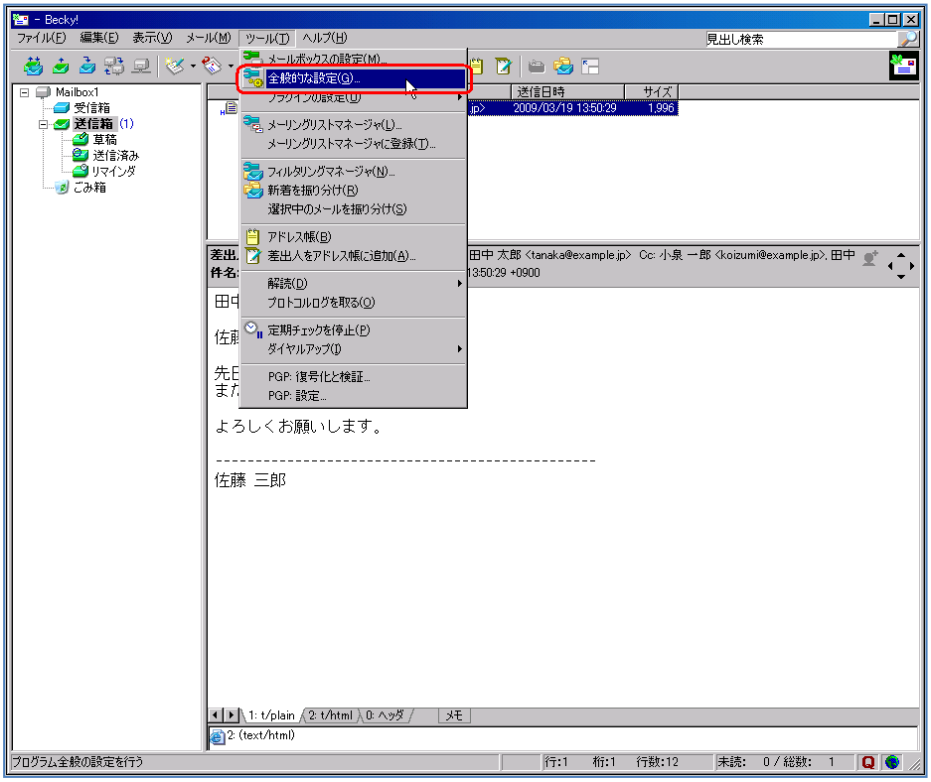


- 「HTML メールの表示」内の「テキストに変換して表示」を選択することで、HTML メールを HTML ソースとして見ることができる。

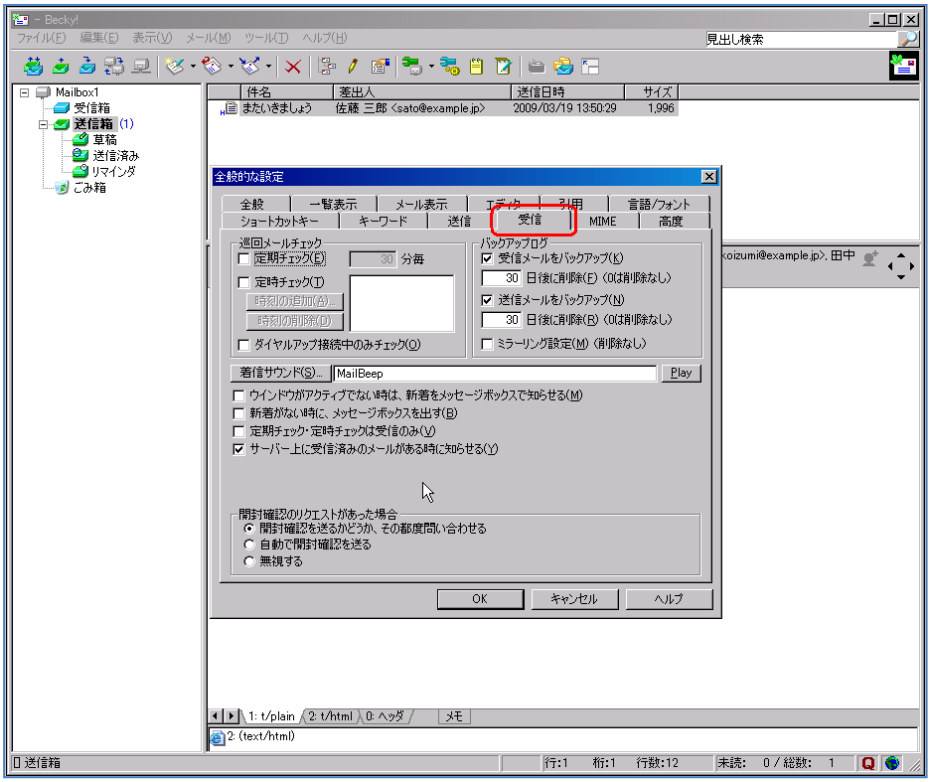


開封確認機能に関する設定

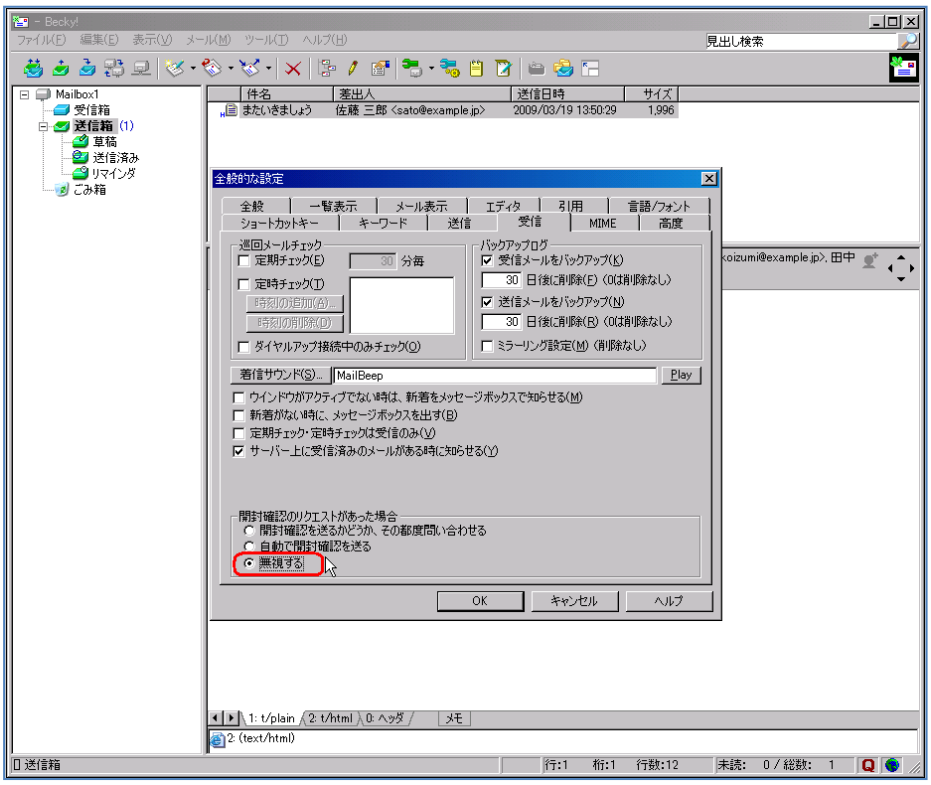
- メニューの「ツール」から「全般的な設定」を選択する。



- 「全体的な設定」ウインドウから「受信」タブを選択する。



- 「開封確認のリクエストがあった場合」内の「無視する」を選択する。

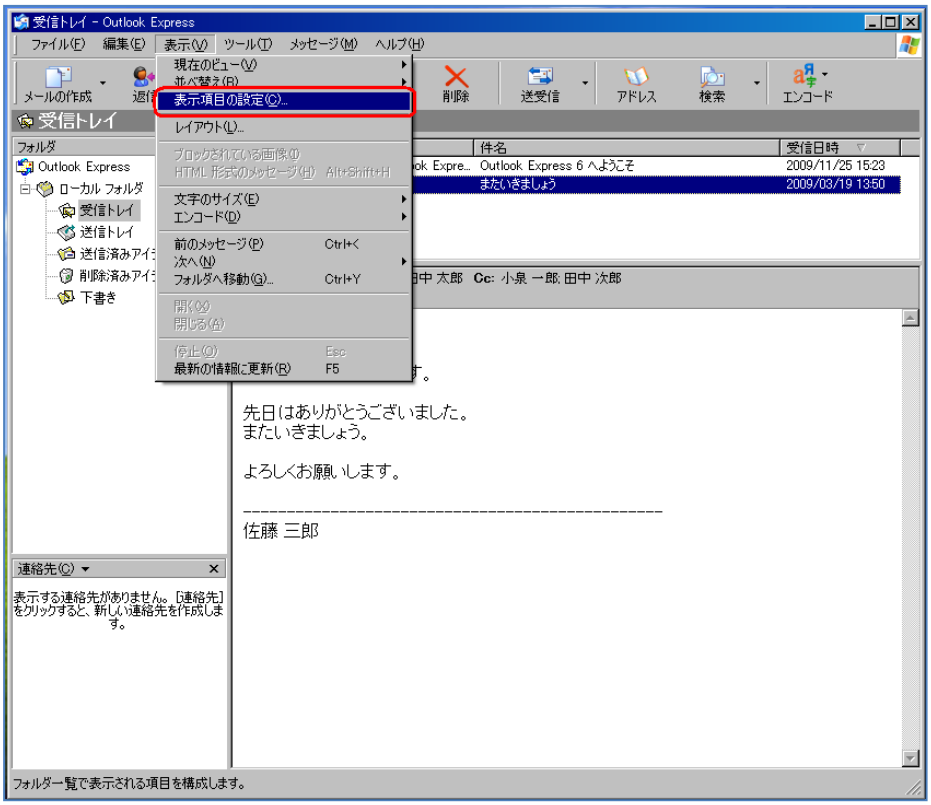


4.3 Outlook Express の設定

4.3.1 各設定

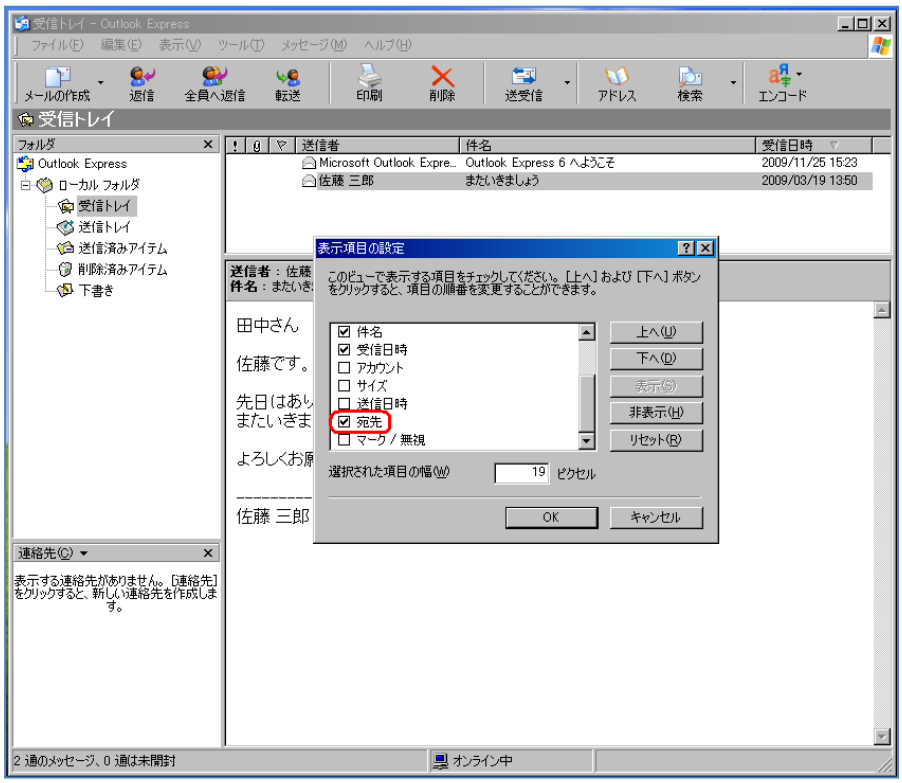
受信メール一覧で表示される情報の拡張

- メニューの「表示」から「表示項目の設定」を選択する。



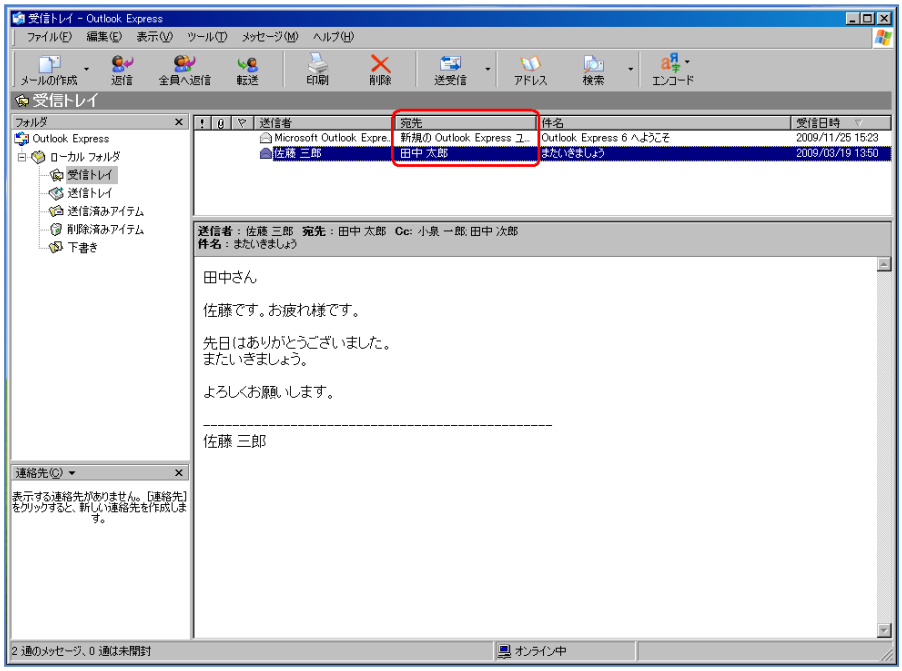
※この画像は Outlook Express 6.00.2900.2180 (xpsp_sp2_rtm.040803-2158) で取得しています。

- 「表示項目の設定」ウインドウの「宛先」のチェックを有効にする。



※この画像は Outlook Express 6.00.2900.2180 (xpsp_sp2_rtm.040803-2158) で取得しています。

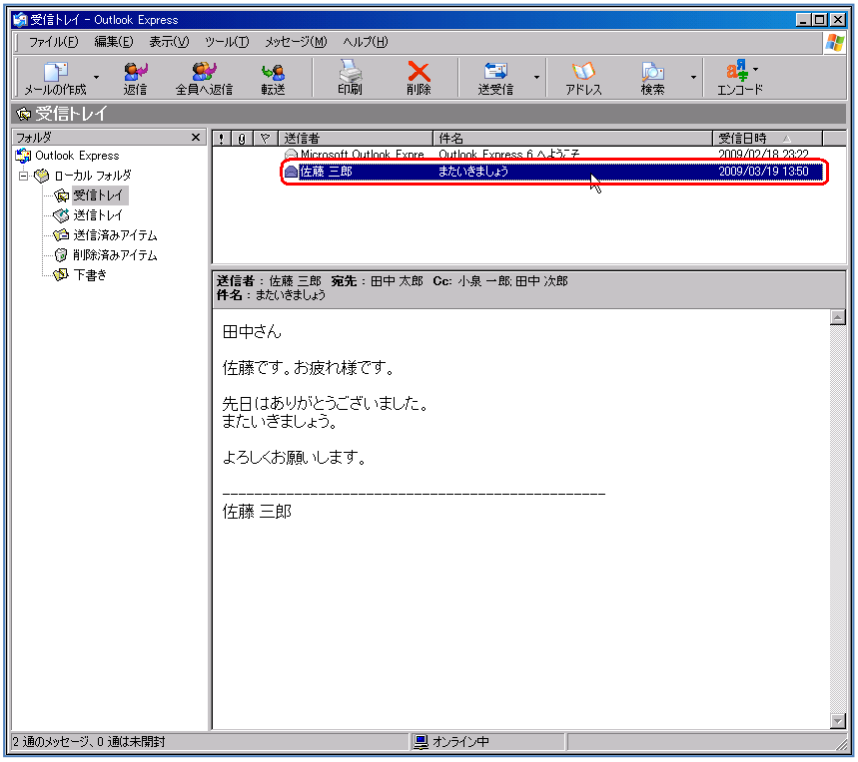
- 「表示項目」に「宛先」が追加されるので、「宛先」をドラッグし「送信者」の右隣に移動する。



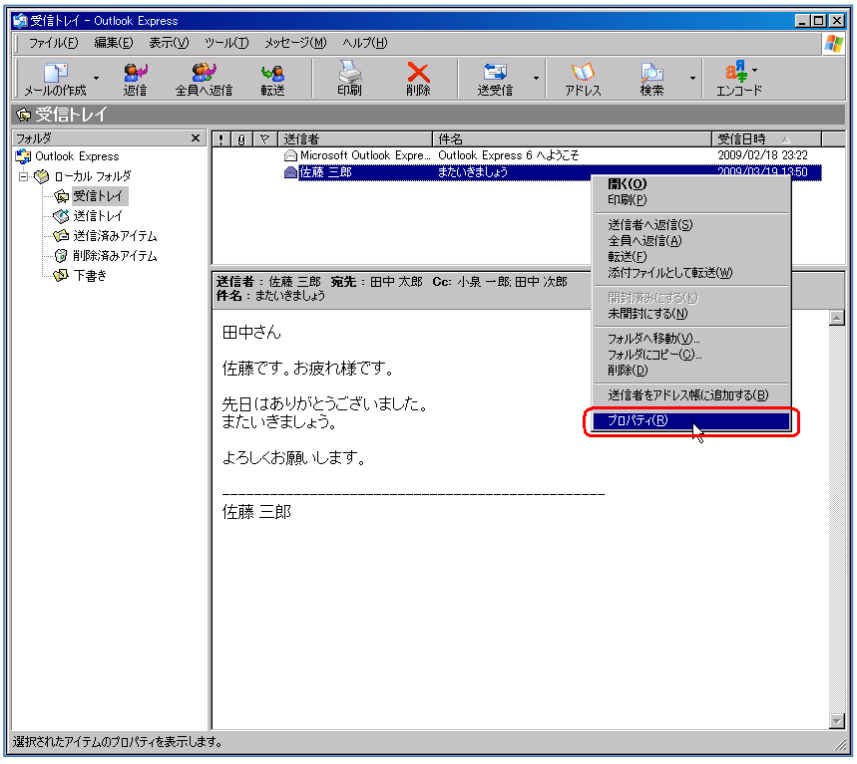
※この画像は Outlook Express 6.00.2900.2180 (xpsp_sp2_rtm.040803-2158) で取得しています。

メールヘッダ情報の確認方法

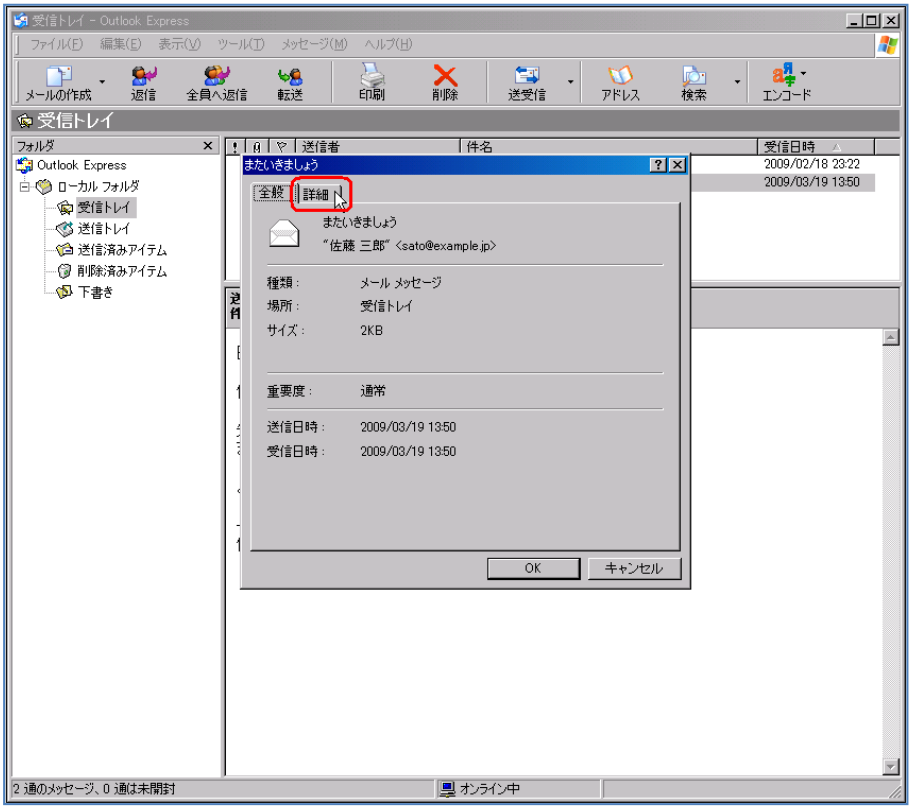
- メールを選択する。



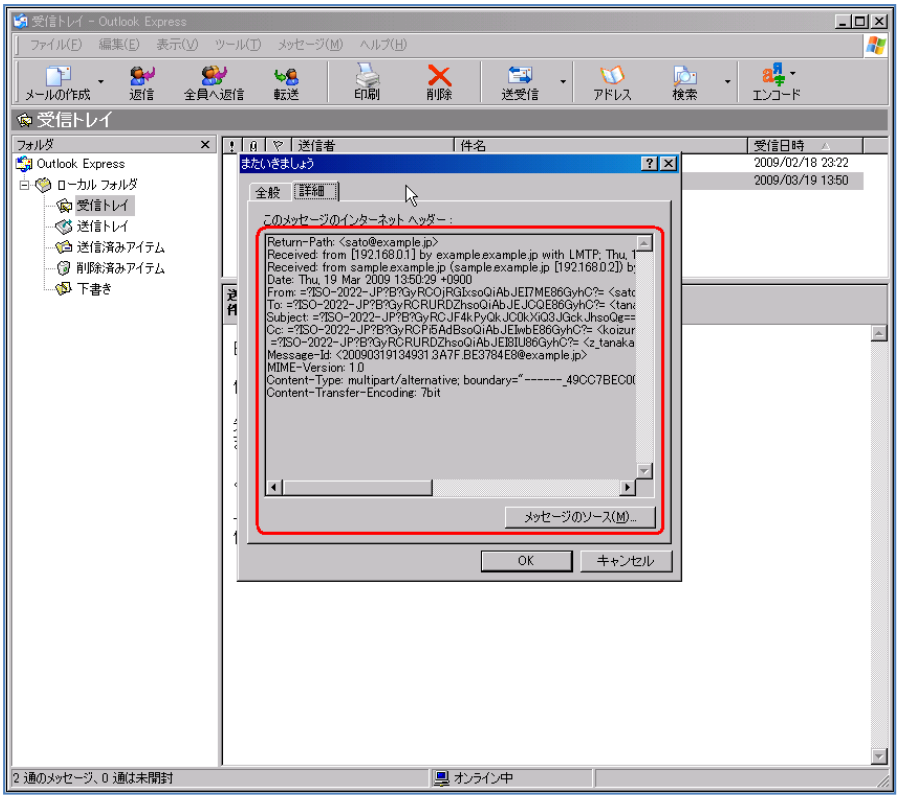
- 右クリックし、「プロパティ」を選択する。



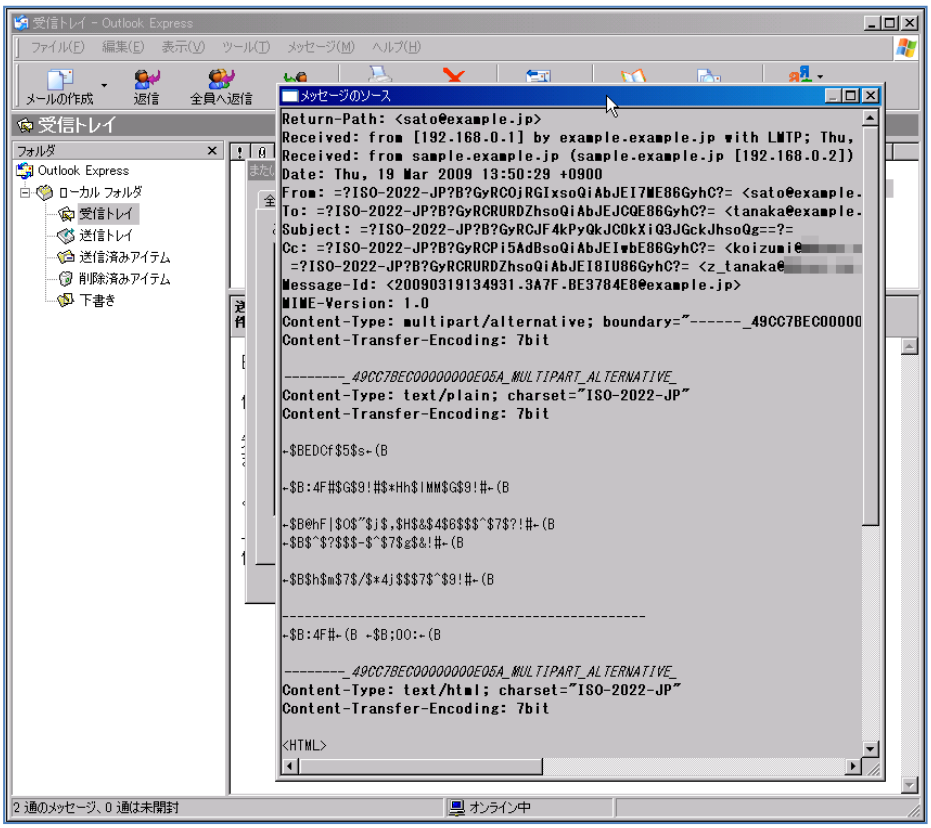
- Subject(件名)ウインドウの「詳細」タブを選択する。



- 「メッセージのソース」をクリックする。



- 「メッセージのソース」ウインドウにヘッダ情報が表示される。

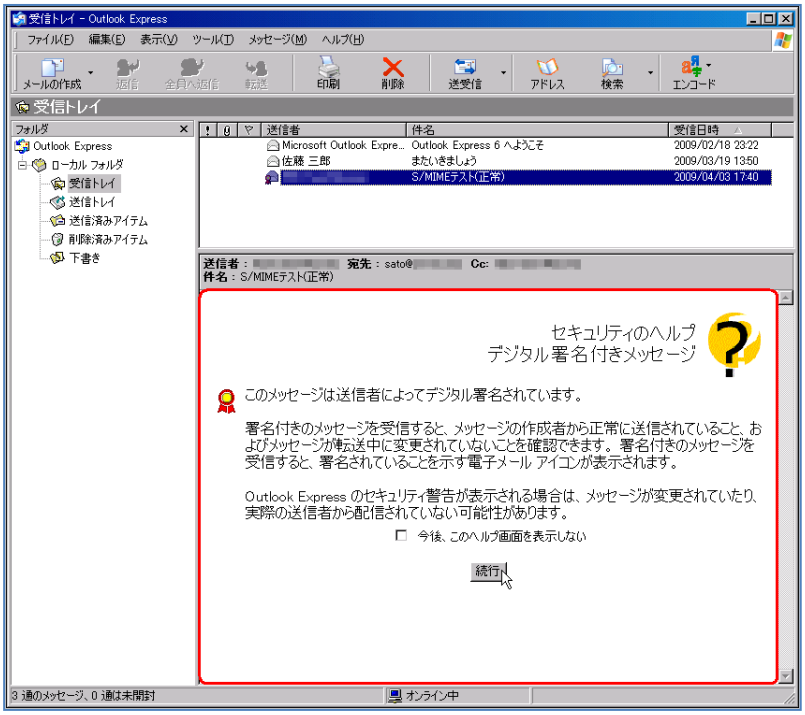


メールアドレスの表示形式の設定

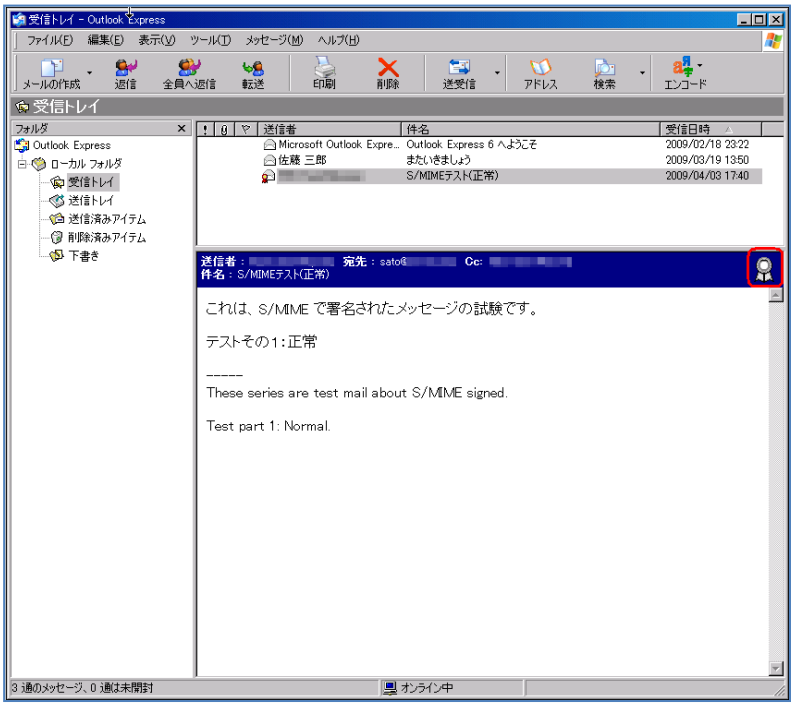
Microsoft Outlook Express のメールアドレスの表示形式は、標準で「表示名」と「メールアドレス」の両方が表示され、変更できません。

S/MIME による署名メールの表示例

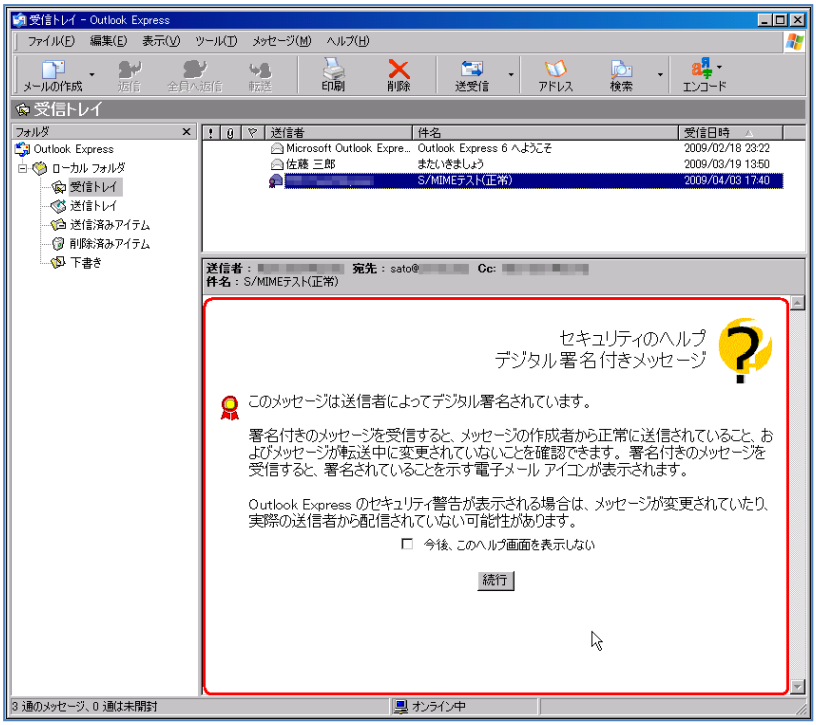
- S/MIME で署名されたメッセージが問題なく検証された場合
  1. デジタル署名されている旨表示される。



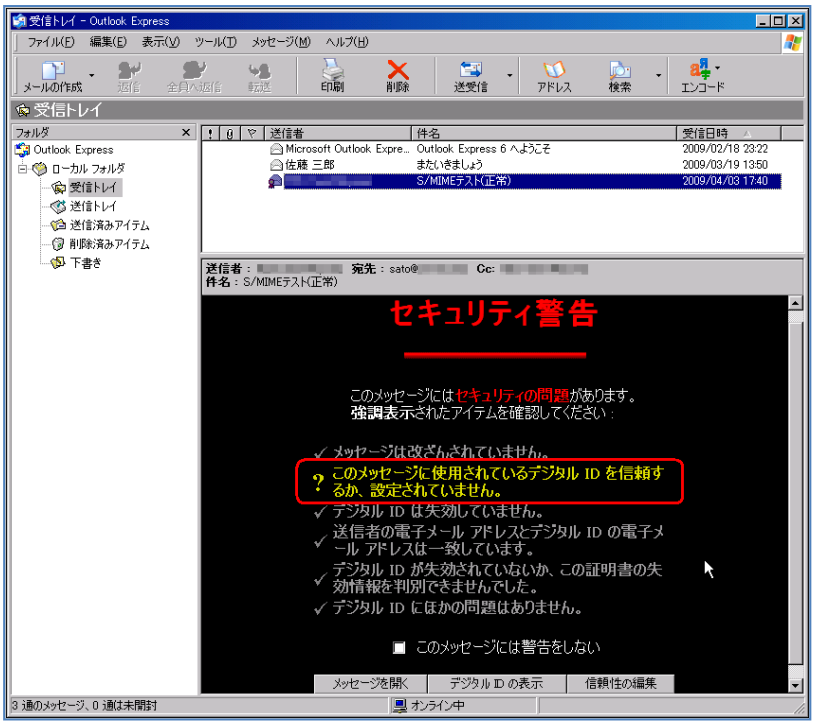
  2. 「続行」ボタンを押すと、メール本文が表示される。
     デジタル署名が正常な場合、メール本文のウインドウの右上にアイコンが表示される。



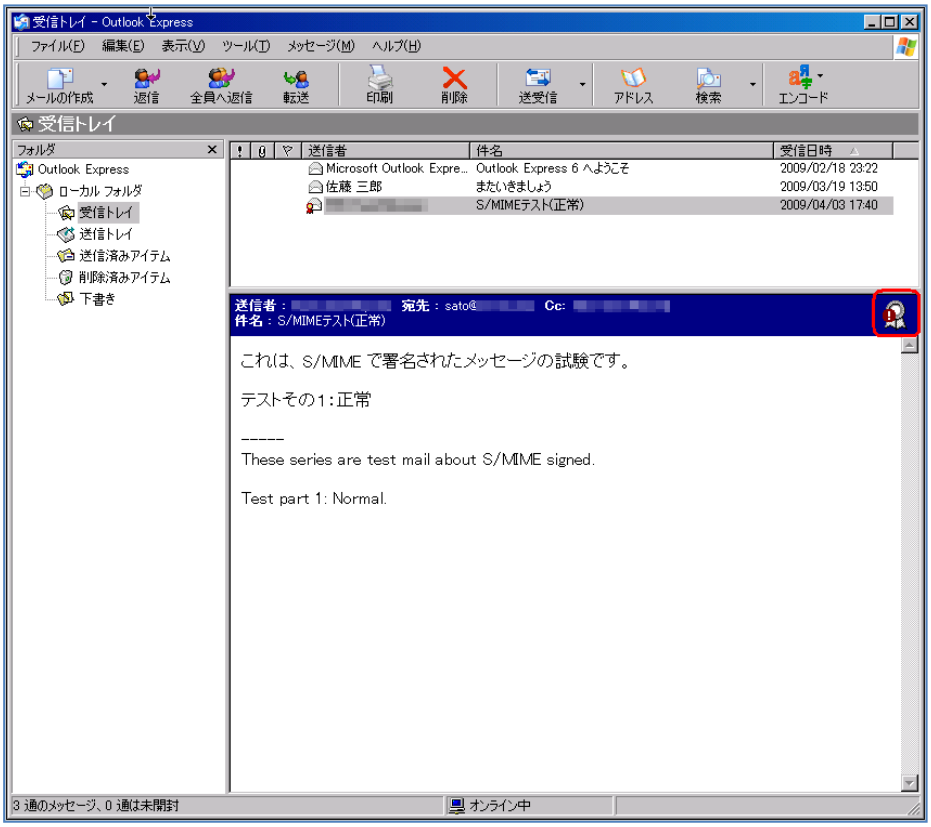
- S/MIME で署名されたメッセージの証明書が検証できない場合
  1. デジタル署名されている旨表示される。



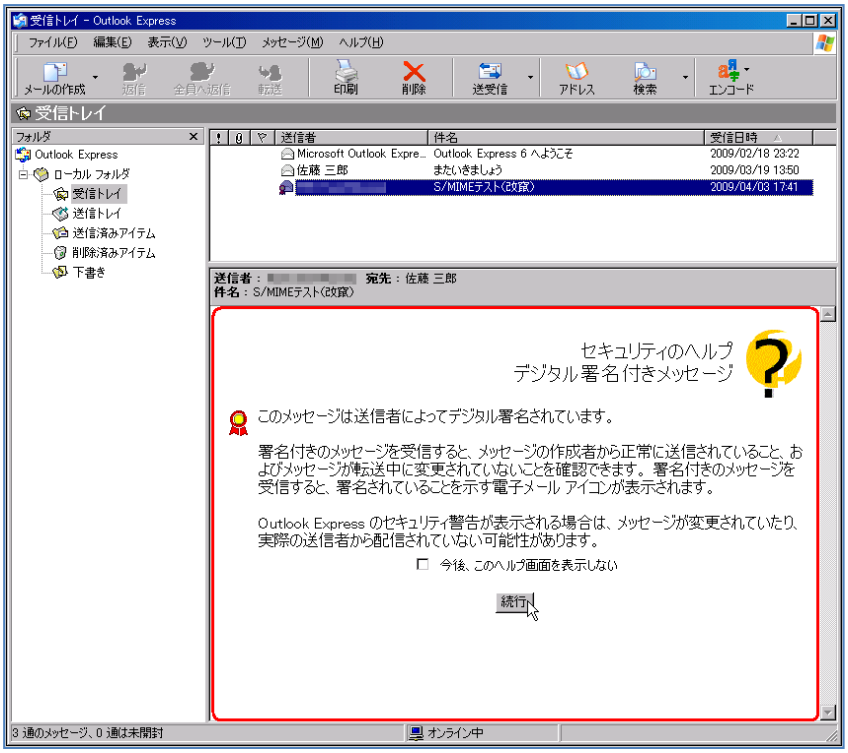
  2. 「続行」ボタンを押すと、セキュリティ警告のメッセージが表示される。
証明書を検証出来ない場合、強調表示されている部分に「このメッセージに使用されているデジタル ID を信頼するか、設定されていません。」と表示される。



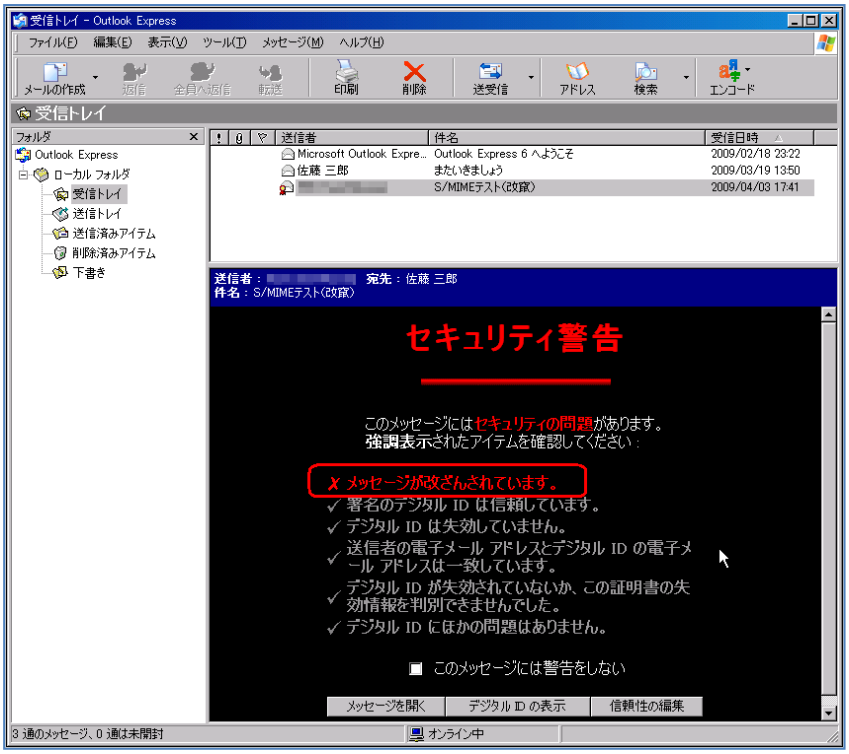
3. 「メッセージを開く」を選択すると、メッセージが表示される。
メール本文のウインドウの右上にアイコンが表示される。このアイコンが表示されている場合、何らかの問題があったことになります。



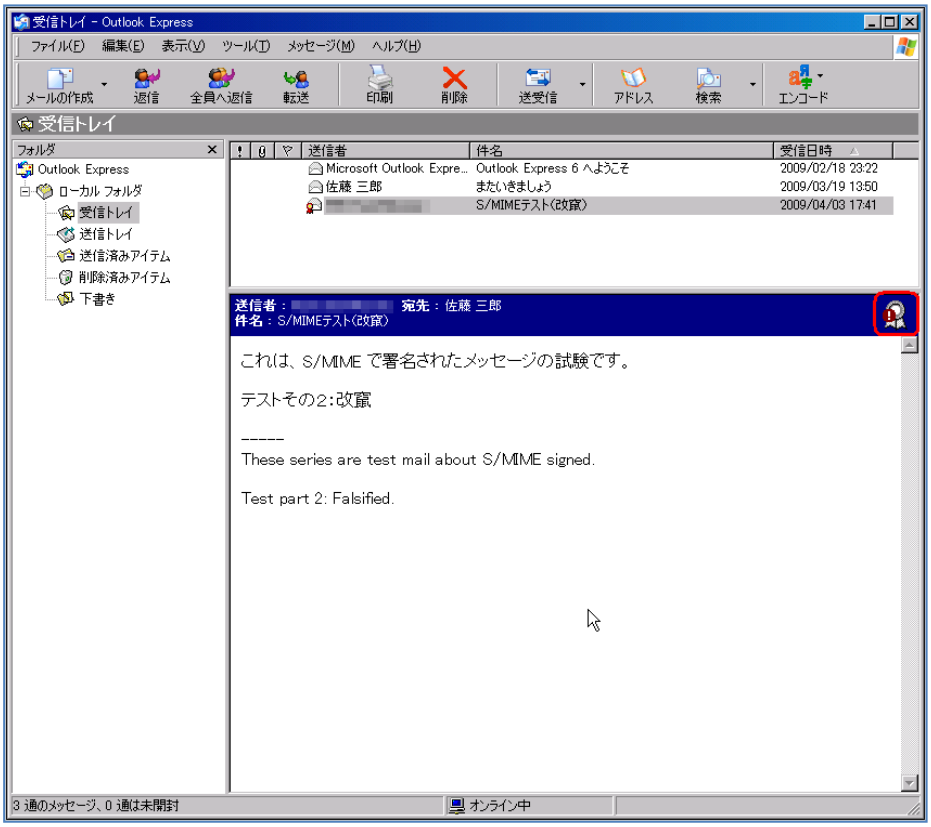
- S/MIME で署名されたメッセージが改ざんされている場合
  1. デジタル署名されている旨表示される。



  2. 「続行」ボタンを押すと、セキュリティ警告のメッセージが表示される。
メッセージが改ざんされている場合、強調表示されている部分に「メッセージが改ざんされています。」と表示される。



3. 「メッセージを開く」を選択すると、メッセージが表示される。
メール本文のウインドウの右上にアイコンが表示される。このアイコンが表示されている場合、何らかの問題があったことになります。



PGP 対応

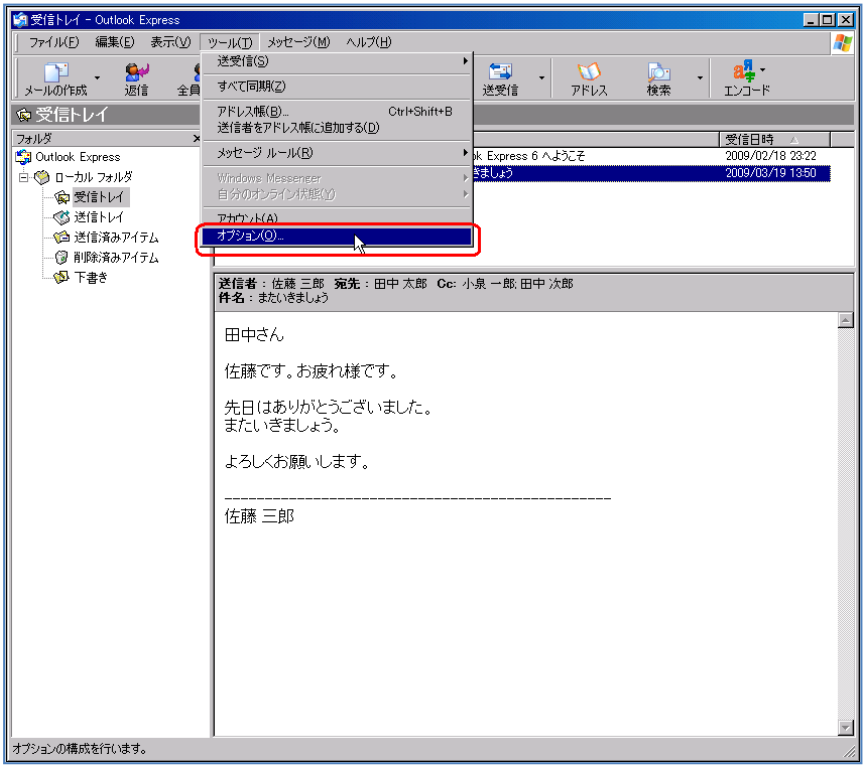
Microsoft Outlook Express は、標準で PGP をサポートしていません。

迷惑メールフィルタの設定

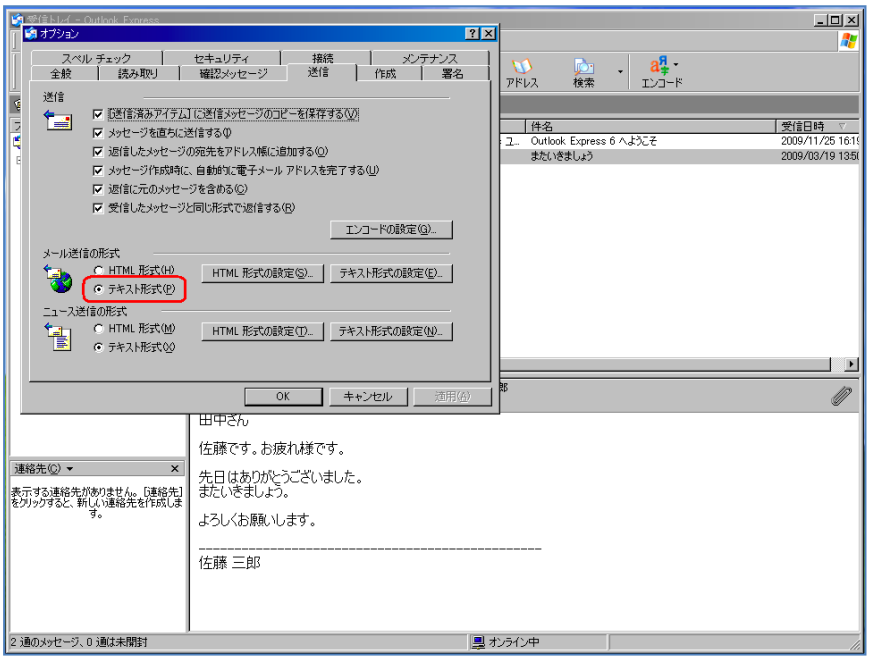
Microsoft Outlook Express は、標準で迷惑メールフィルタをサポートしていません。

メール送信フォーマットに関する設定

- メニューの「ツール」から「オプション」を選択する。



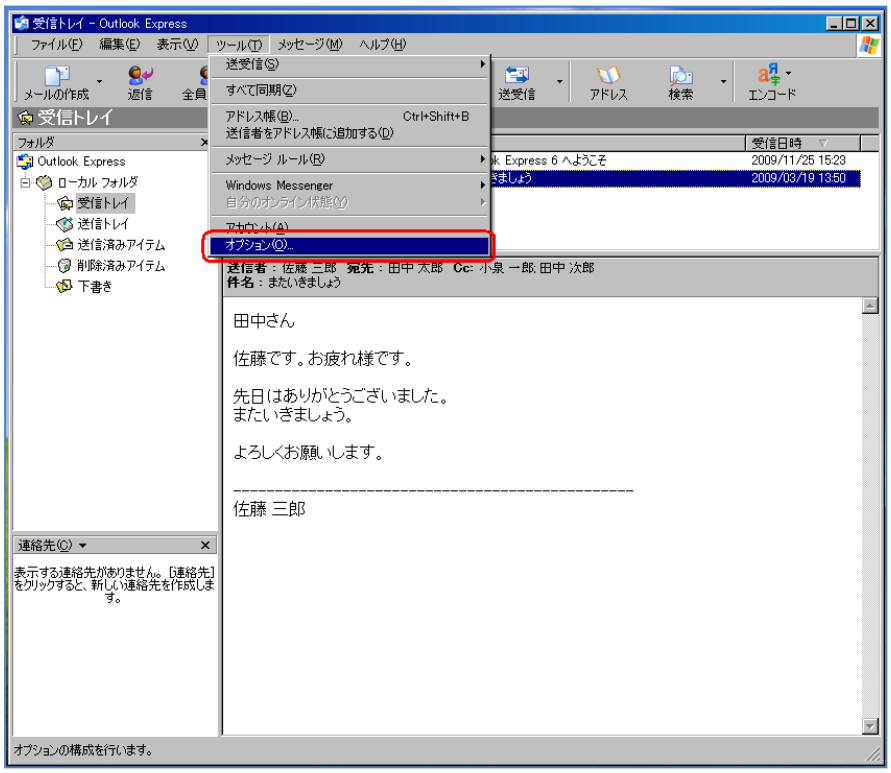
- 「オプション」ウインドウの「送信」タブを選択し、「メール送信形式」を「テキスト形式」にする。



※この画像は Outlook Express 6.00.2900.2180 (xpsp_sp2_rtm.040803-2158) で取得しています。

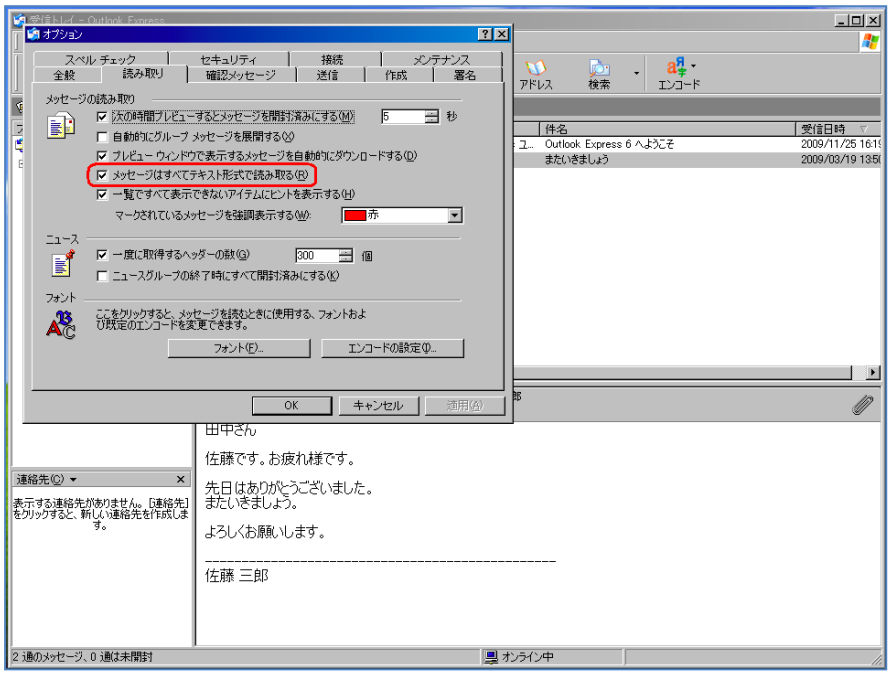
HTML メールの表示に関する設定

- メニューの「ツール」から「オプション」を選択する。



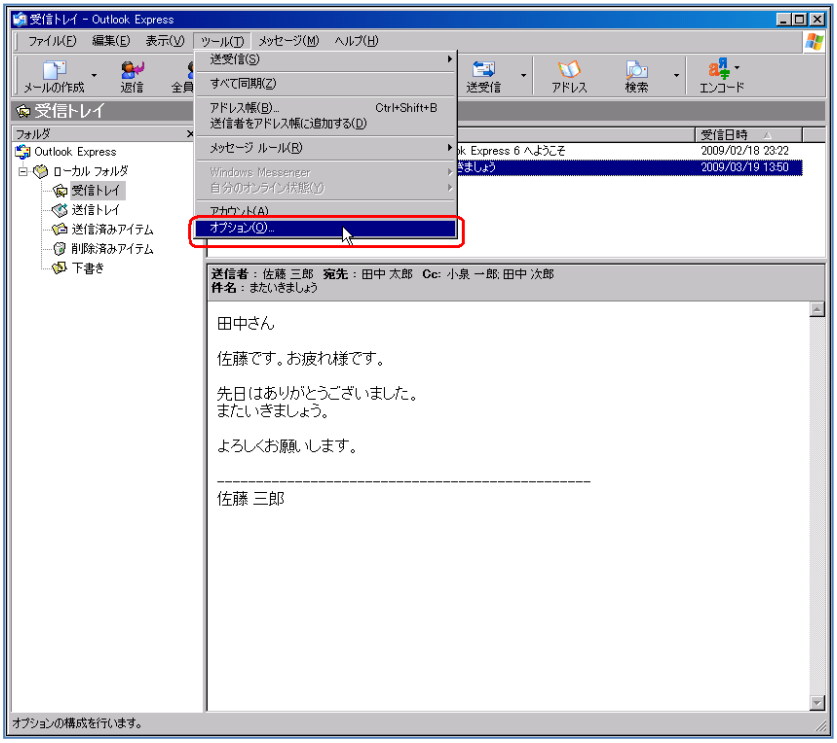
※この画像は Outlook Express 6.00.2900.2180 (xpsp_sp2_rtm.040803-2158) で取得しています。

- 「オプション」ウインドウの「読み取り」タブを選択し、「メッセージはすべてテキスト形式で読み取る」のチェックを有効にする。

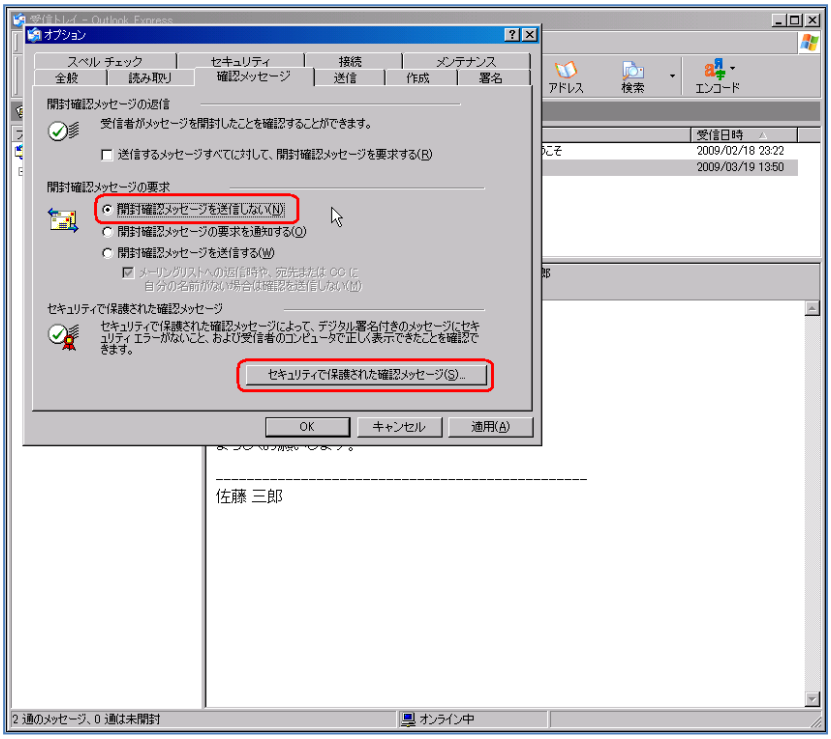


開封確認機能に関する設定

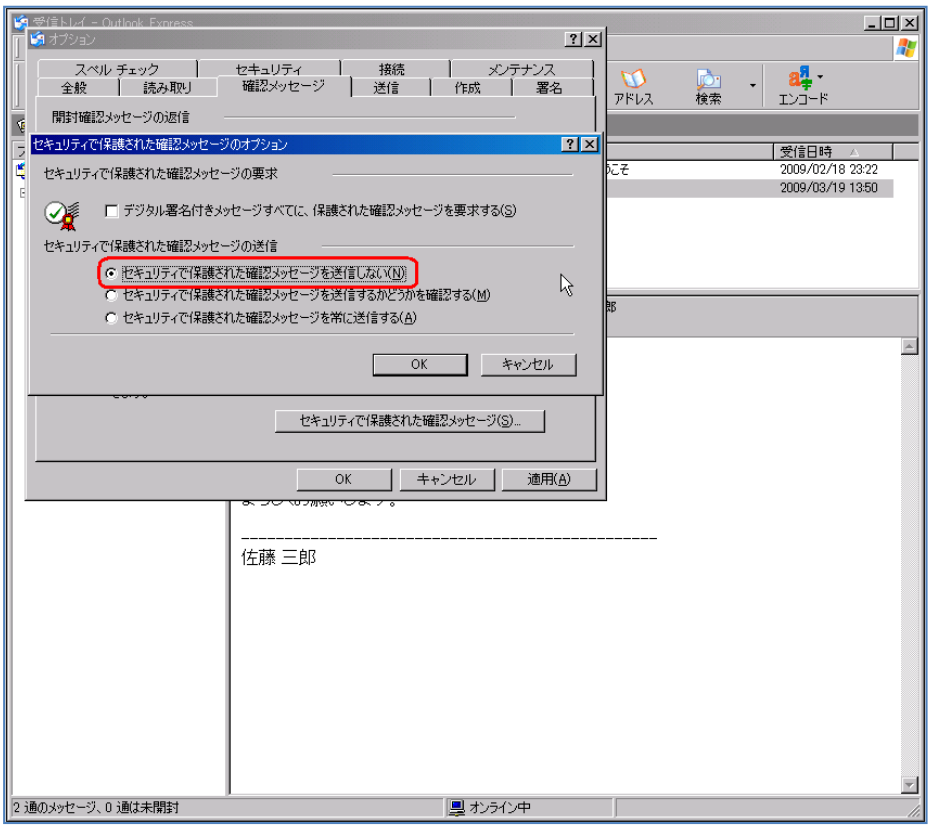
- メニューの「ツール」から「オプション」を選択する。



- 「オプション」ウインドウの「確認メッセージ」タブを選択し、「開封確認メッセージを送信しない」をチェック後、「セキュリティで保護された確認メッセージ」を選択する。



- 「セキュリティで保護された確認メッセージを送信しない」をチェックする。

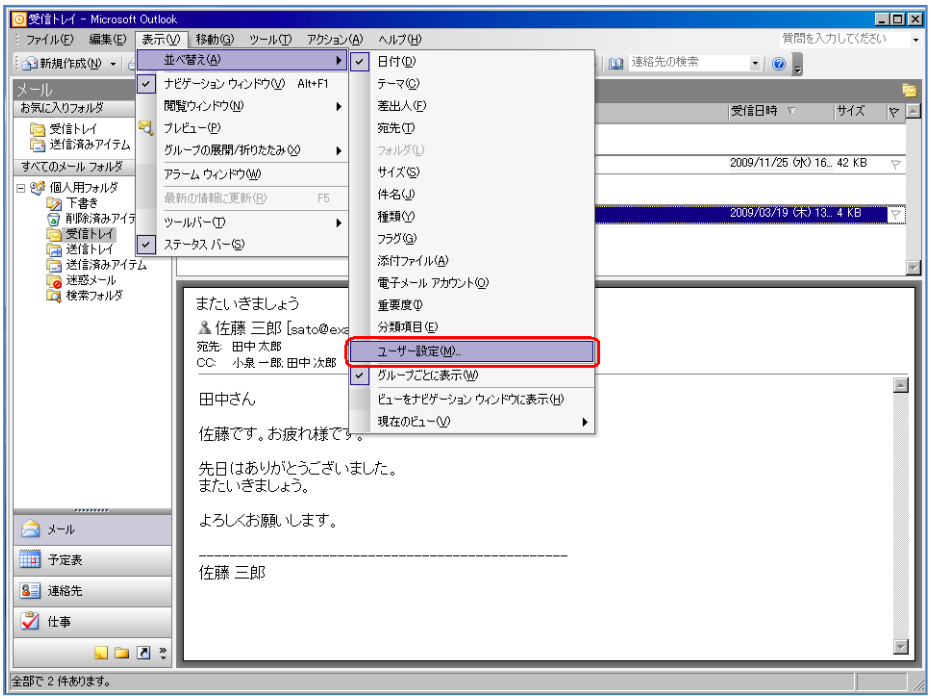


4.4 Outlook 2003 の設定

4.4.1 各設定

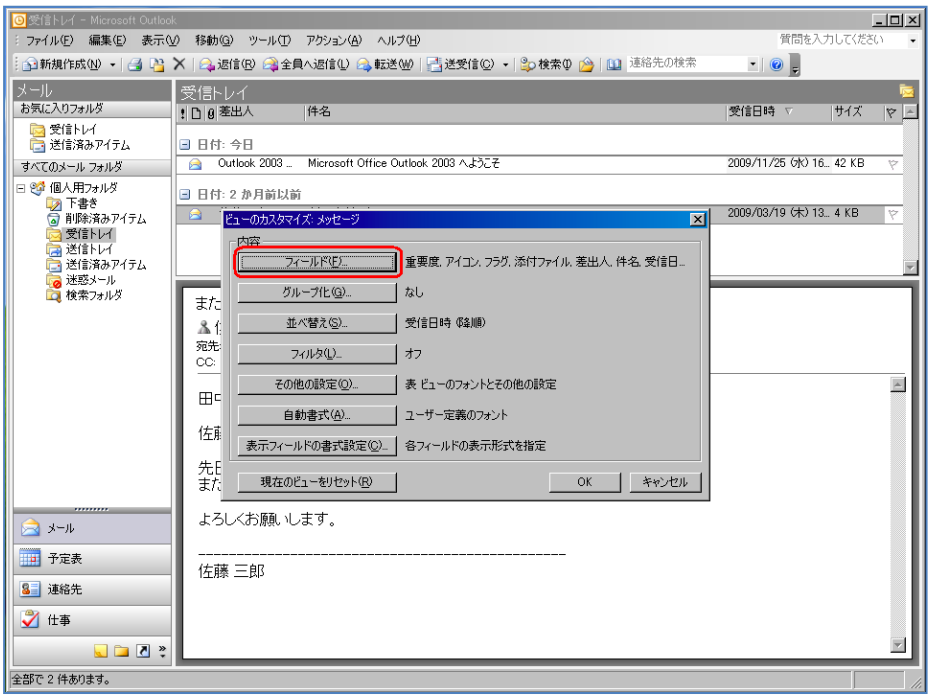
受信メール一覧で表示される情報の拡張

- メニューの「表示」から「並び替え」を選択し、「ユーザ設定」を選択する。



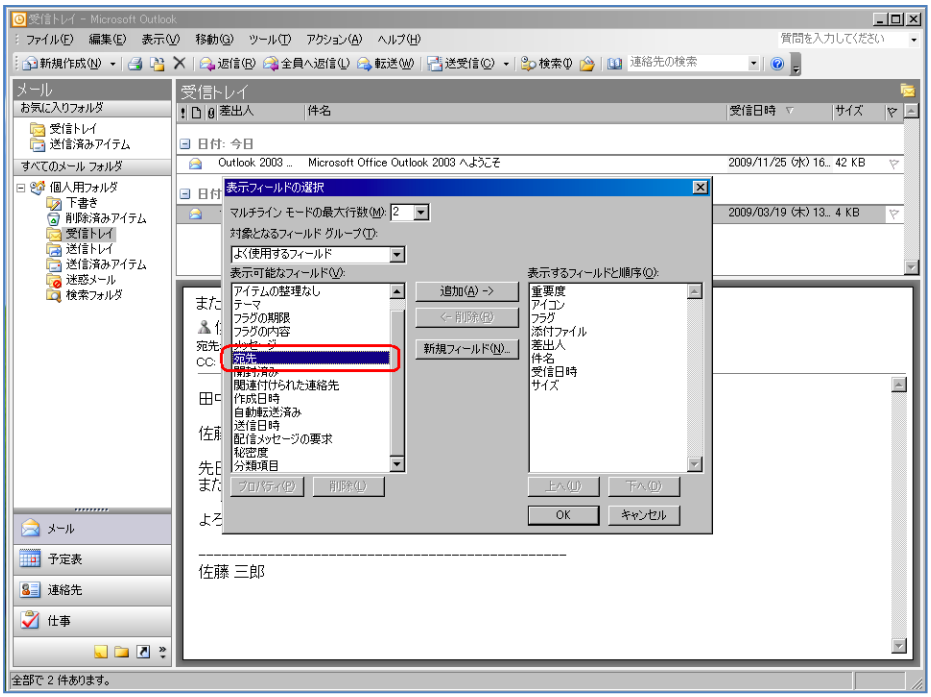
※この画像は Microsoft(R) Office Outlook(R) 2003(11.5608.5606) で取得しています。

- 「ビューのカスタマイズ：メッセージ」ウインドウの「フィールド」ボタンを押す。



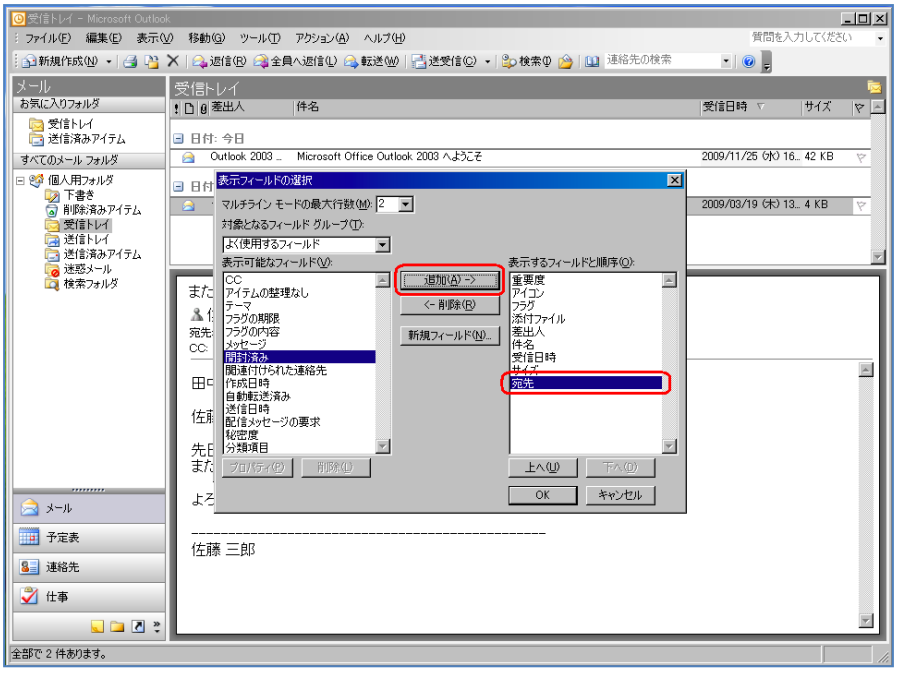
※この画像は Microsoft(R) Office Outlook(R) 2003(11.5608.5606) で取得しています。

- 「表示フィールドの選択」ウインドウの「表示可能なフィールド」内の「宛先」を選択する。



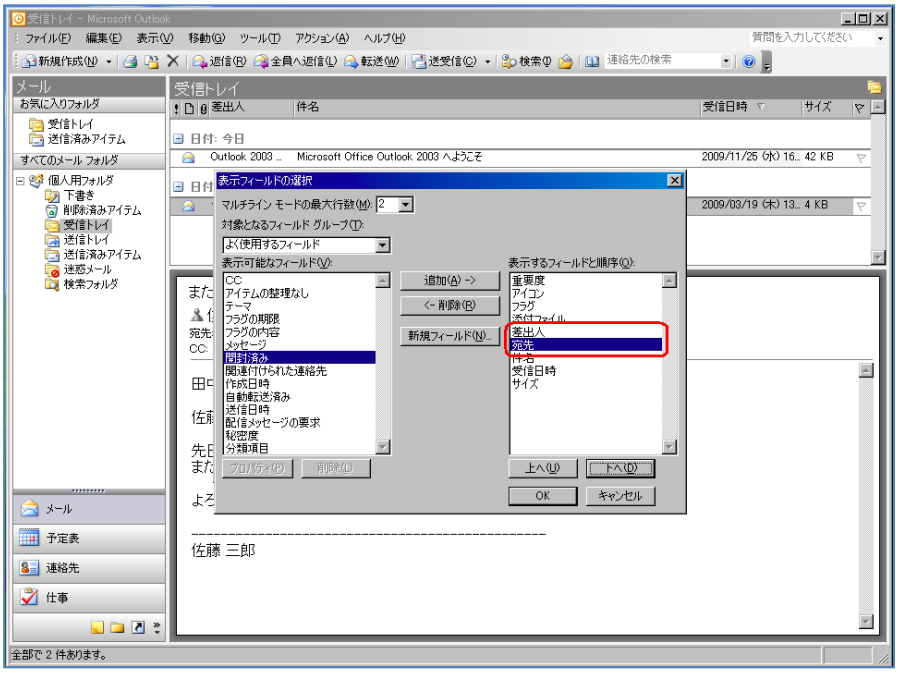
※この画像は Microsoft(R) Office Outlook(R) 2003(11.5608.5606) で取得しています。

- 「表示フィールドの選択」ウインドウの「追加」ボタンを押して、「表示するフィールドと順序」に「宛先」を追加する。



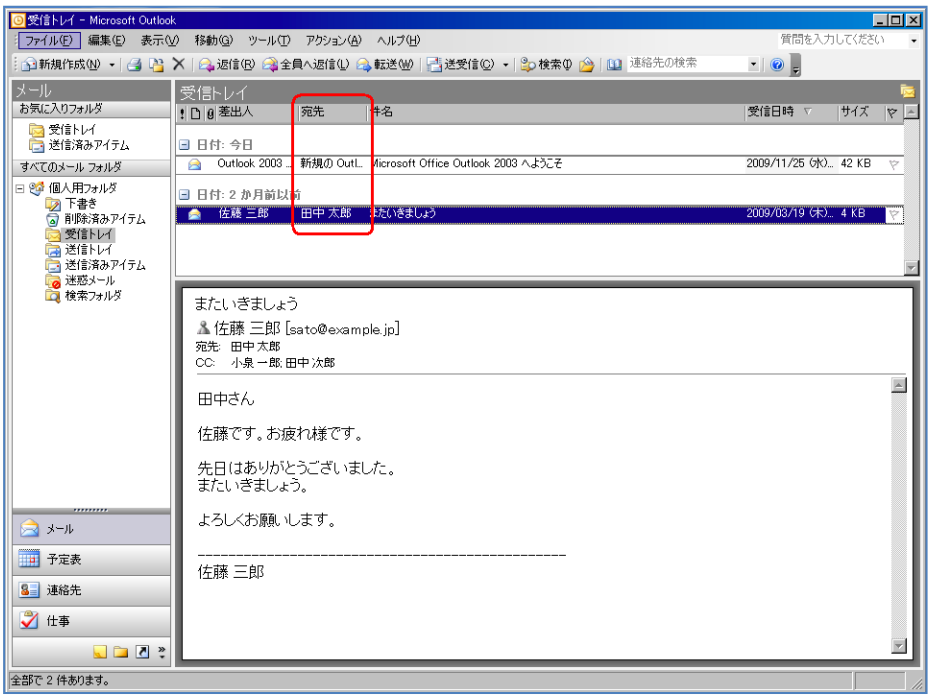
※この画像は Microsoft(R) Office Outlook(R) 2003(11.5608.5606) で取得しています。

- 「表示するフィールドと順序」に追加された「宛先」を「差出人」の下部に移動する。



※この画像は Microsoft(R) Office Outlook(R) 2003(11.5608.5606) で取得しています。

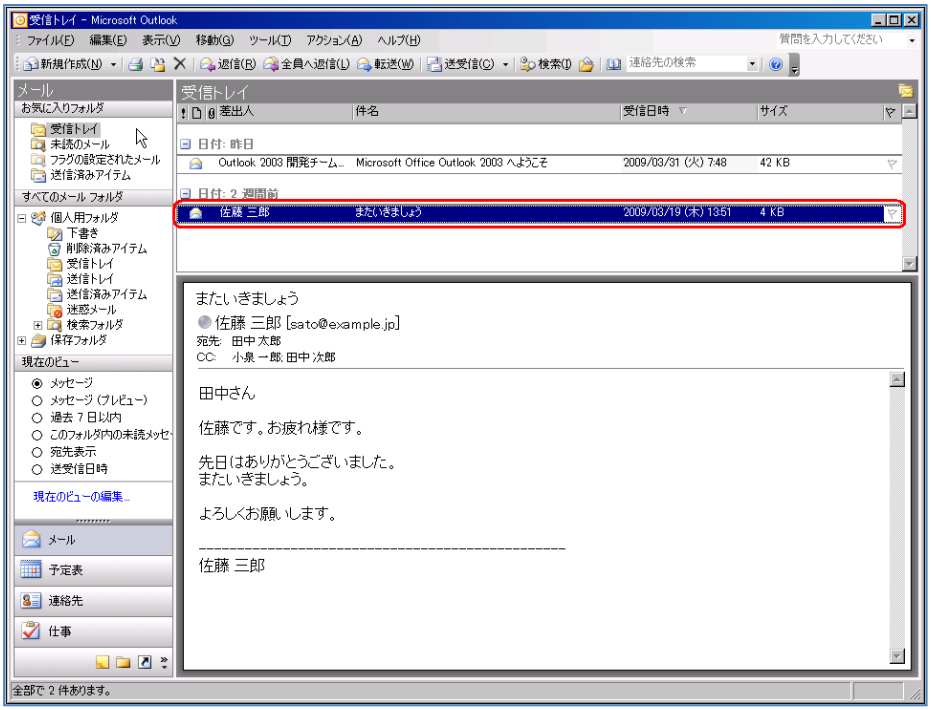
- 表示項目に「宛先」が追加される。



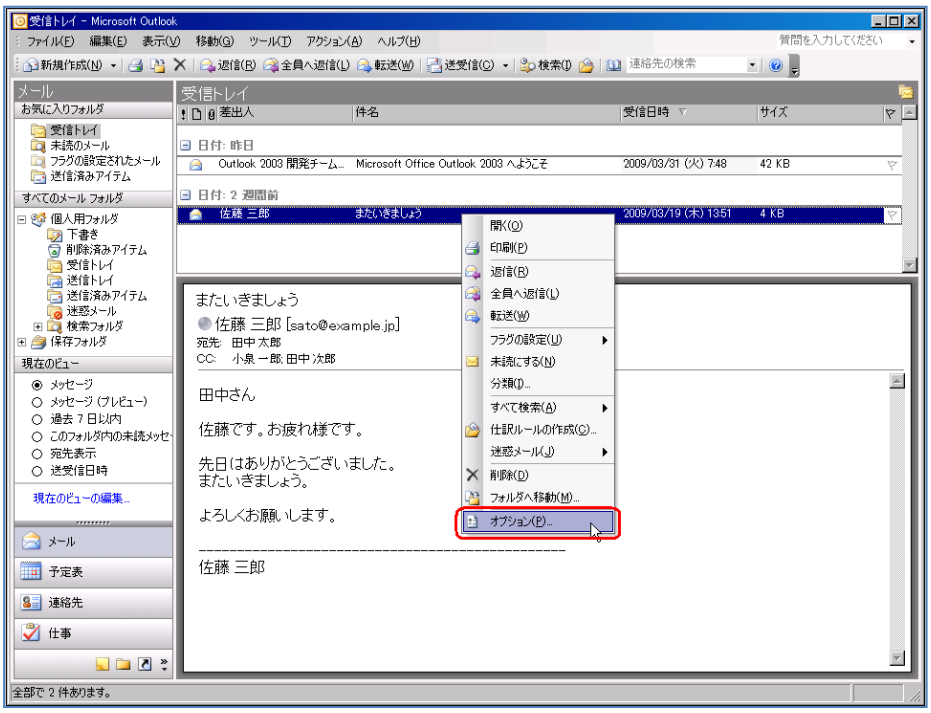
※この画像は Microsoft(R) Office Outlook(R) 2003(11.5608.5606) で取得しています。

メールヘッダ情報の確認方法

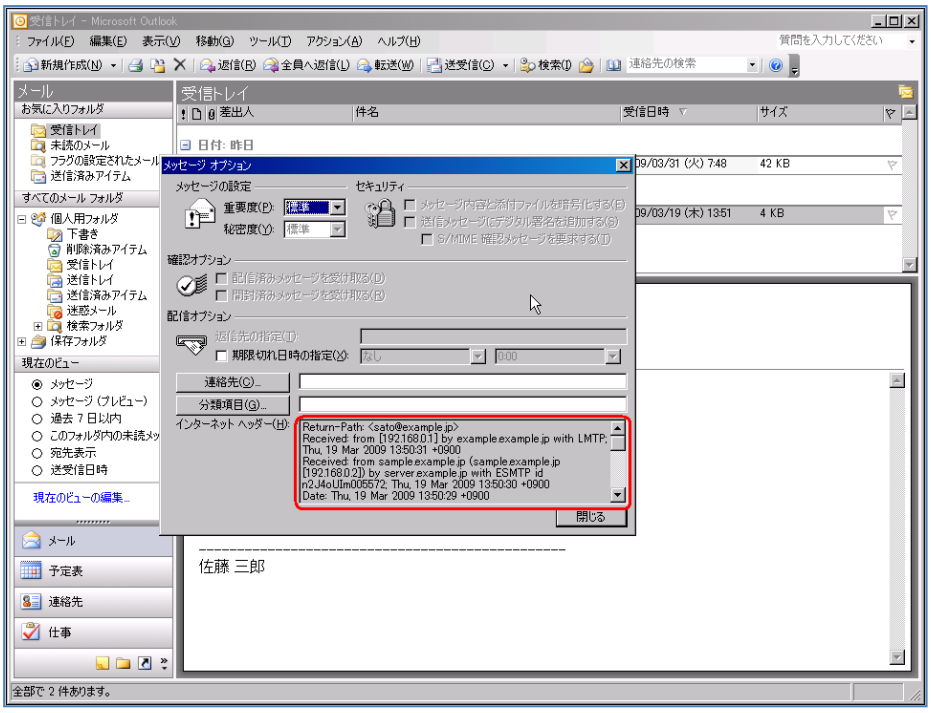
- メールを選択する。



- 右クリックし、「オプション」を選択する。



- 「メッセージオプション」ウインドウの「インターネットヘッダ」にヘッダ情報が表示される。

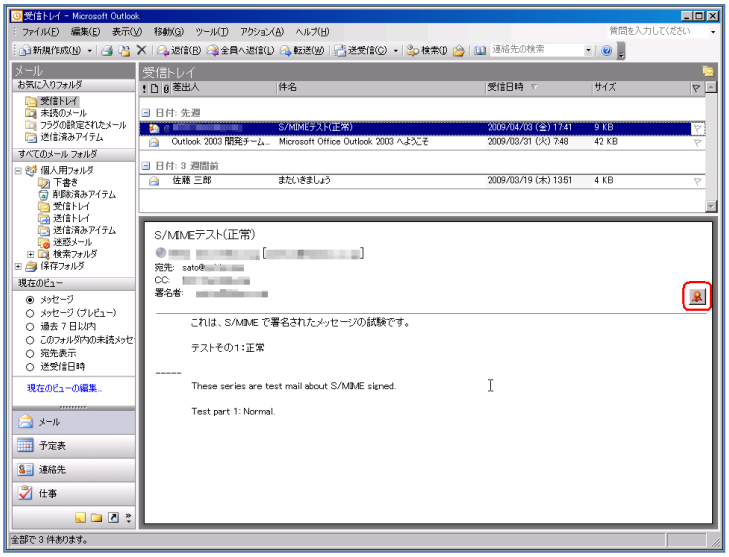


メールアドレスの表示形式の設定

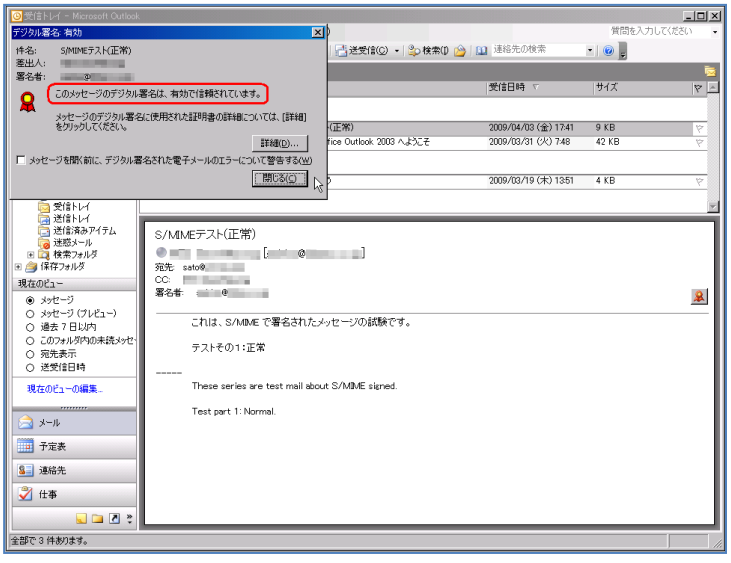
Microsoft Outlook 2003 は、標準で差出人の情報として「表示名」と「メールアドレス」の両方を表示します。特別な設定は必要ありません。

S/MIME による署名メールの表示例

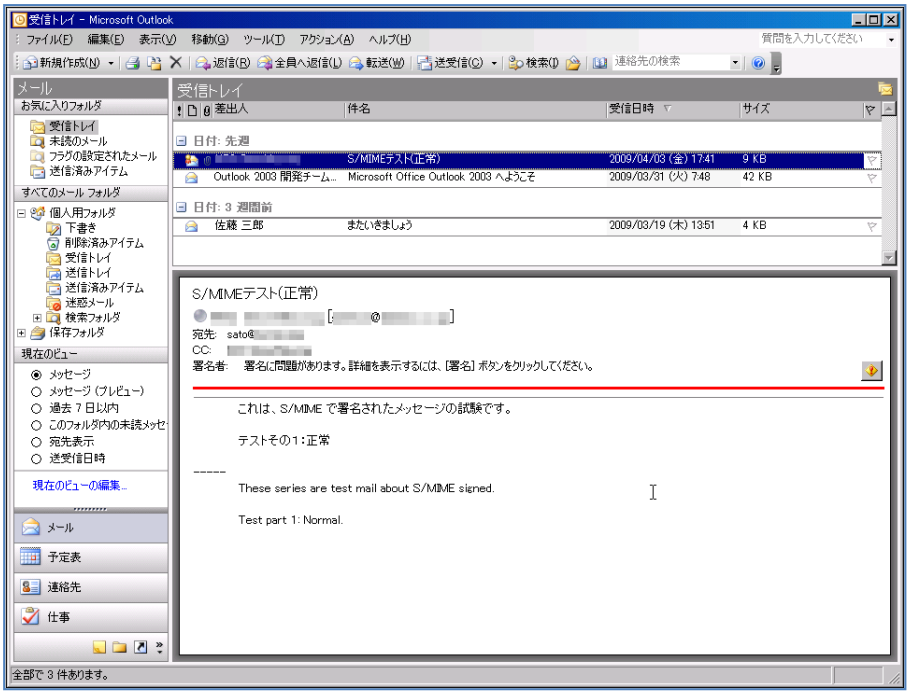
- S/MIME で署名されたメッセージが問題なく検証された場合
  1. メール本文は表示され、ウインドウの右上にアイコンが表示される。



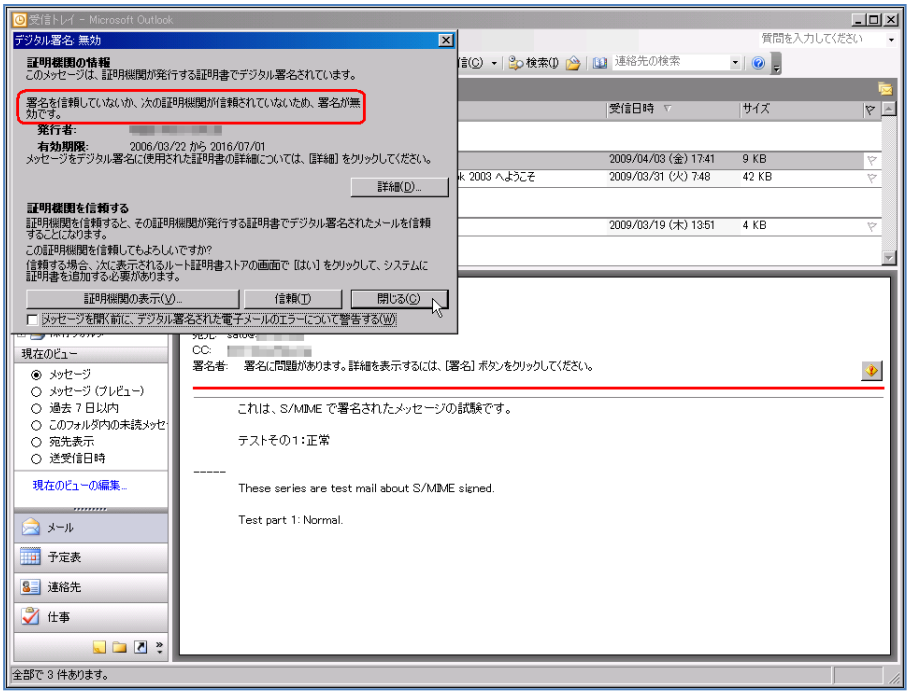
  2. アイコンをクリックすると、「デジタル署名：有効」ウインドウが開く。
     ウインドウ内に「このメッセージのデジタル署名は、有効で信頼されています。」と表示される。



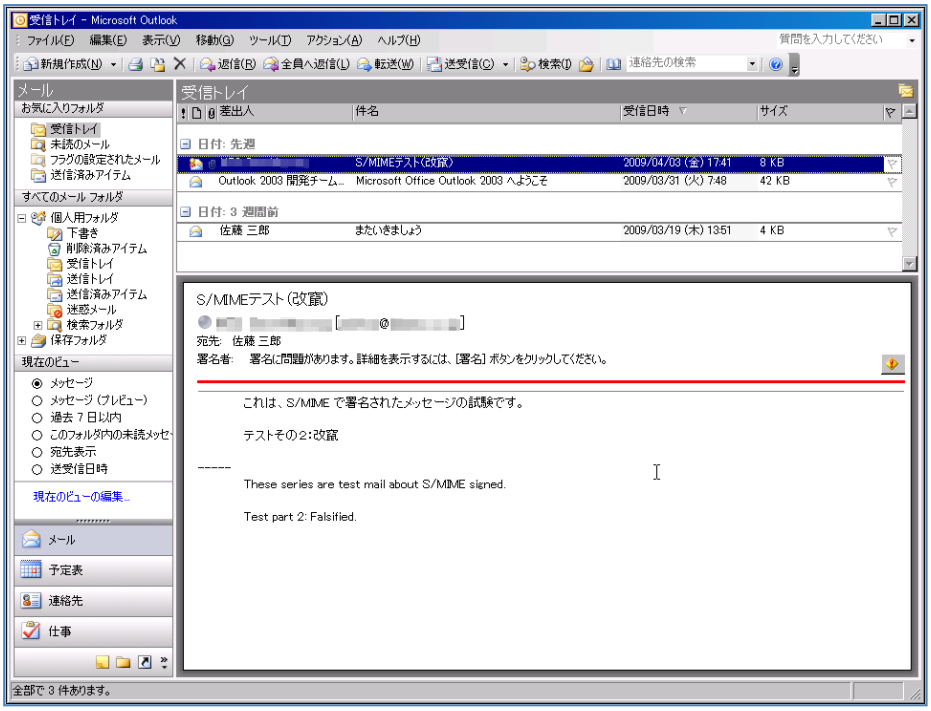
- S/MIME で署名されたメッセージの証明書が検証できない場合
  1. メール本文は表示され、メール本文上部に「赤い線」とアイコンが表示される。



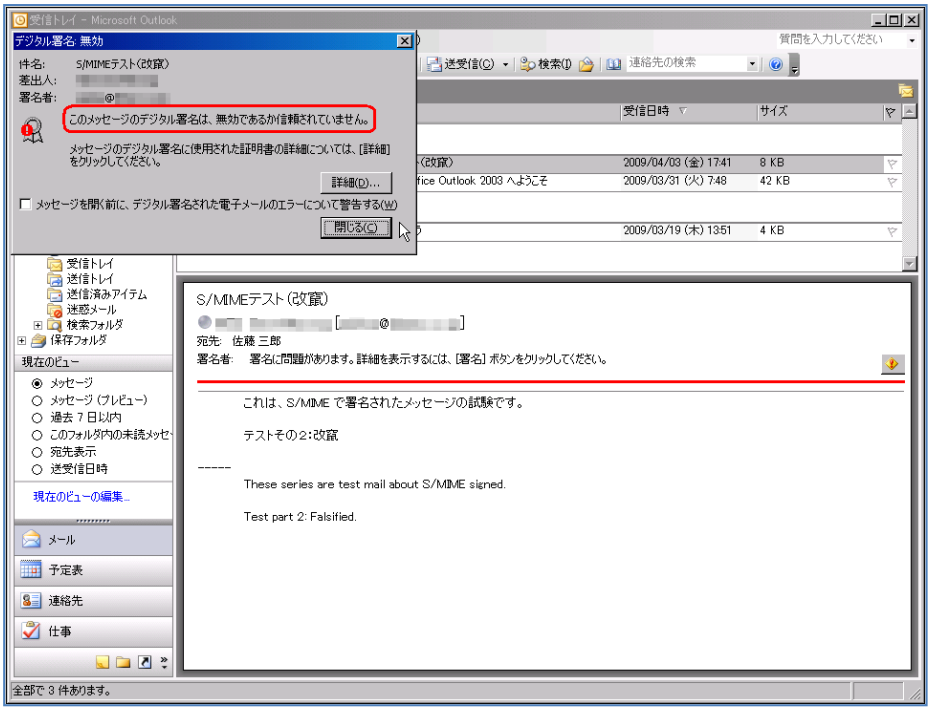
  2. アイコンをクリックすると、「デジタル署名：無効」ウインドウが開く。
     ウインドウ内に「署名を信頼していないか、次の証明書が信頼されていないため、署名が無効です。」と表示される。



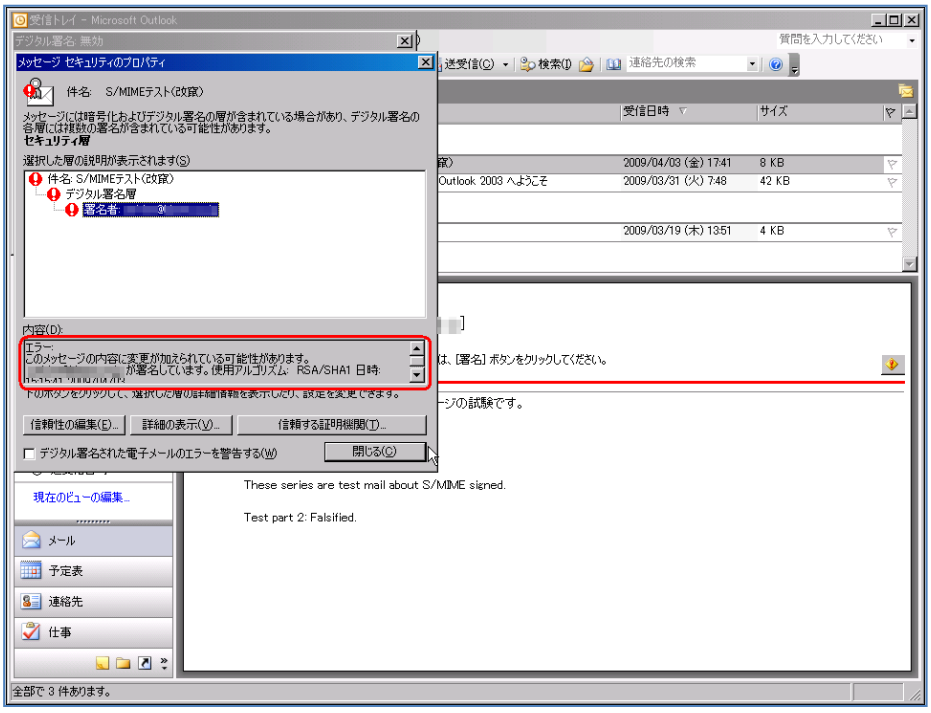
- S/MIME で署名されたメッセージが改竄されている場合
  1. メール本文は表示され、メール本文上部に「赤い線」とアイコンが表示される。



  2. アイコンをクリックすると、「デジタル署名：無効」ウインドウが開く。
     ウインドウ内に「このメッセージのデジタル署名は、無効であるか信頼されていません。」と表示される。



3. 詳細ボタンをクリックすると、「メッセージ セキュリティのプロパティ」ウインドウが開く。
ウインドウ内の「内容」欄に、「メッセージの内容に変更が加えられている可能性があります。」と表示される。

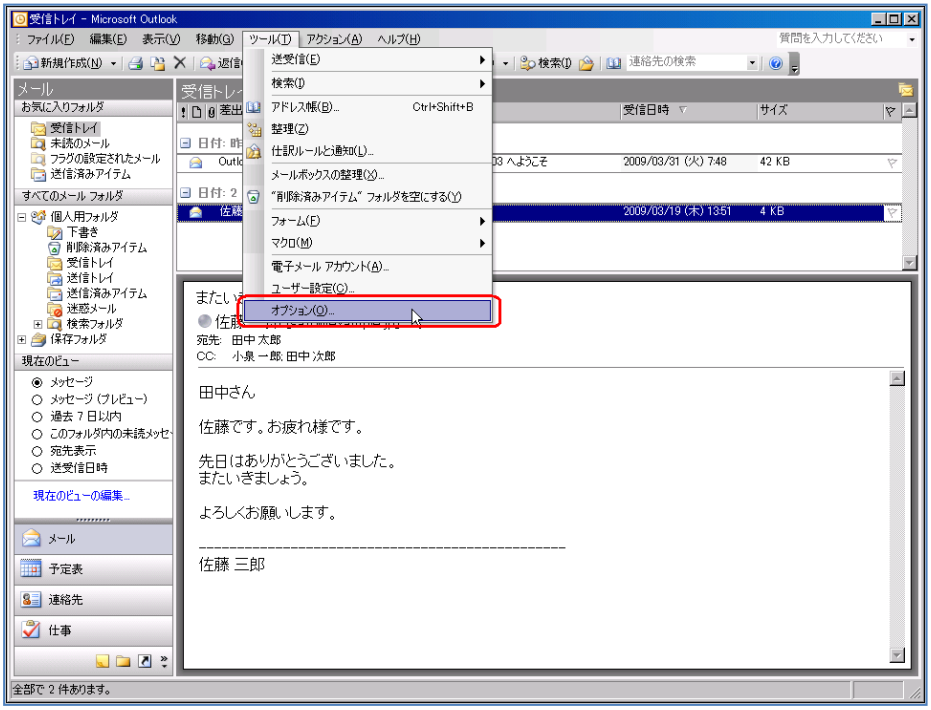


PGP 対応

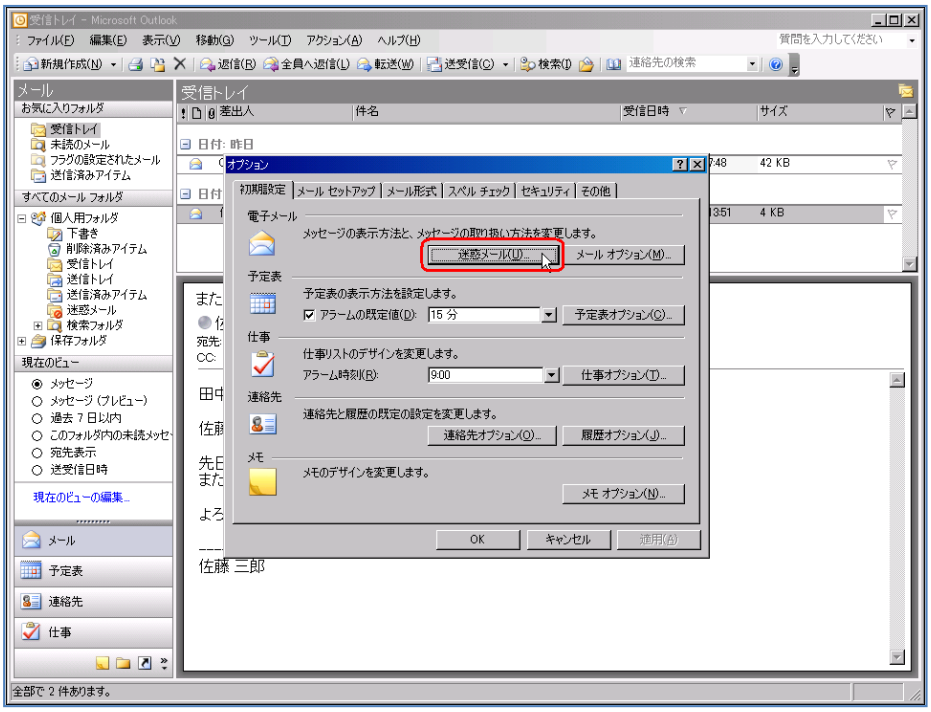
Microsoft Outlook 2003 は、標準で PGP をサポートしていません。

迷惑メールフィルタの設定

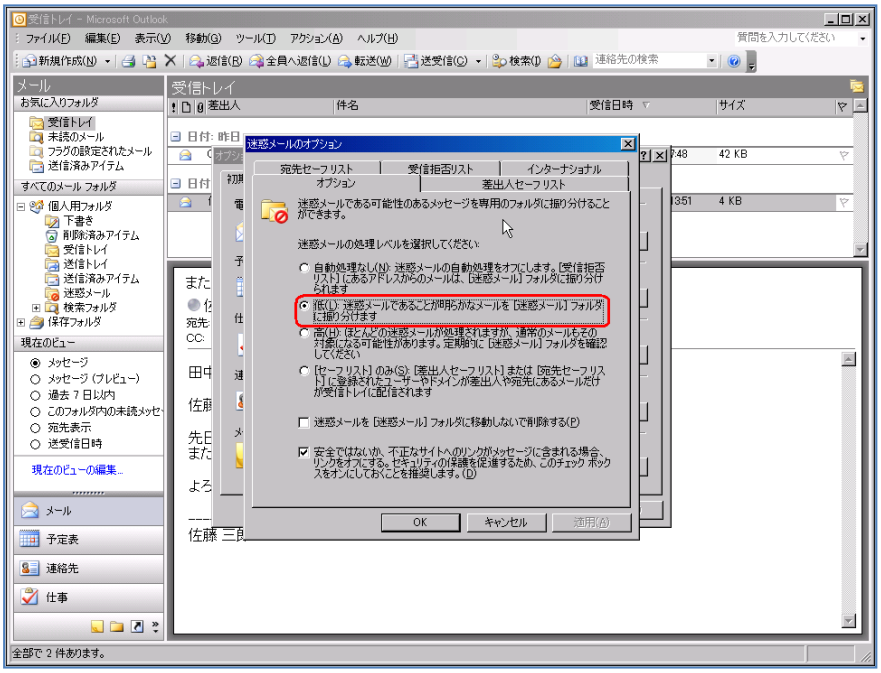
- メニューの「ツール」から「オプション」を選択する。



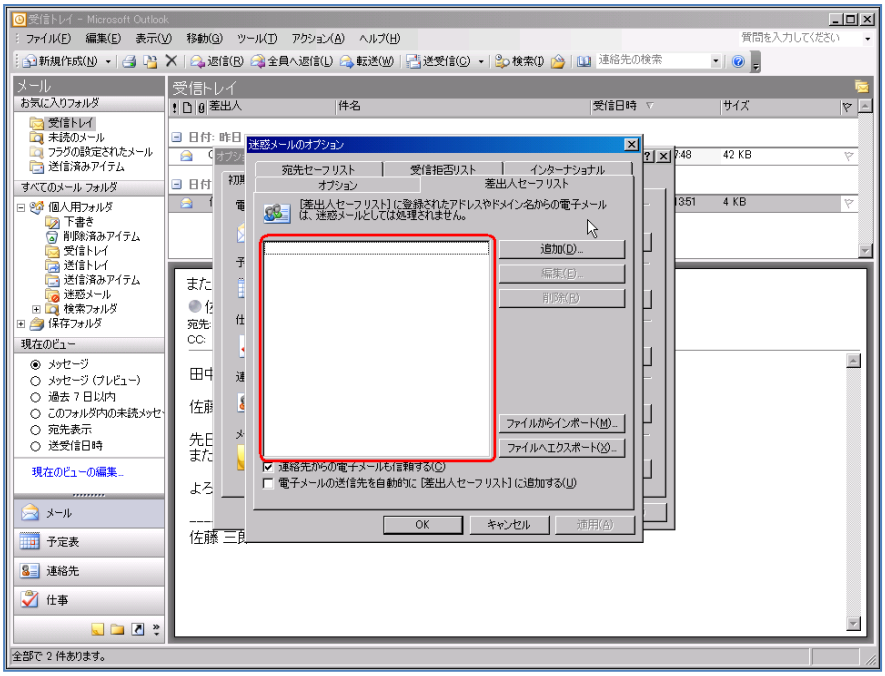
- 「オプション」ウインドウの「初期設定」タブを選択し、「迷惑メール」ボタンを押す。



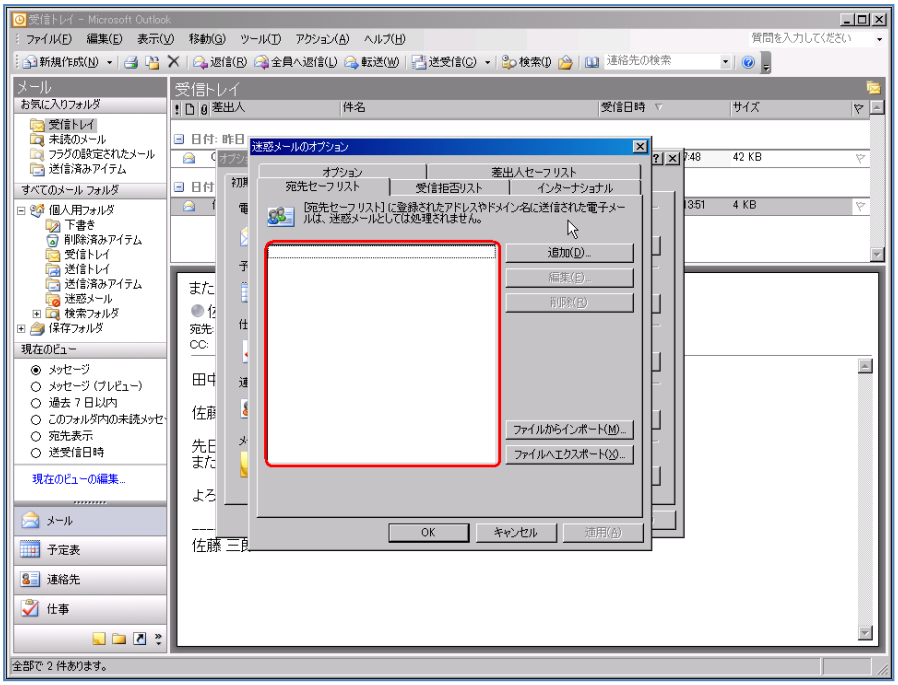
- 「迷惑メール」ウインドウの「オプション」タブを選択する。
必要に応じて、迷惑メールの処理レベルを選択してください。 ここでは、「低：迷惑メールであることが明らかなメールを「迷惑メール」フォルダに振り分けます。」を選択。



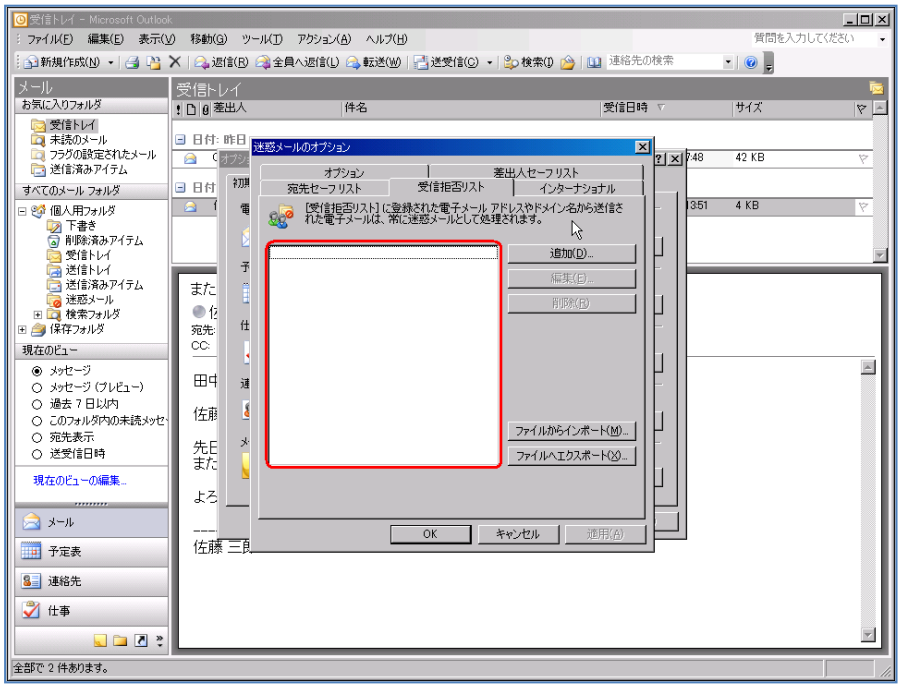
- 「差出人セーフリスト」タブを選択する。
必要に応じて、迷惑メールの処理を行わない差出人メールアドレスを登録して下さい。



- 「宛先セーフリスト」タブを選択する。
  必要に応じて、迷惑メールの処理を行わない宛先メールアドレスを登録して下さい。

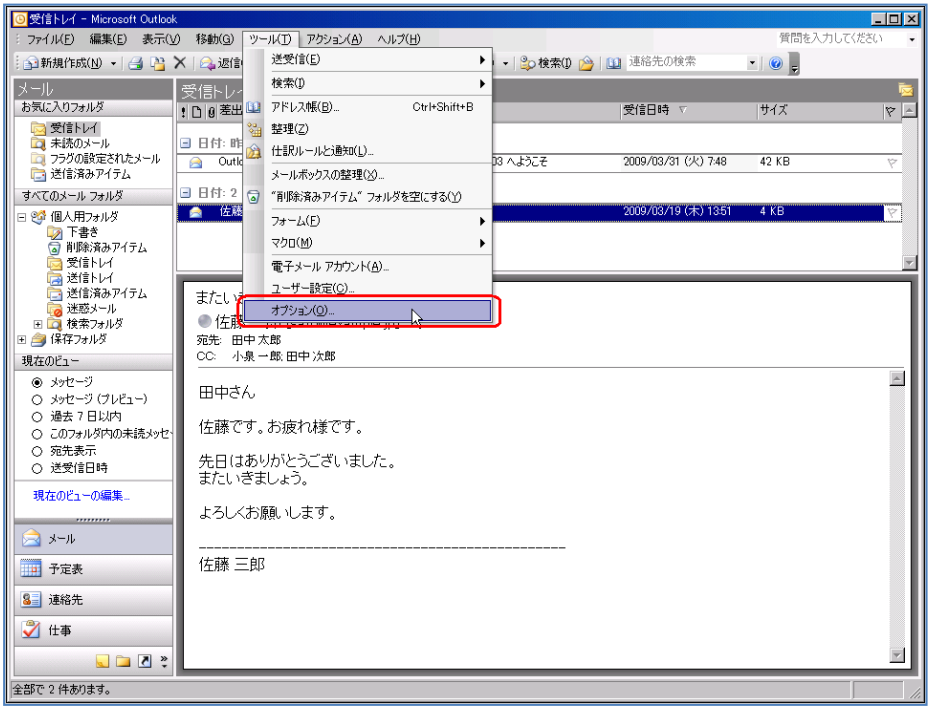


- 「受信拒否リスト」タブを選択する。
  必要に応じて、迷惑メールの処理を行うメールアドレスを登録して下さい。

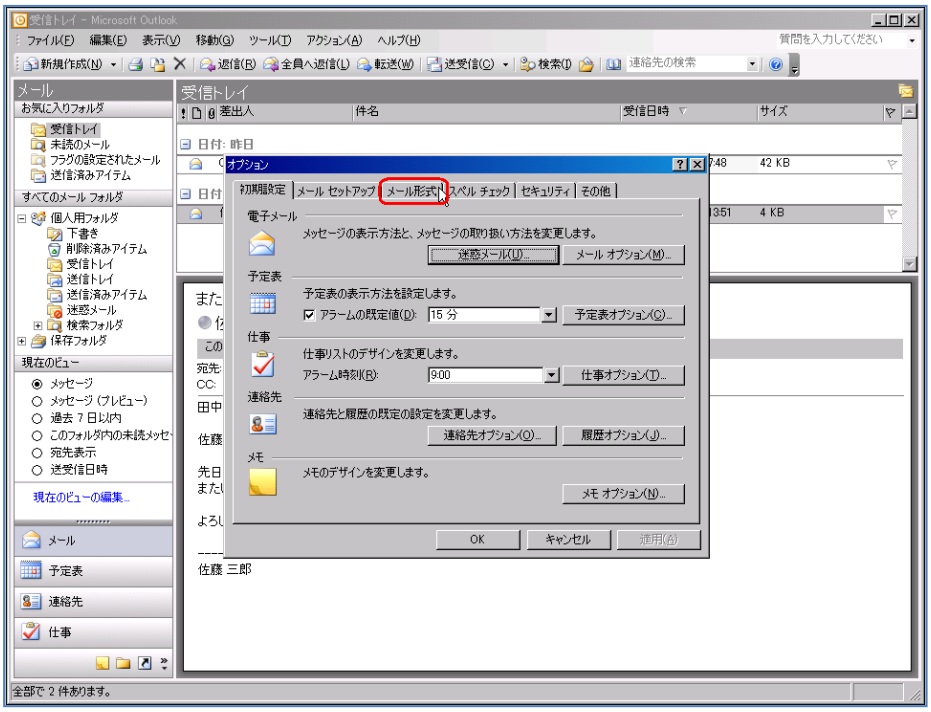


メール送信フォーマットに関する設定

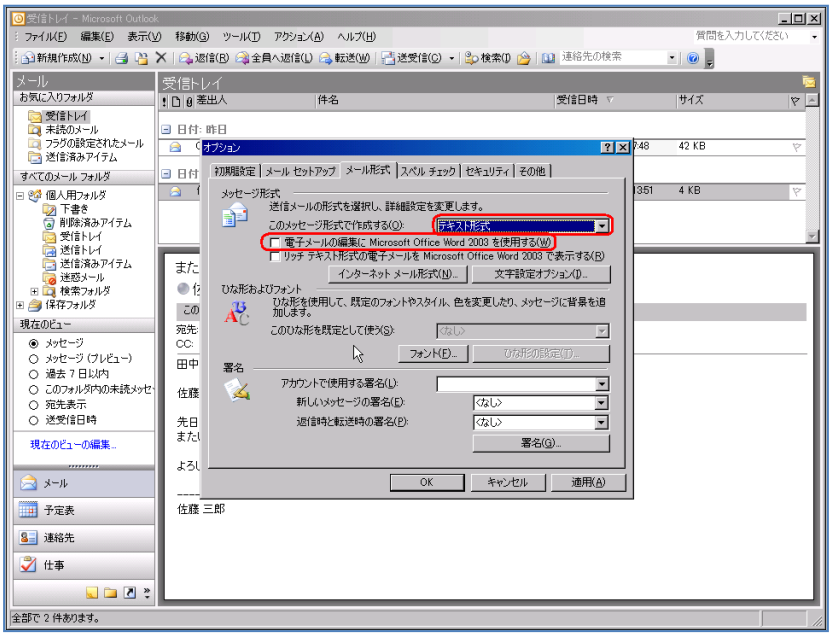
- メニューの「ツール」から「オプション」を選択する。



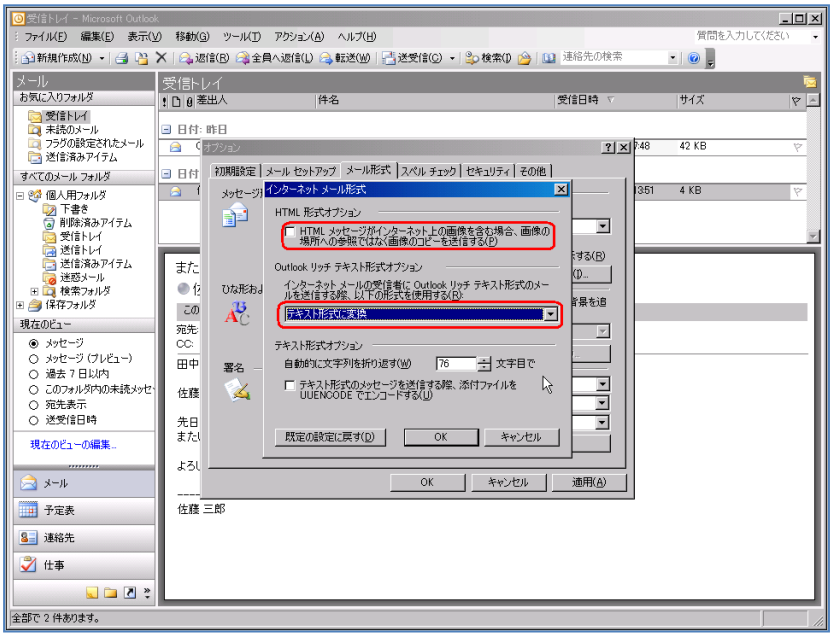
- 「オプション」ウインドウの「メール形式」タブを選択する。



- 「メッセージ形式」内の「このメッセージ形式で作成する」プルダウンメニューから、「テキスト形式」を選択する。
  あわせて、「電子メールの編集に Microsoft Office Word 2003 を使用する」のチェックを外します。

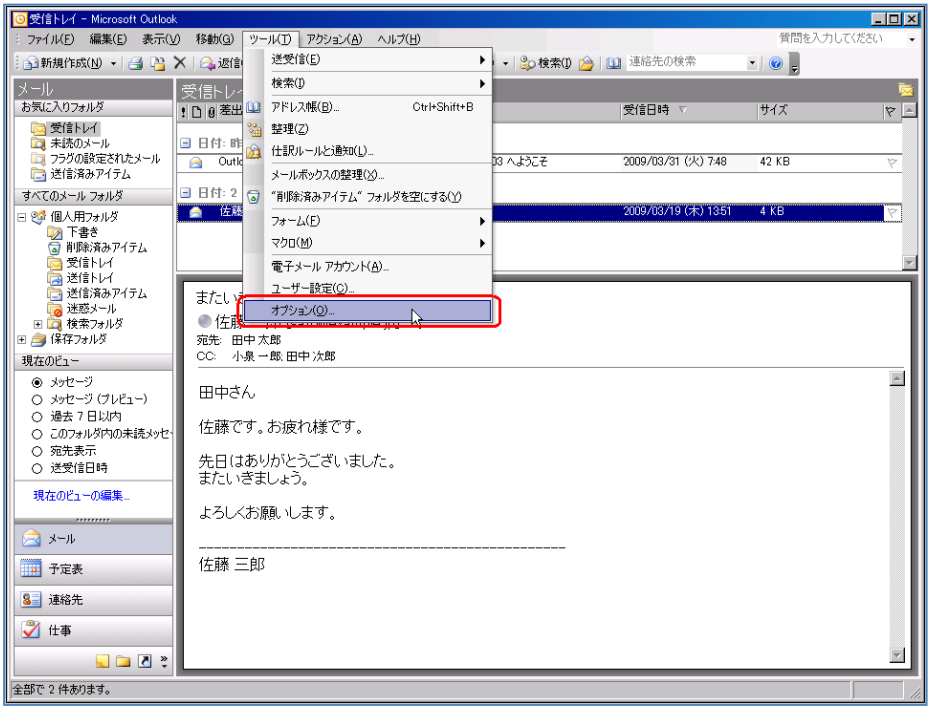


- 「インターネットメール形式」ボタンを押す。
  「HTML 形式オプション」内の「HTML メッセージがインターネット上の画像を含む場合、画像の場所への参照ではなく画像のコピーを送信する」のチェックを外す。
  「Outlook リッチテキスト形式オプション」内のプルダウンメニューから「テキスト形式に変換」を選択する。

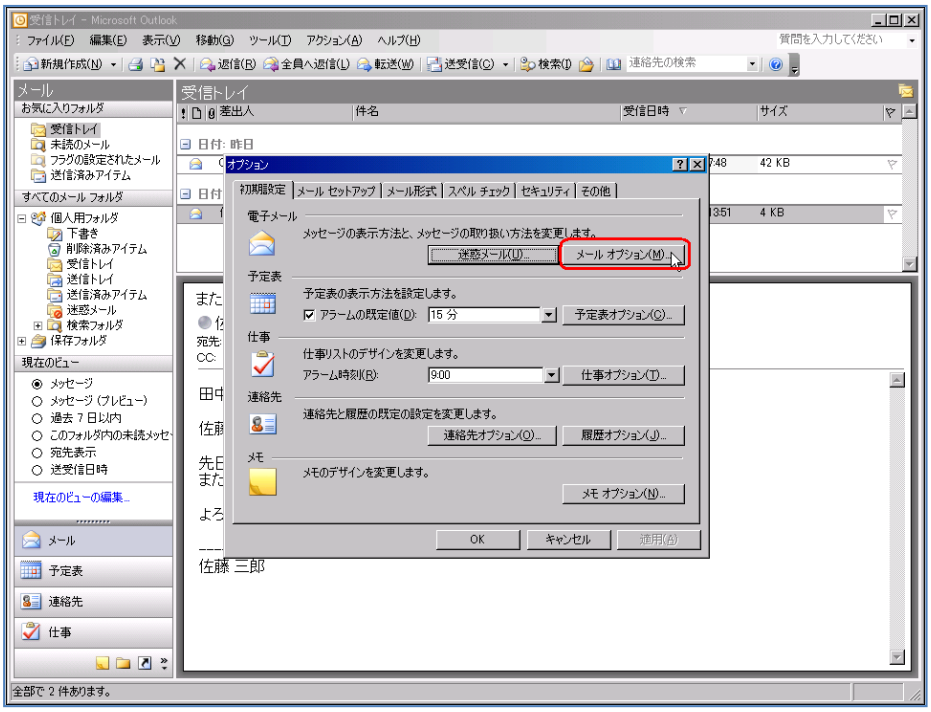


HTML メールの表示に関する設定

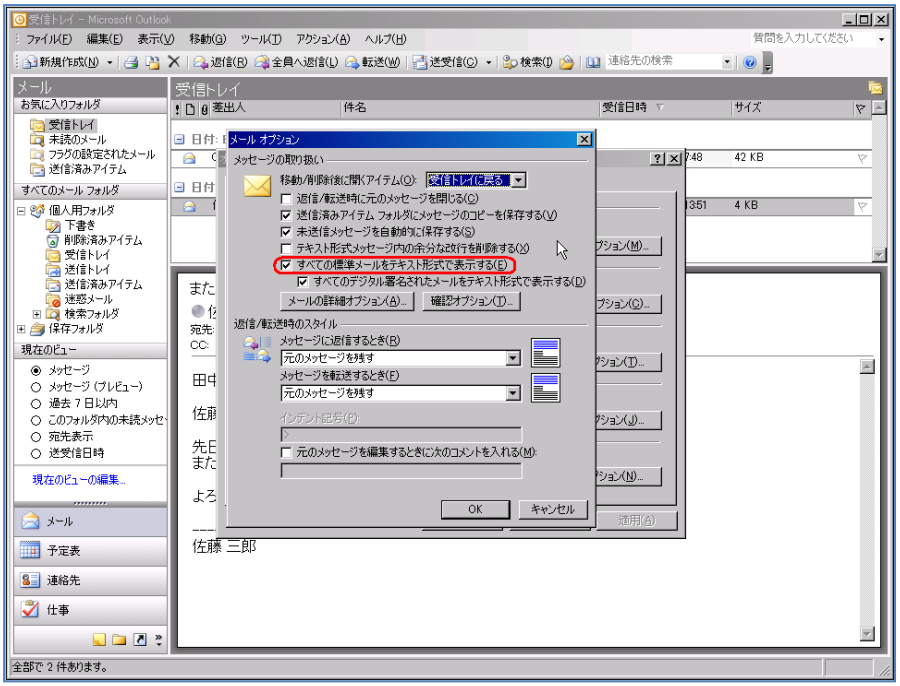
- メニューの「ツール」から「オプション」を選択する。



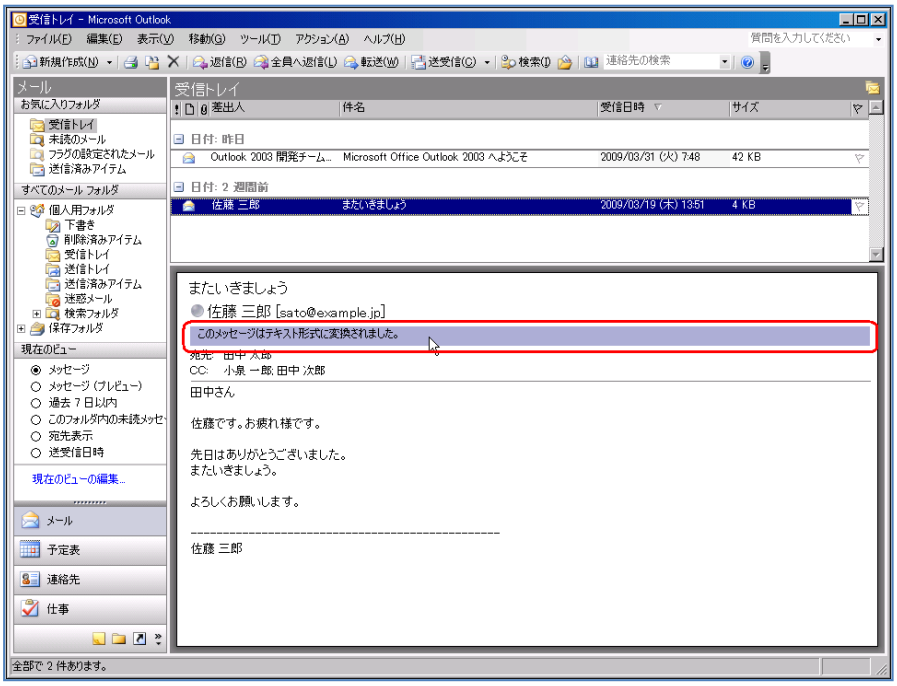
- 「オプション」ウインドウの「初期設定」タブを選択し、「メールオプション」ボタンを押す。



- 「メールオプション」ウインドウ内の「全ての標準メールをテキスト形式で表示する」にチェックする。

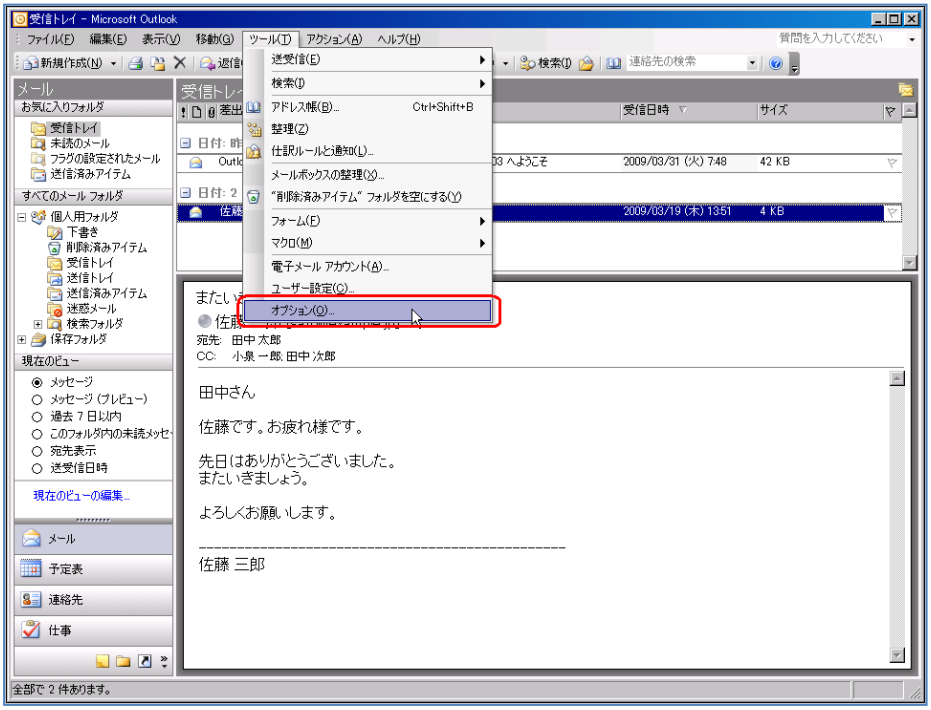


- 「全ての標準メールをテキスト形式で表示する」にチェックした場合、HTML メール等を表示する際、「このメッセージはテキスト形式に変換されました」と表示される。

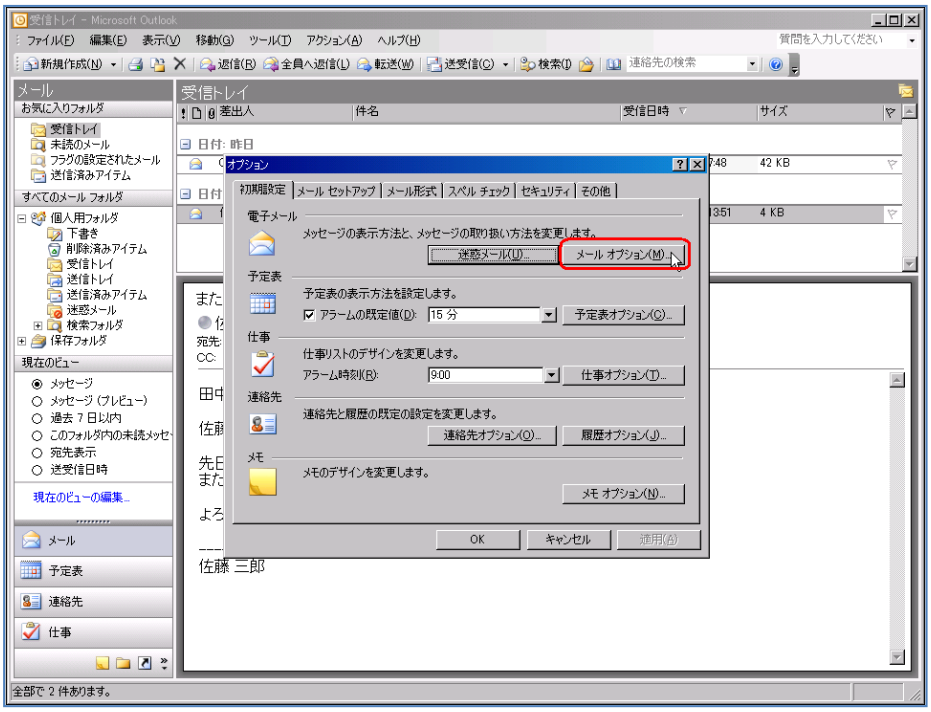


開封確認機能に関する設定

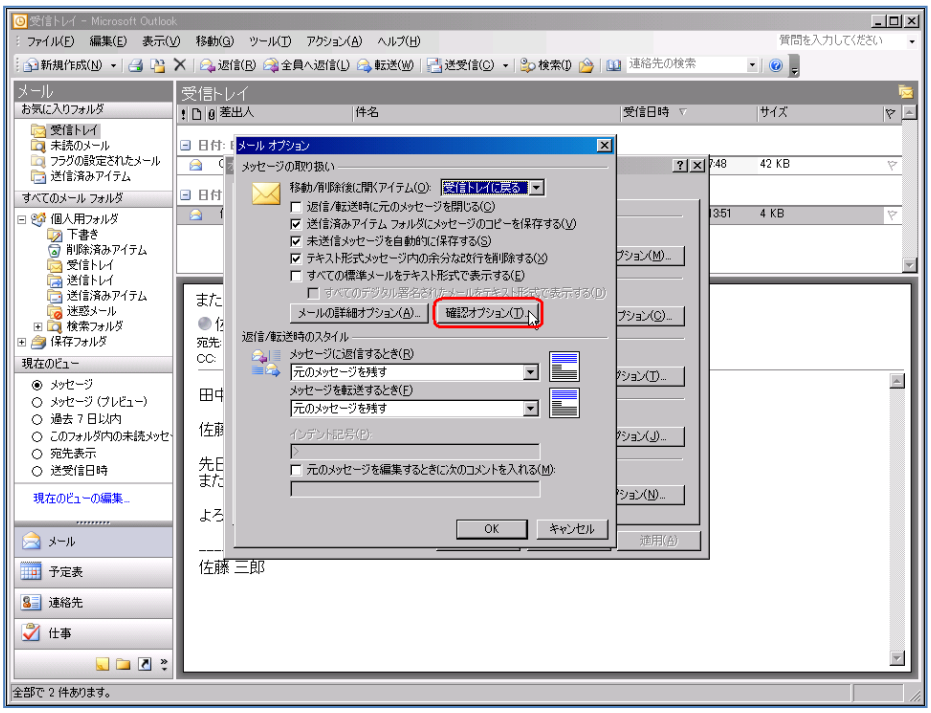
- メニューの「ツール」から「オプション」を選択する。



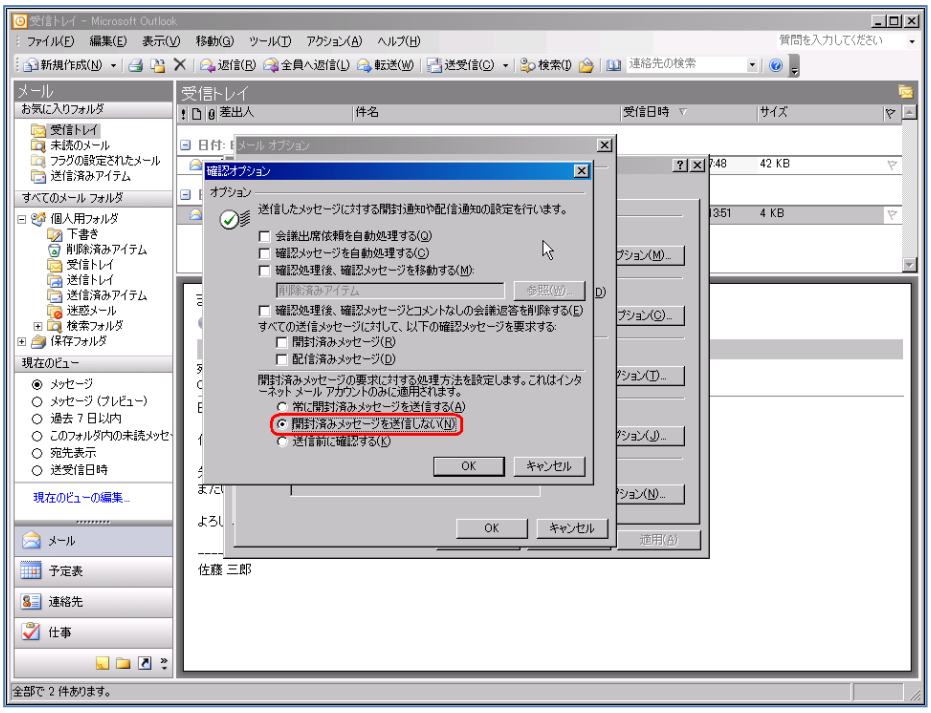
- 「オプション」ウインドウの「初期設定」タブを選択し、「メールオプション」ボタンを押す。



- 「メールオプション」ウインドウの「確認オプション」ボタンを押す。



- 「開封済みメッセージを送信しない」にチェックする。

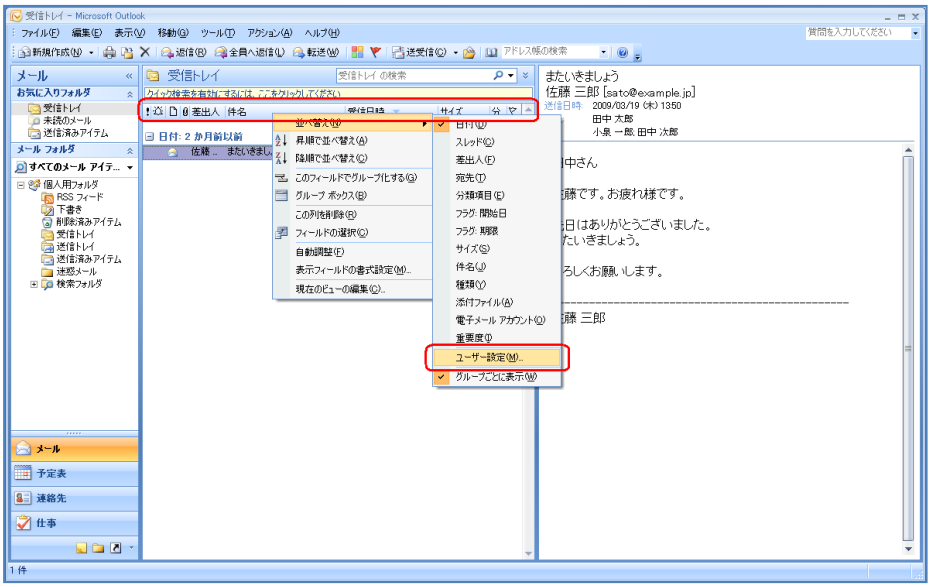


4.5 Outlook 2007 の設定

4.5.1 各設定

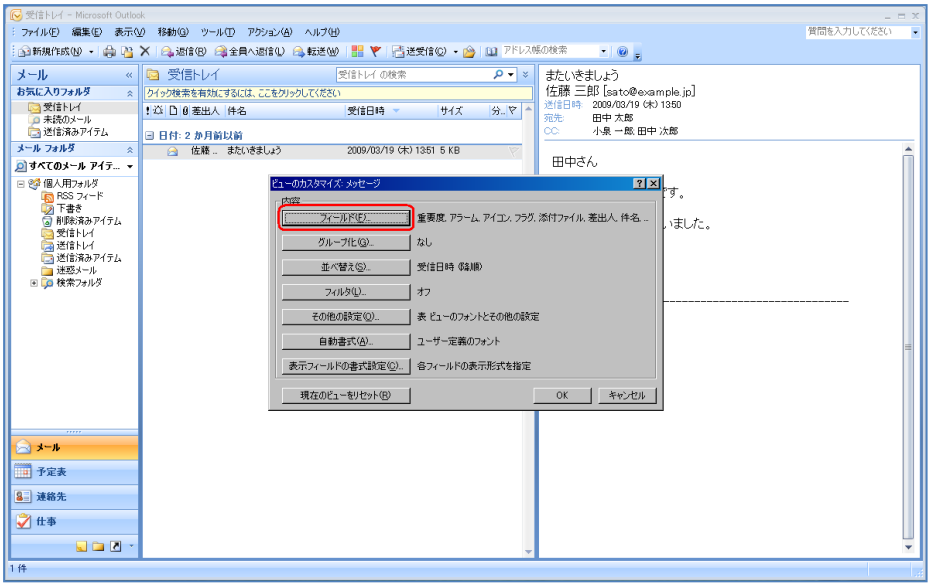
受信メール一覧で表示される情報の拡張

- 表示項目の箇所で右クリックし、「並び替え」から「ユーザ設定」を選択する。



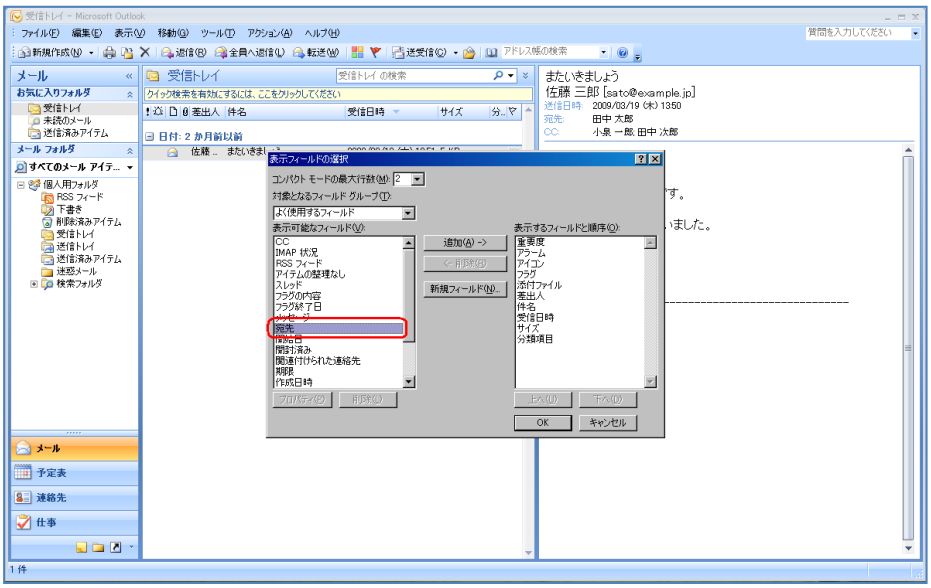
※この画像は Microsoft(R) Office Outlook(R) 2007(12.0.4518.10140) で取得しています。

- 「ビューのカスタマイズ：メッセージ」 ウインドウの「フィールド」ボタンを押す。



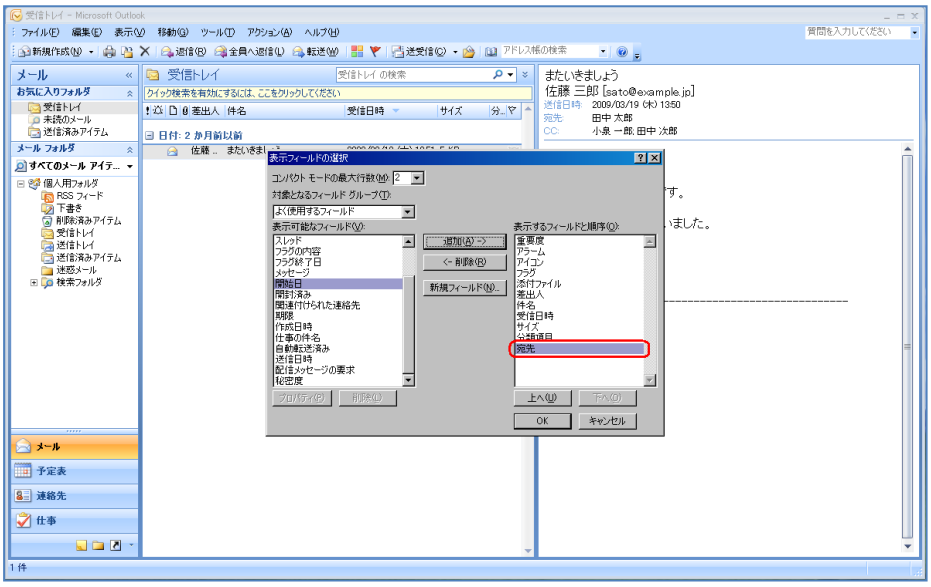
※この画像は Microsoft(R) Office Outlook(R) 2007(12.0.4518.10140) で取得しています。

- 「表示フィールドの選択」ウインドウの「表示可能なフィールド」内の「宛先」を選択する。



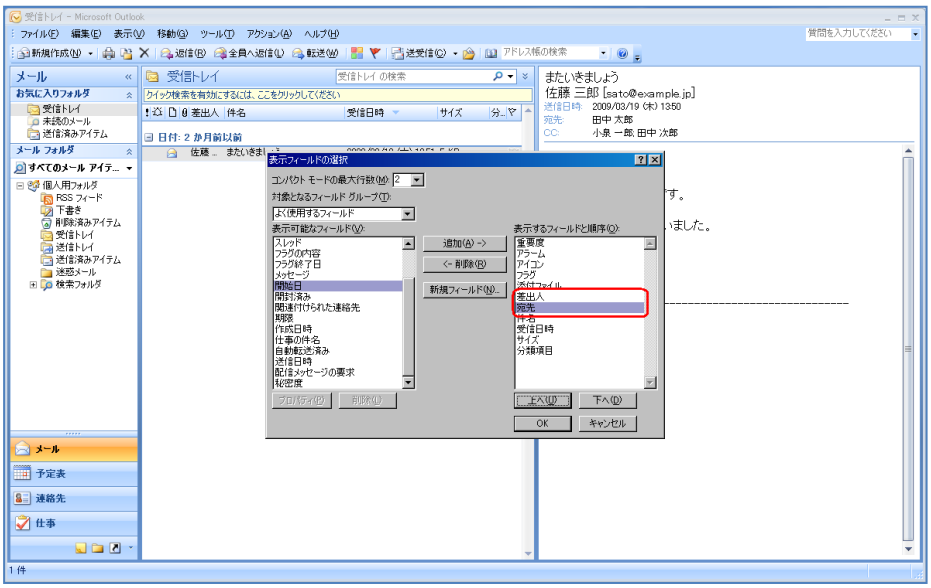
※この画像は Microsoft(R) Office Outlook(R) 2007(12.0.4518.10140) で取得しています。

- 「表示フィールドの選択」ウインドウの「追加」ボタンを押して、「表示するフィールドと順序」に「宛先」を追加する。



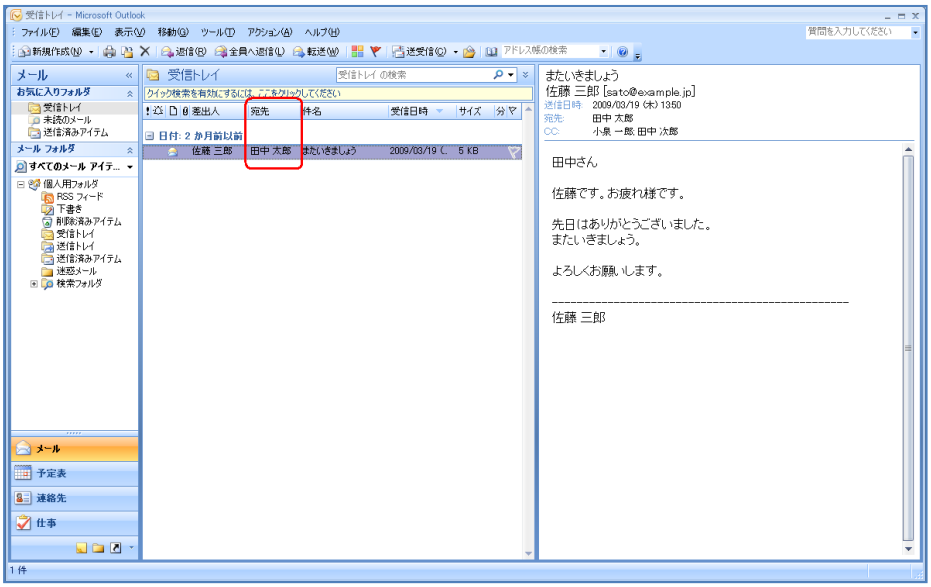
※この画像は Microsoft(R) Office Outlook(R) 2007(12.0.4518.10140) で取得しています。

- 「表示するフィールドと順序」に追加された「宛先」を「差出人」の下部に移動する。



※この画像は Microsoft(R) Office Outlook(R) 2007(12.0.4518.10140) で取得しています。

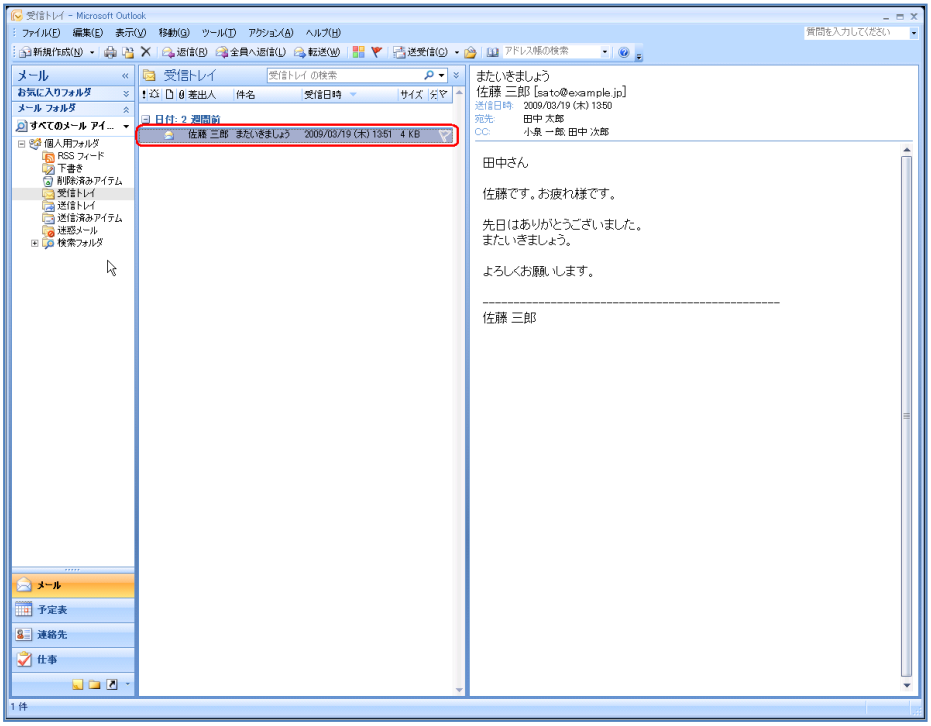
- 表示項目に「宛先」が追加される。



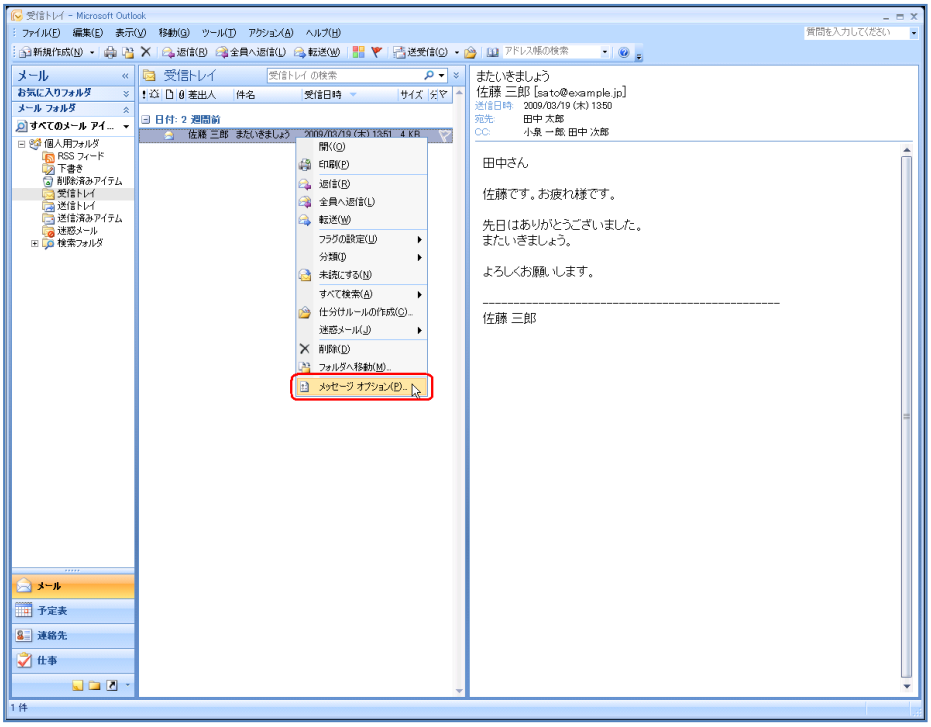
※この画像は Microsoft(R) Office Outlook(R) 2007(12.0.4518.10140) で取得しています。

メールヘッダ情報の確認方法

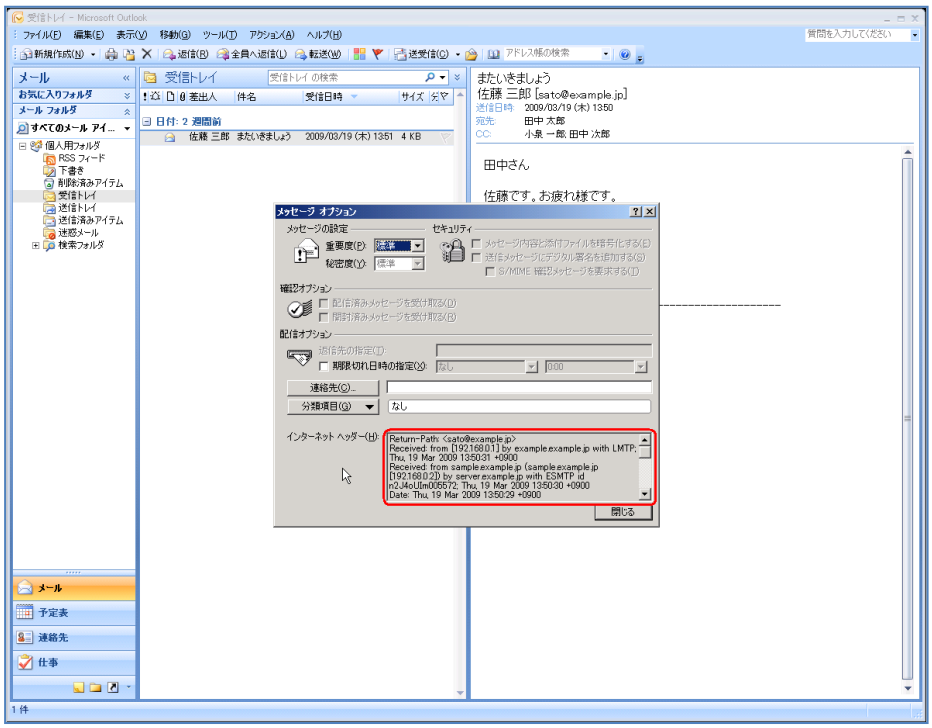
- メールを選択する。



- 右クリックし、「メッセージオプション」を選択する。



- 「メッセージオプション」ウインドウの「インターネットヘッダ」にヘッダ情報が表示される。

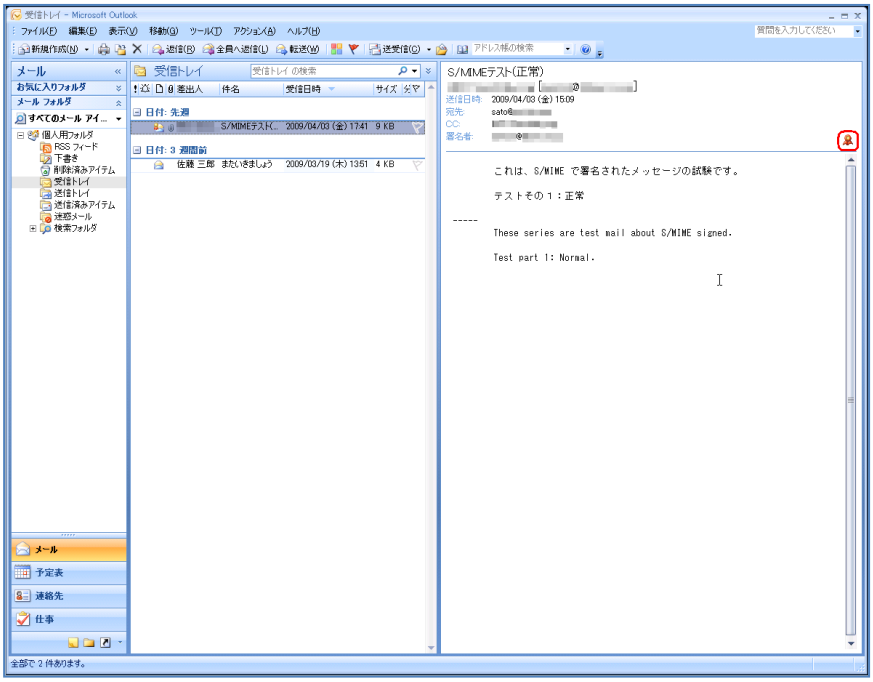


メールアドレスの表示形式の設定

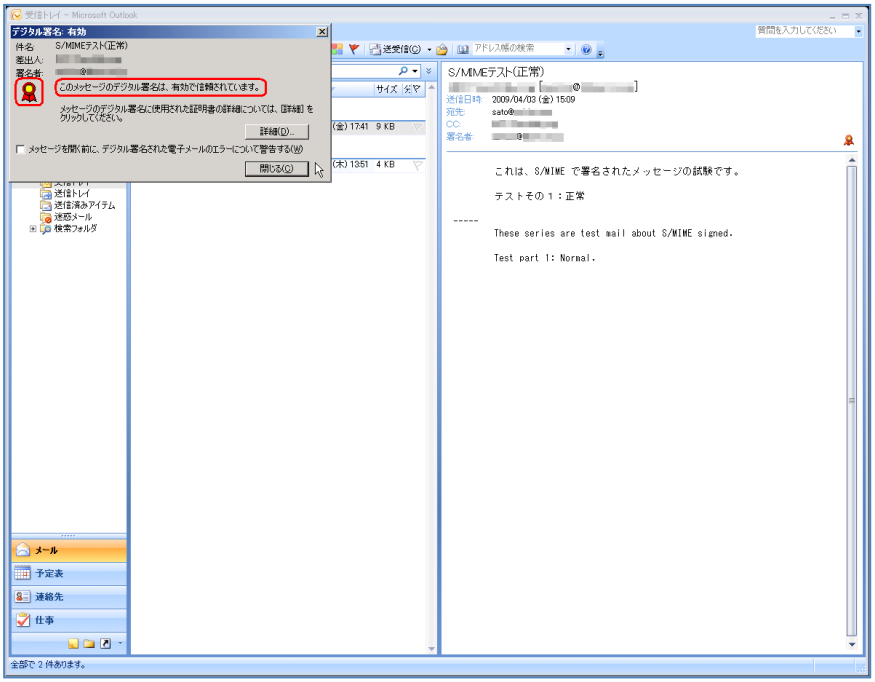
Microsoft Outlook 2007 は、標準で差出人の情報として「表示名」と「メールアドレス」の両方を表示します。特別な設定は必要ありません。

S/MIME による署名メールの表示例

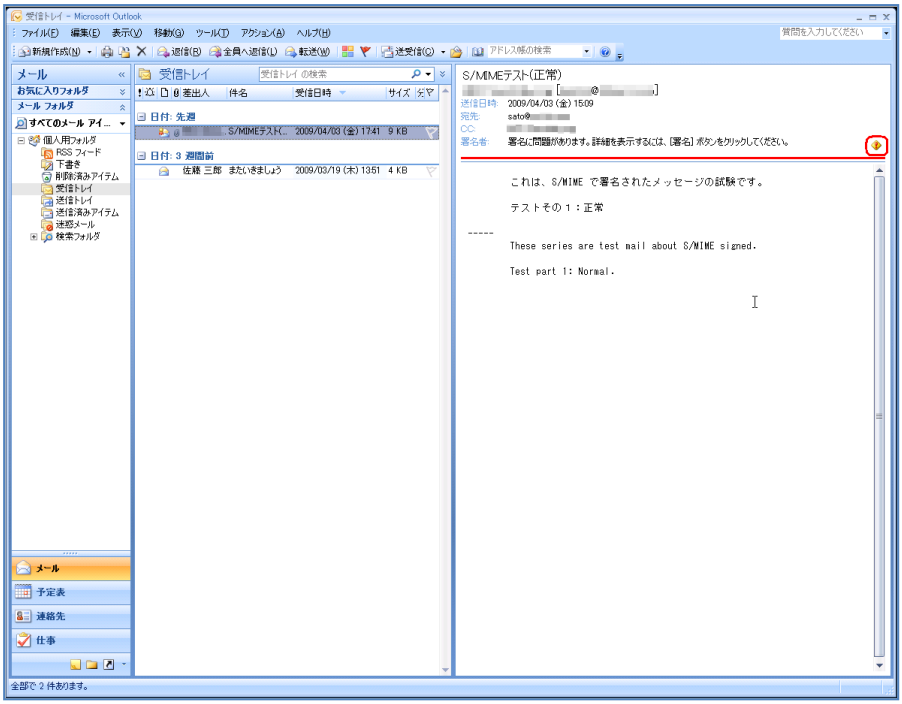
- S/MIME で署名されたメッセージが問題なく検証された場合
  1. メール本文は表示され、ウインドウの右上にアイコンが表示される。



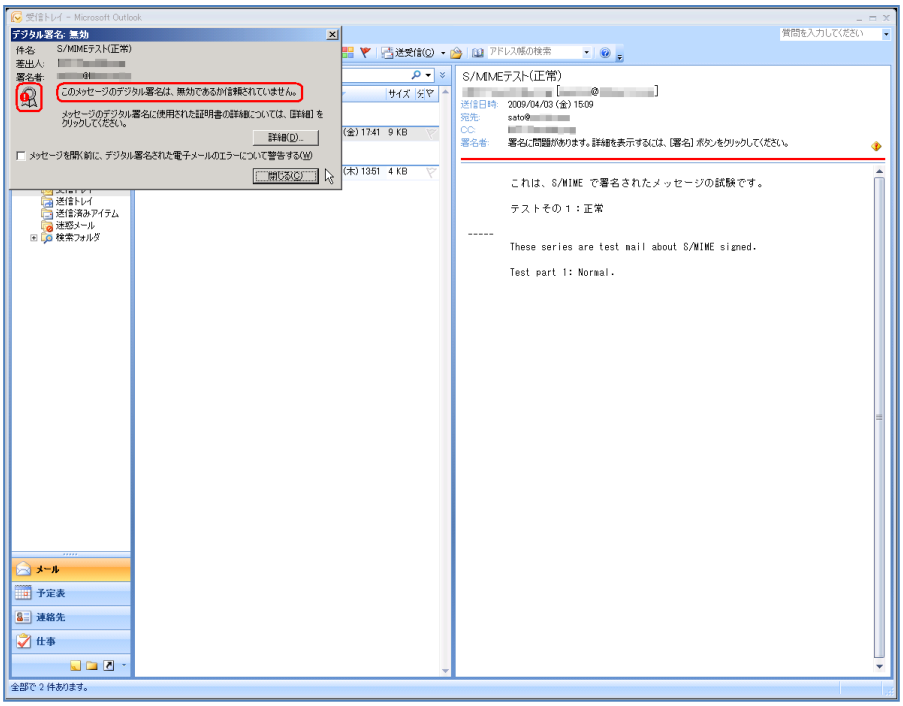
  2. アイコンをクリックすると、「デジタル署名：有効」ウインドウが開く。
     ウインドウ内に「このメッセージのデジタル署名は、有効で信頼されています。」と表示される。



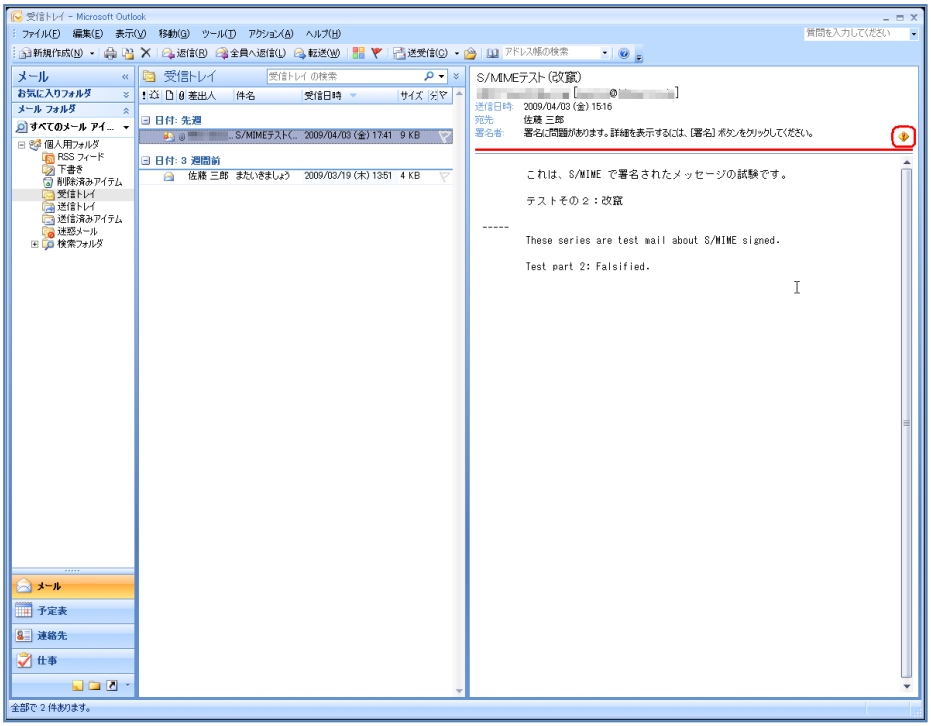
- S/MIME で署名されたメッセージの証明書が検証できない場合
  1. メール本文は表示され、メール本文上部に「赤い線」とアイコンが表示される。



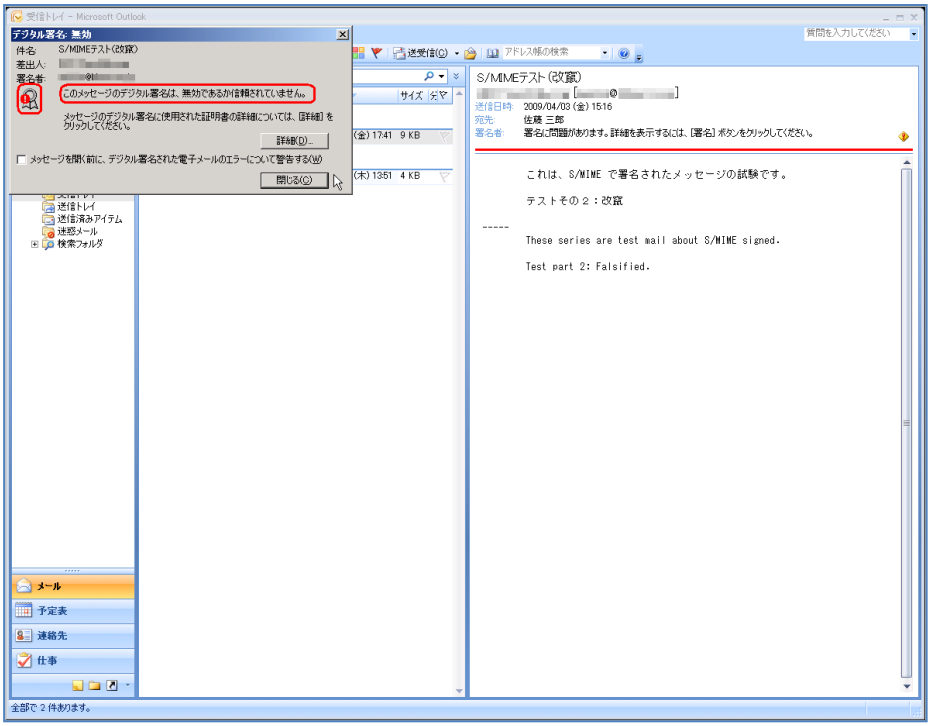
  2. アイコンをクリックすると、「デジタル署名：無効」ウインドウが開く。
     ウインドウ内に「このメッセージのデジタル署名は、無効であるか信頼されていません。」と表示される。



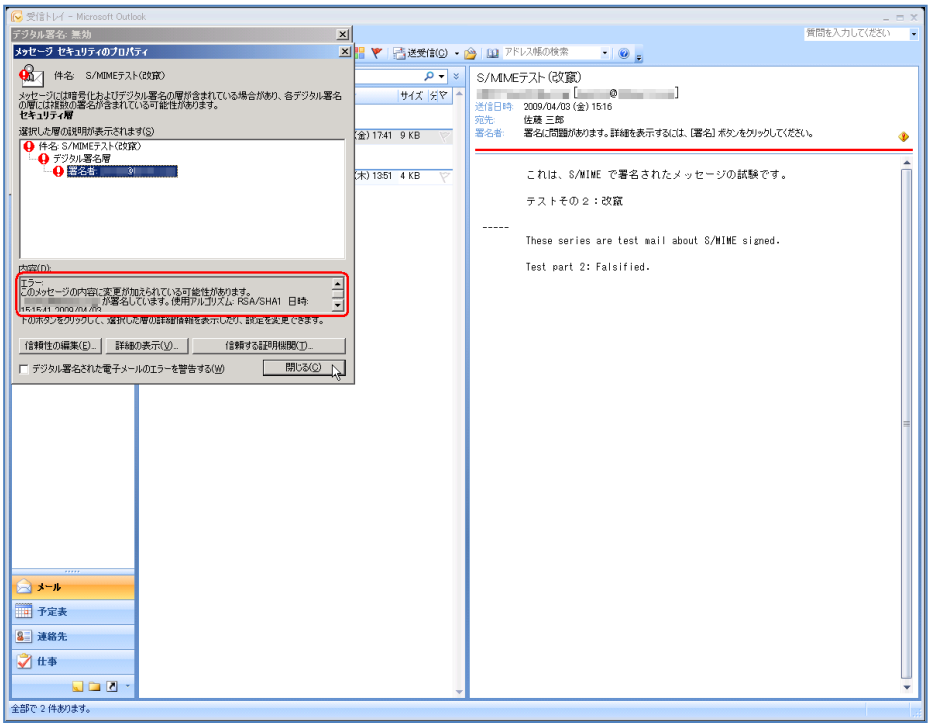
- S/MIME で署名されたメッセージが改ざんされている場合
  1. メール本文は表示され、メール本文上部に「赤い線」とアイコンが表示される。



  2. アイコンをクリックすると、「デジタル署名：無効」ウインドウが開く。
     ウインドウ内に「このメッセージのデジタル署名は、無効であるか信頼されていません。」と表示される。



3. 詳細ボタンをクリックすると、「メッセージ セキュリティのプロパティ」ウインドウが開く。
ウインドウ内の「内容」欄に、「メッセージの内容に変更が加えられている可能性があります。」と表示される。

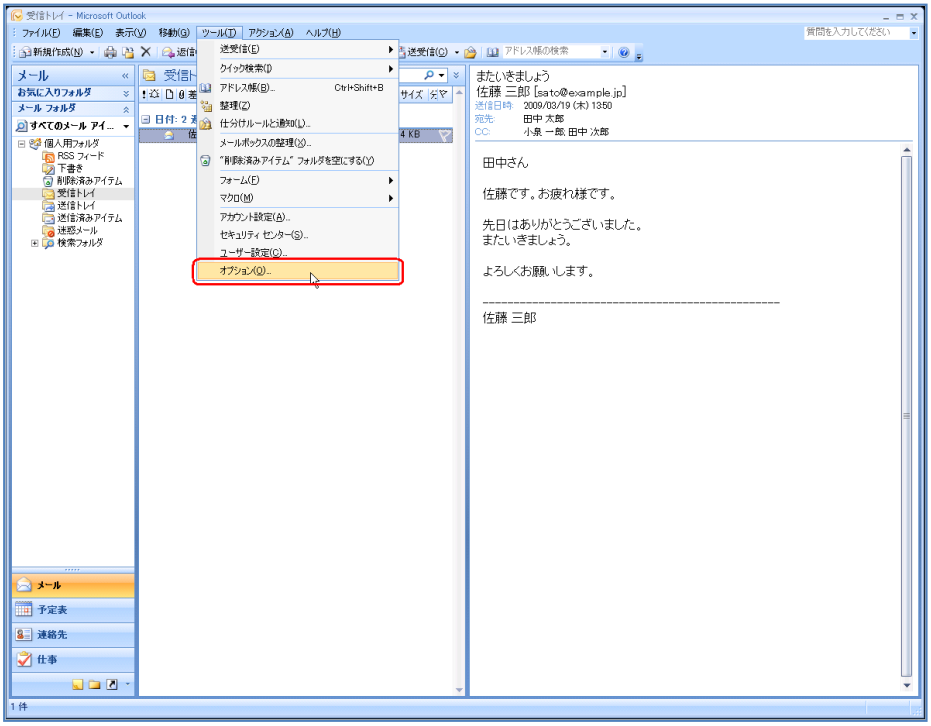


PGP 対応

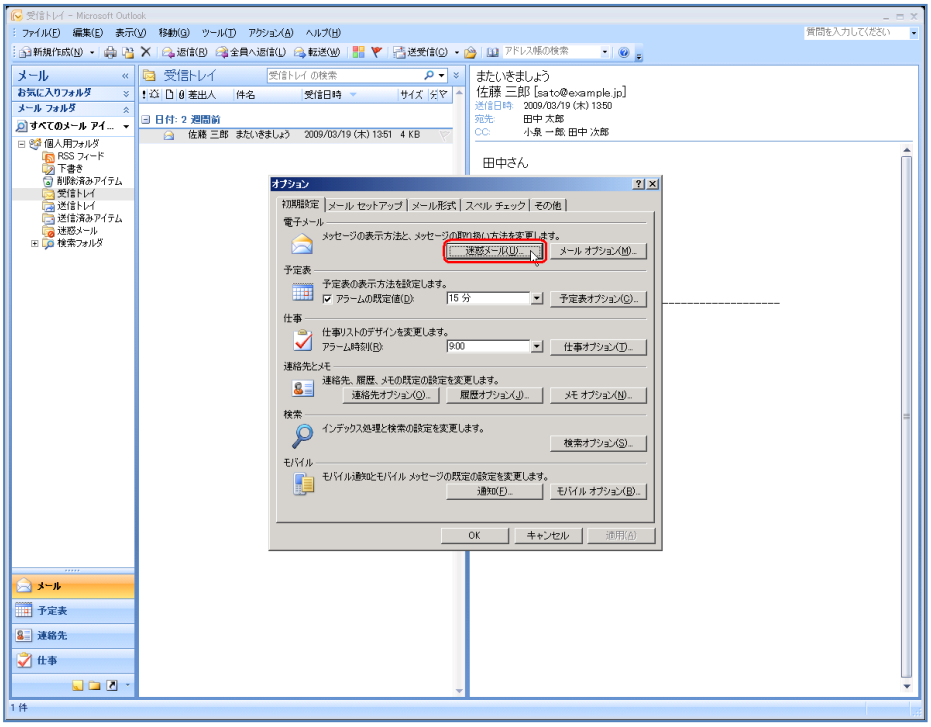
Microsoft Outlook 2007 は、標準で PGP をサポートしていません。

迷惑メールフィルタの設定

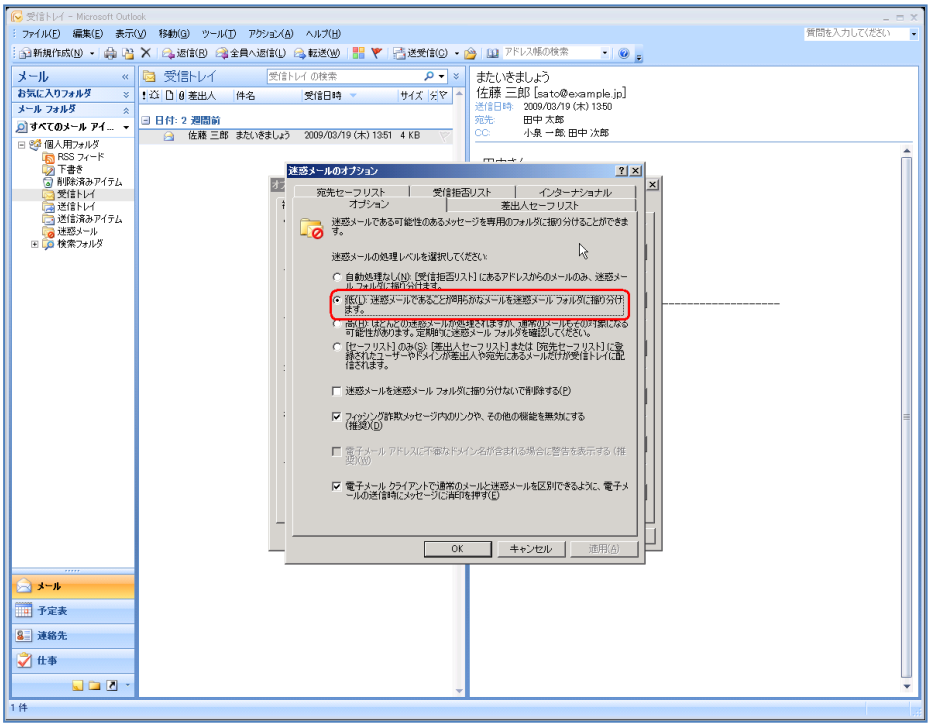
- メニューの「ツール」から「オプション」を選択する。



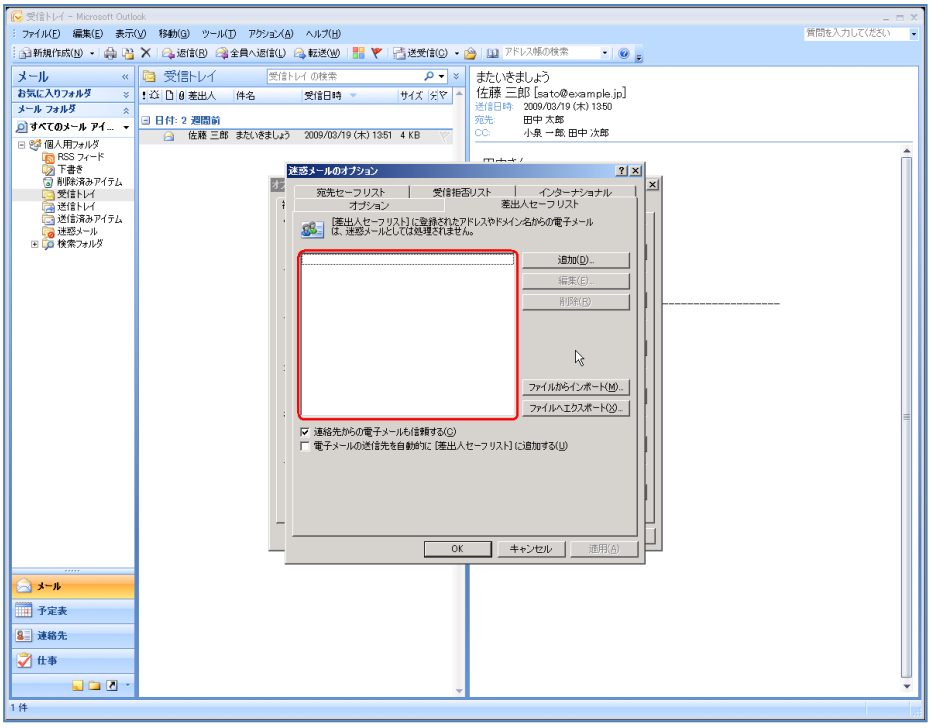
- 「オプション」ウインドウの「初期設定」タブを選択し、「迷惑メール」ボタンを押す。



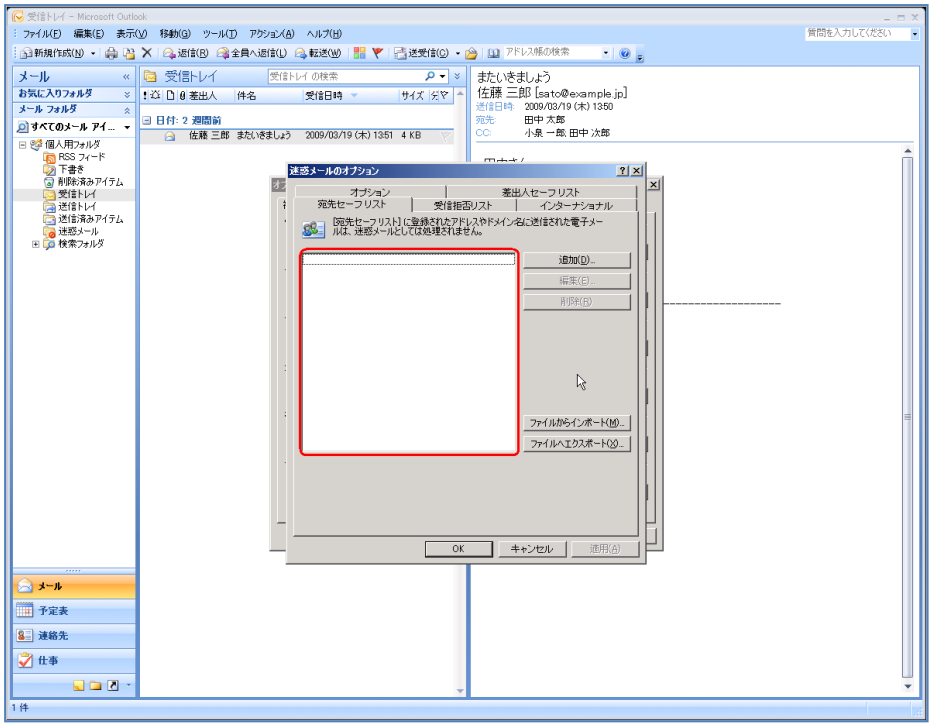
- 「迷惑メール」ウインドウの「オプション」タブを選択する。
必要に応じて、迷惑メールの処理レベルを選択してください。ここでは、「低：迷惑メールであることが明らかなメールを「迷惑メール」フォルダに振り分けます。」を選択。



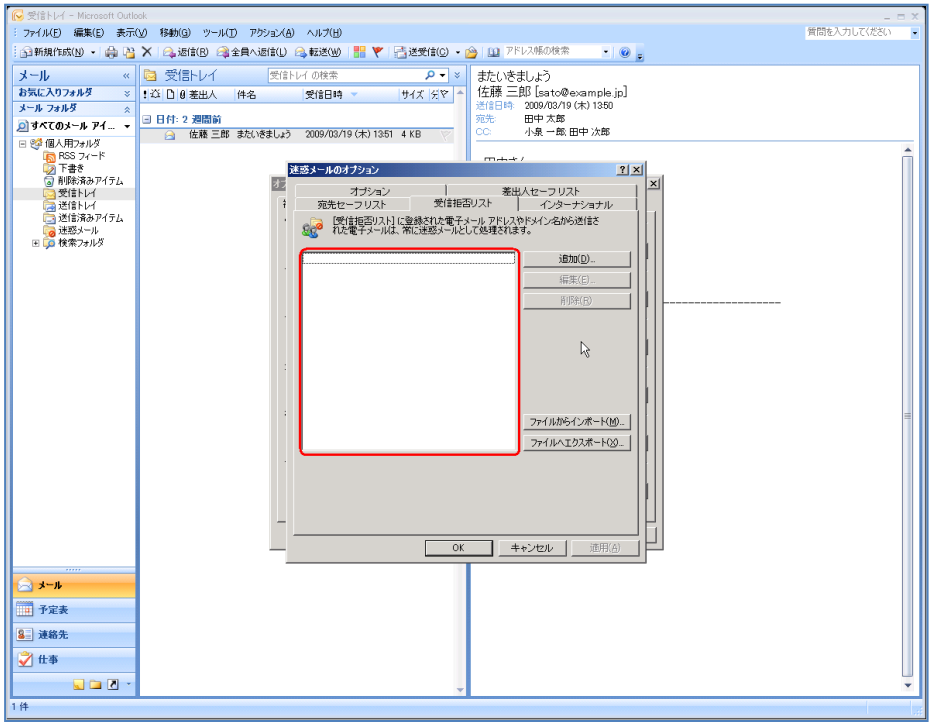
- 「差出人セーフリスト」タブを選択する。
必要に応じて、迷惑メール処理を行わない差出人メールアドレスを登録して下さい。



- 「宛先セーフリスト」タブを選択する。
必要に応じて、迷惑メール処理を行わない宛先メールアドレスを登録して下さい。

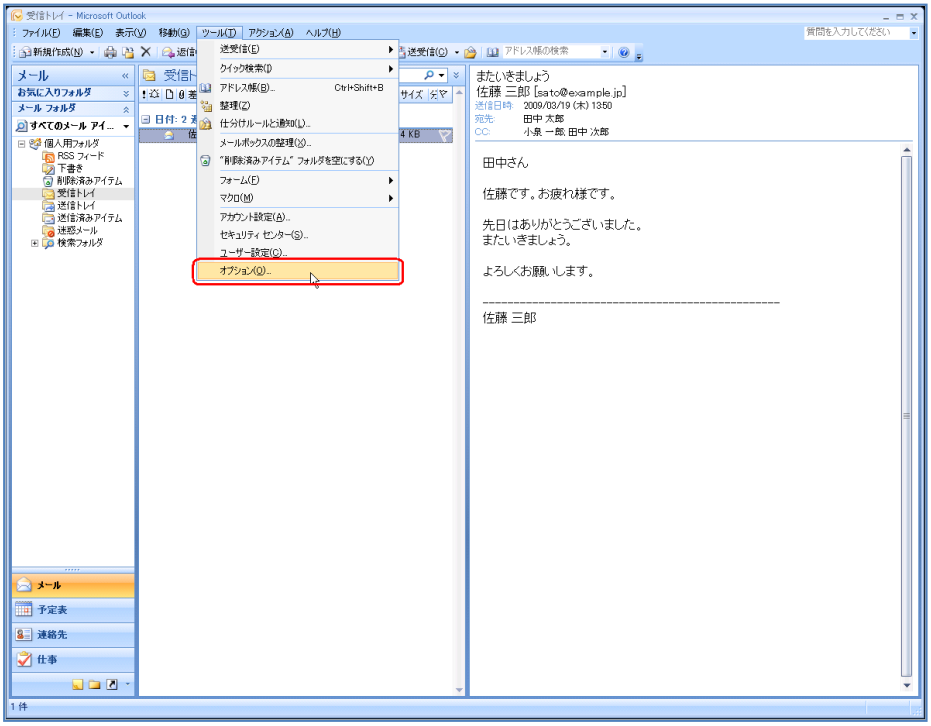


- 「受信拒否リスト」タブを選択する。
必要に応じて、迷惑メール処理を行うメールアドレスを登録して下さい。

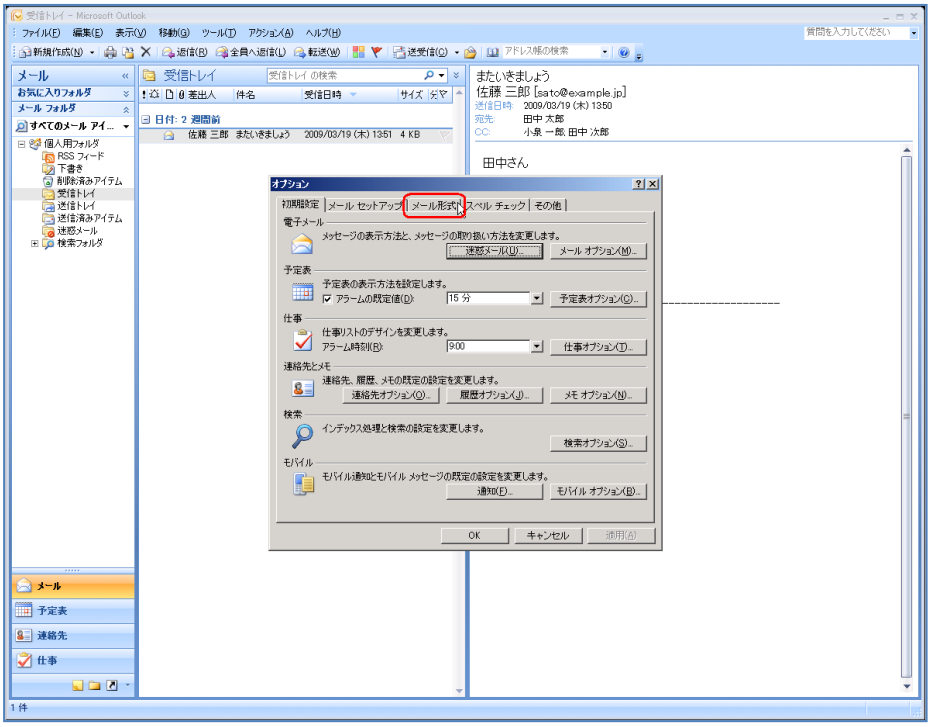


メール送信フォーマットに関する設定

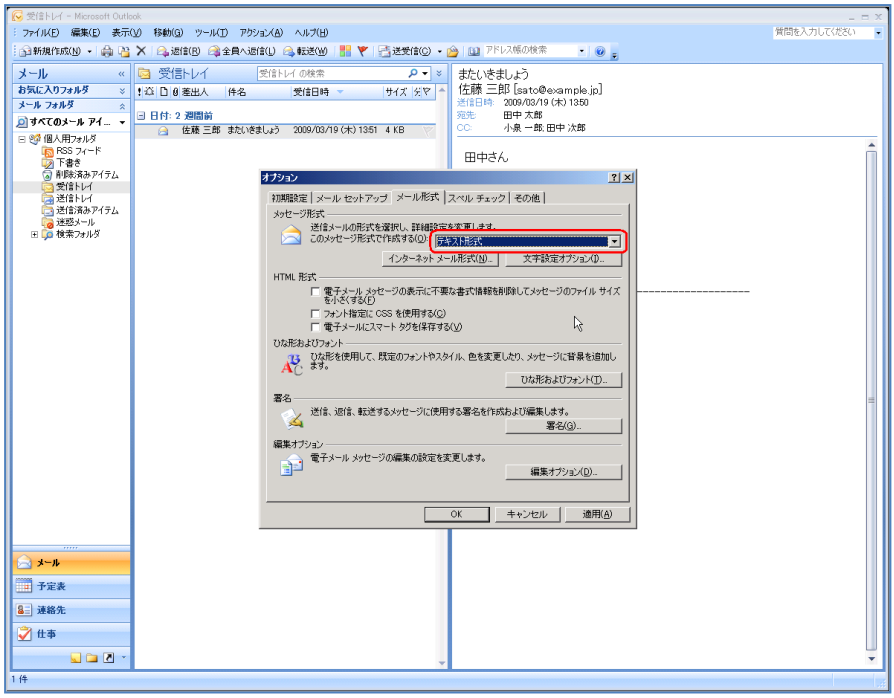
- メニューの「ツール」から「オプション」を選択する。



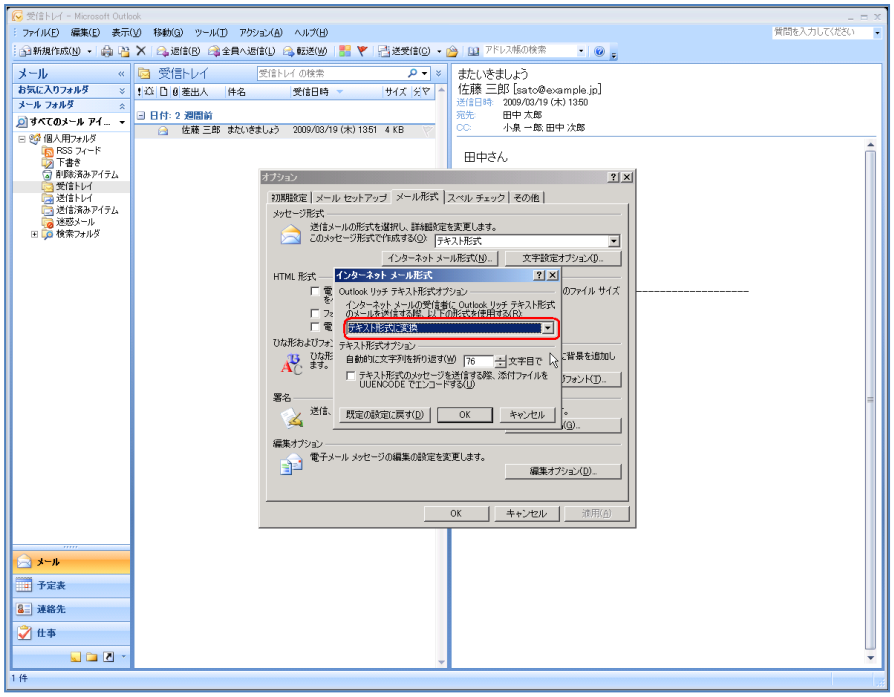
- 「オプション」ウインドウの「メール形式」タブを選択する。



- 「メッセージ形式」内の「このメッセージ形式で作成する」プルダウンメニューから、「テキスト形式」を選択する。

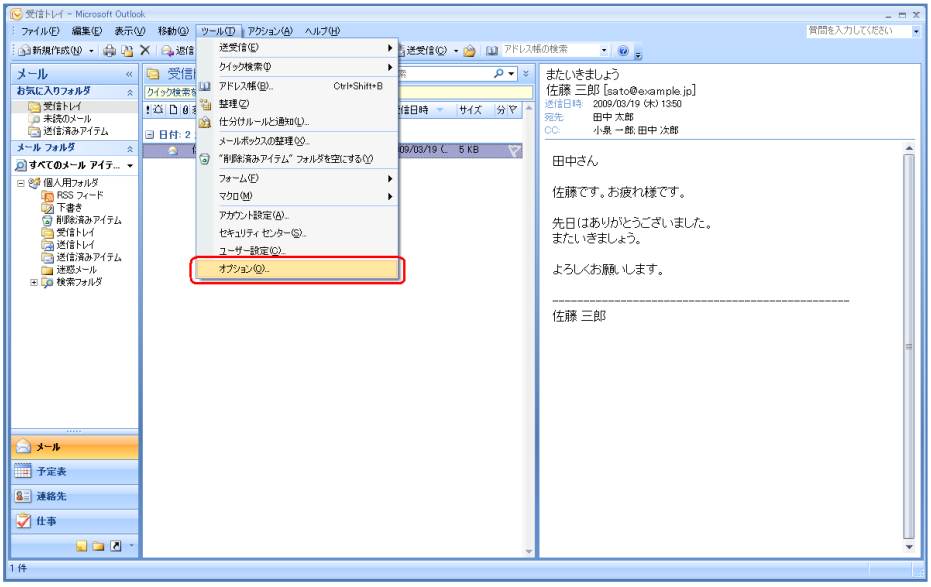


- 「インターネットメール形式」ボタンを押す。
「Outlook リッチテキスト形式オプション」内のプルダウンメニューから「テキスト形式に変換」を選択する。



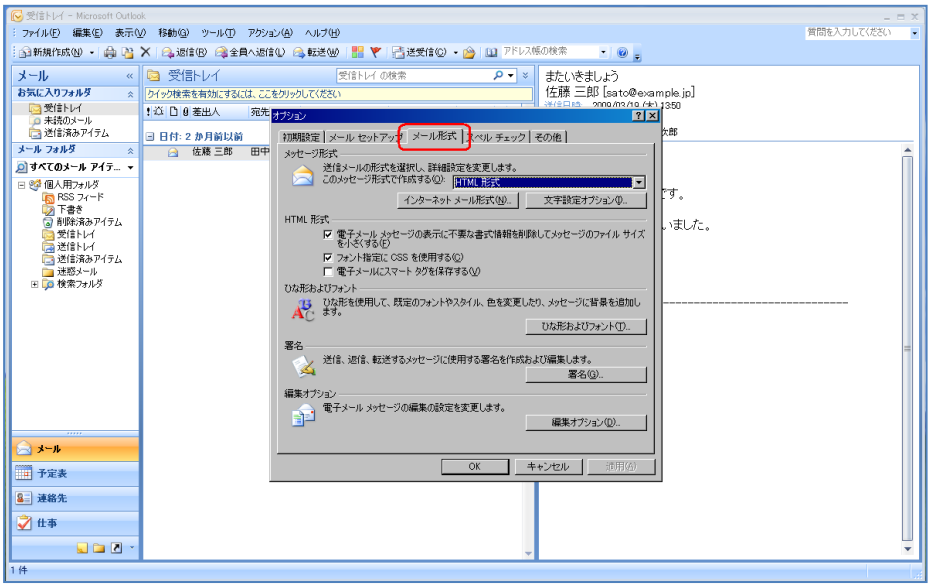
HTML メールの表示に関する設定

- メニューの「ツール」から「オプション」を選択する。



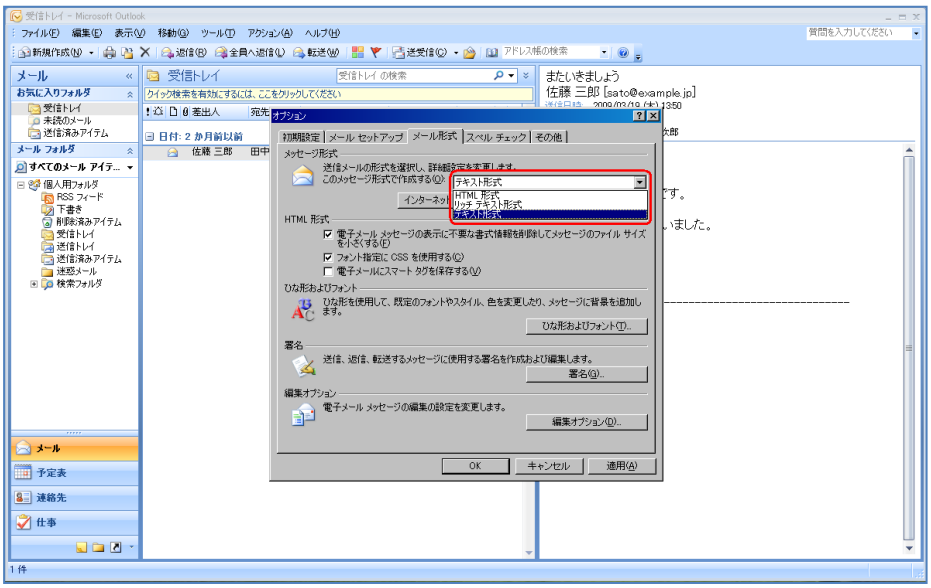
※この画像は Microsoft(R) Office Outlook(R) 2007(12.0.4518.10140) で取得しています。

- 「オプション」ウインドウの「メール形式」タブを選択する。



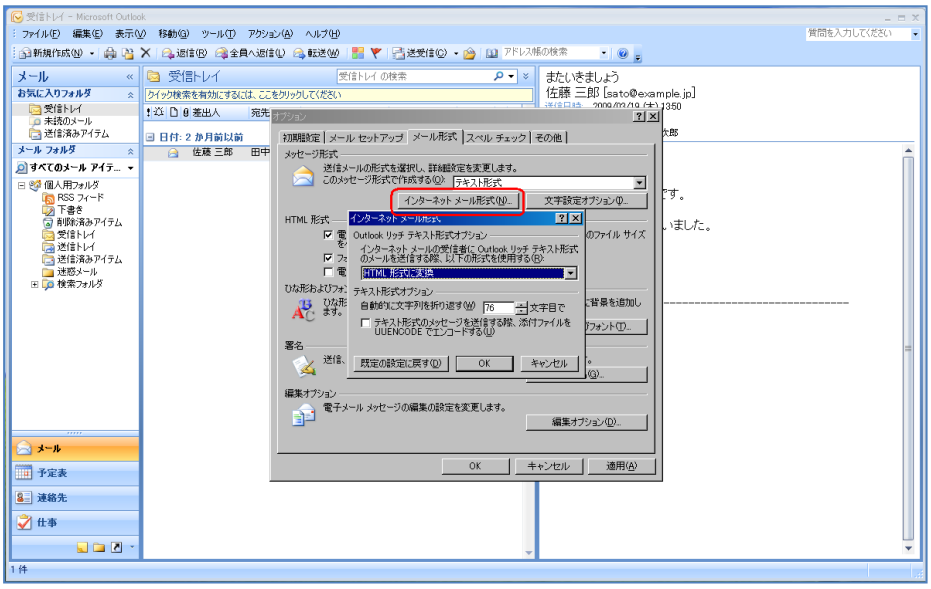
※この画像は Microsoft(R) Office Outlook(R) 2007(12.0.4518.10140) で取得しています。

- 「このメッセージ形式で作成する」を「テキスト形式」に変更する。



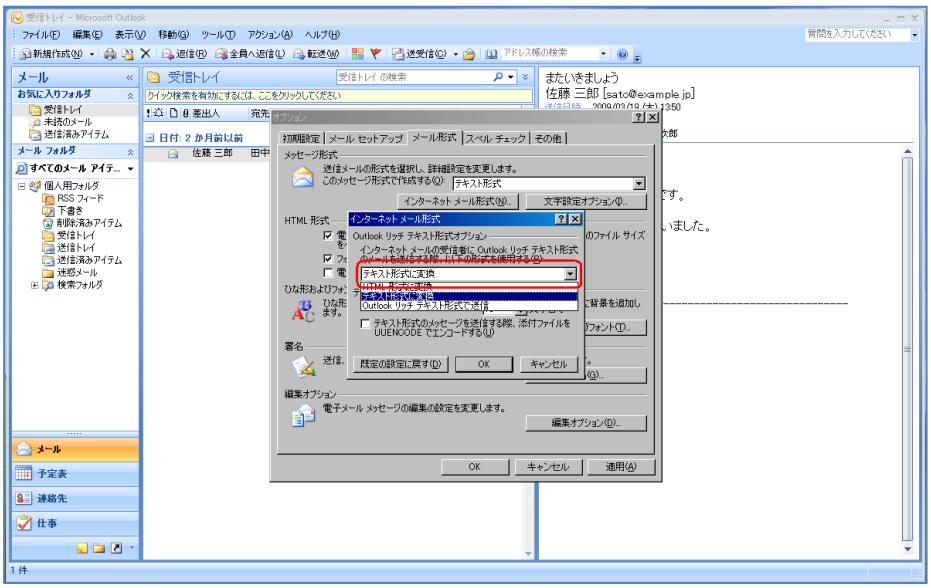
※この画像は Microsoft(R) Office Outlook(R) 2007(12.0.4518.10140) で取得しています。

- 「インターネットメール形式」ボタンを押し、「インターネットメール形式」ウインドウを開く。



※この画像は Microsoft(R) Office Outlook(R) 2007(12.0.4518.10140) で取得しています。

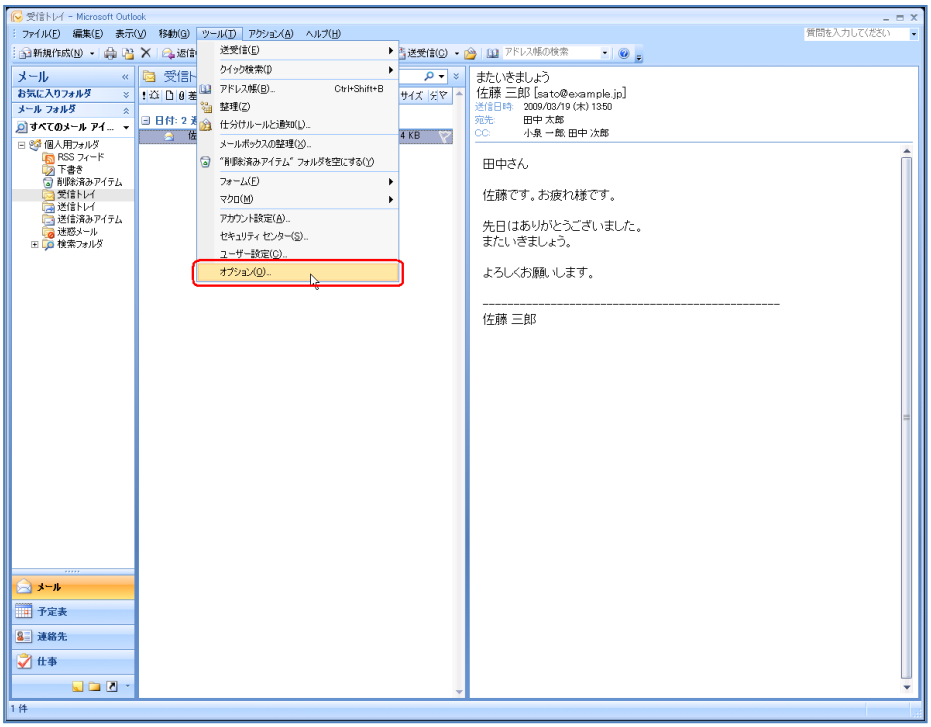
- 「インターネットメール形式」ウインドウ内を「テキスト形式に変換」に変更する。



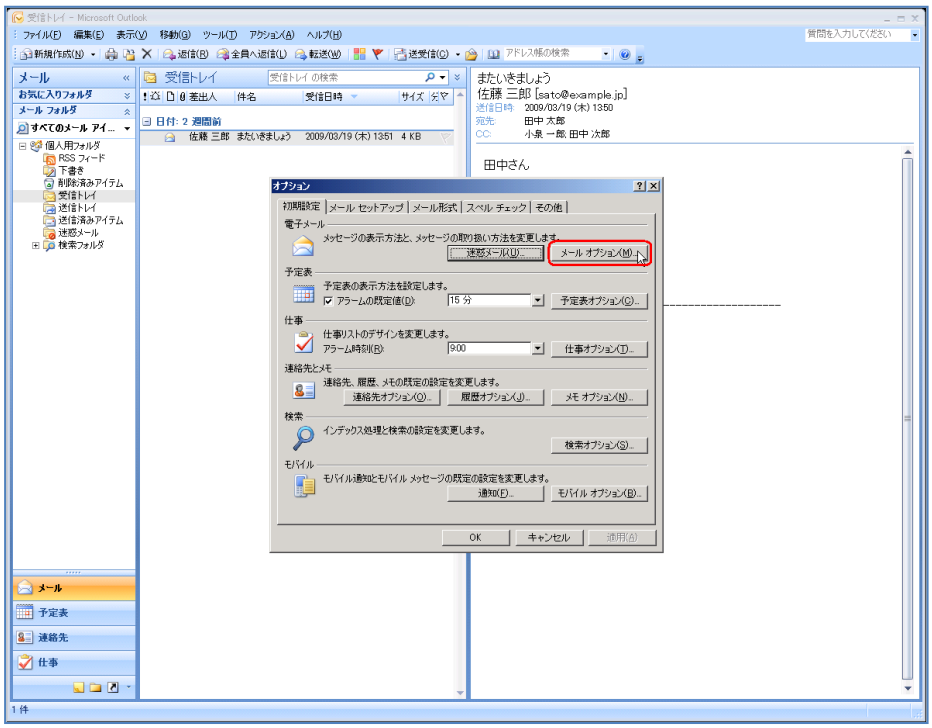
※この画像は Microsoft(R) Office Outlook(R) 2007(12.0.4518.10140) で取得しています。

開封確認機能に関する設定

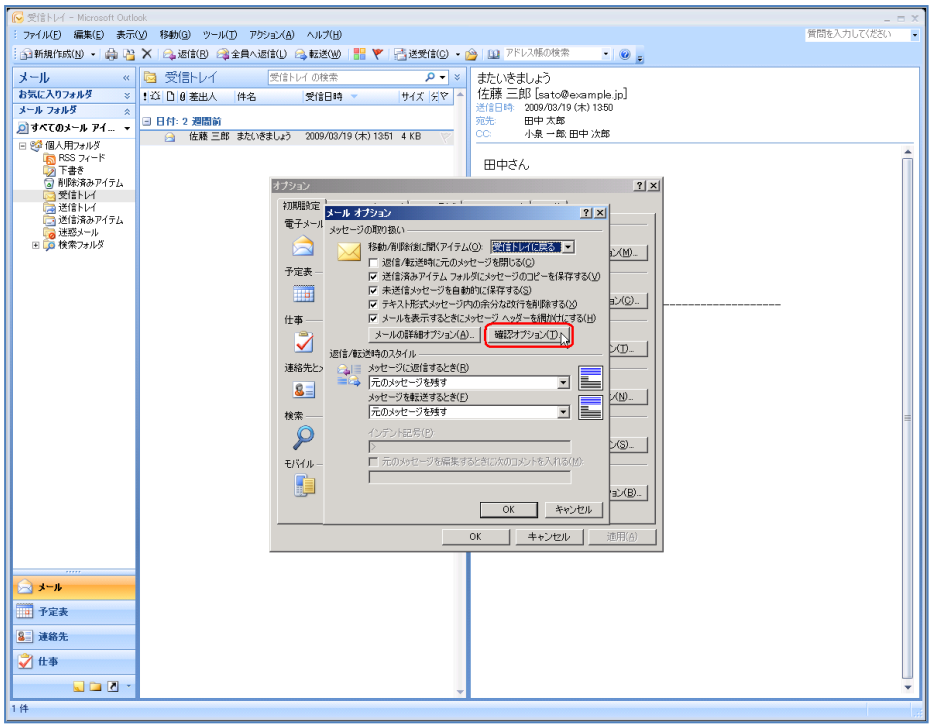
- メニューの「ツール」から「オプション」を選択する。



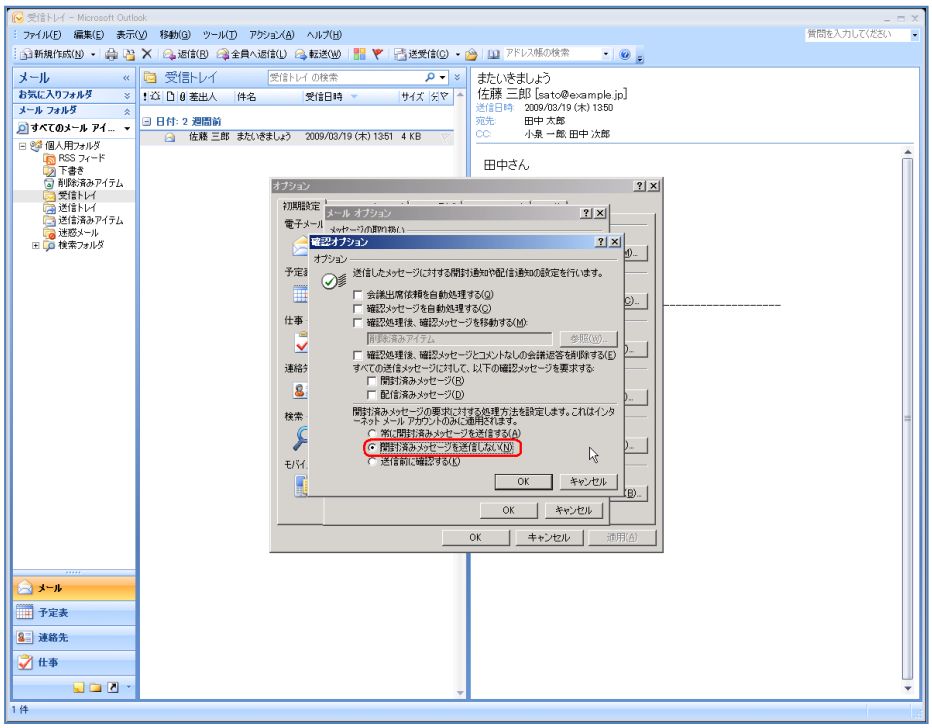
- 「オプション」ウインドウの「初期設定」タブを選択し、「メールオプション」ボタンを押す。



- 「メールオプション」ウインドウの「確認オプション」ボタンを押す。



- 「開封済みメッセージを送信しない」にチェックする。

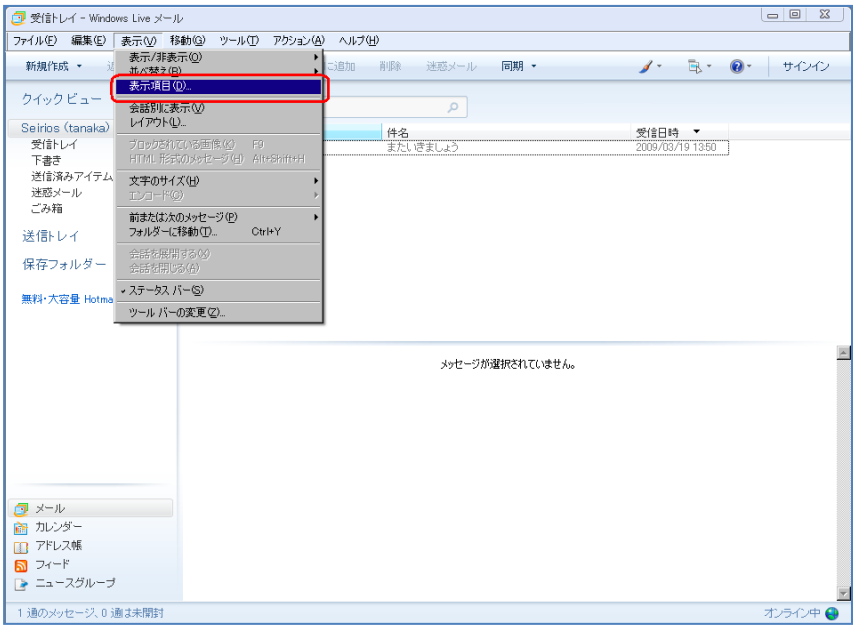


4.6 Windows Live Mail の設定

4.6.1 各設定

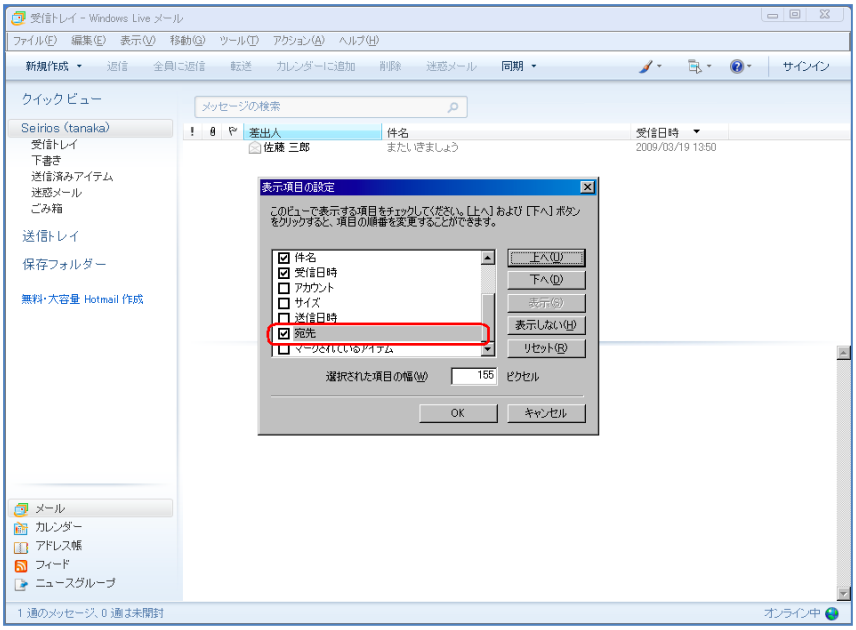
受信メール一覧で表示される情報の拡張

- メニューの「表示」から「表示項目の設定」を選択する。



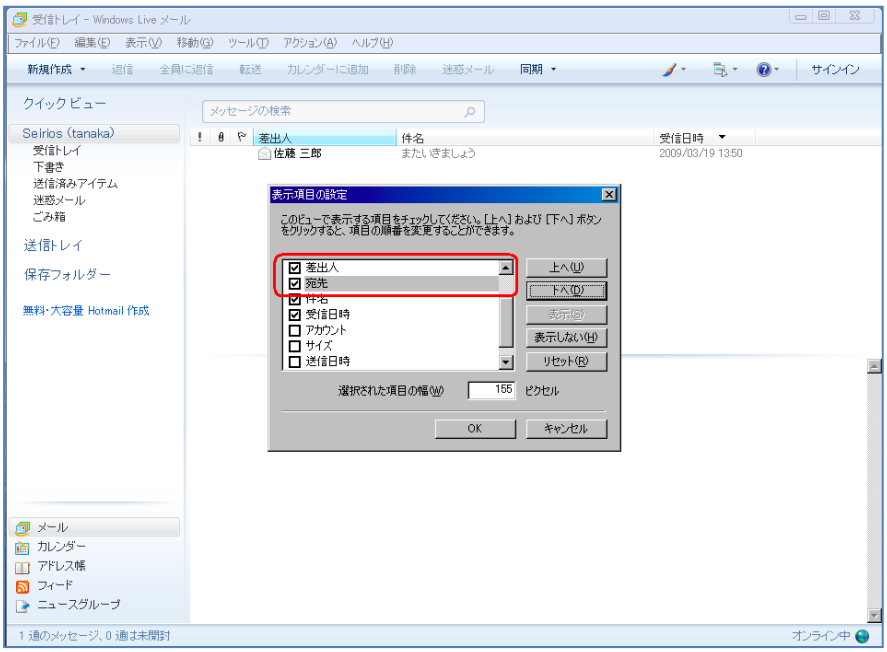
※この画像は Windows Live Mail Version 2009 (Build 14.0.8089.0726) で取得しています。

- 「表示項目の設定」ウインドウの「宛先」のチェックを有効にする。



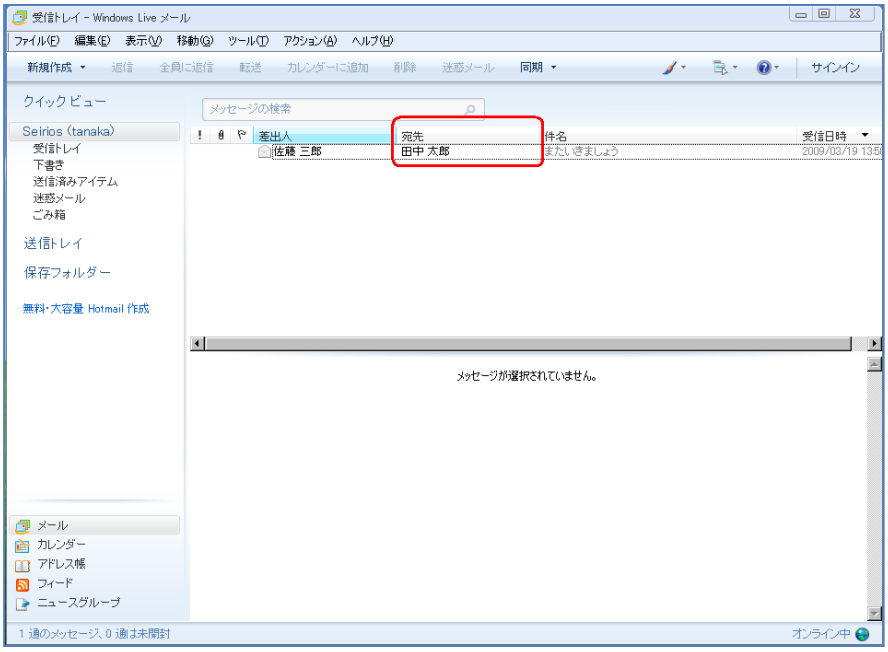
※この画像は Windows Live Mail Version 2009 (Build 14.0.8089.0726) で取得しています。

- 「宛先」を「差出人」の下部に移動する。



※この画像は Windows Live Mail Version 2009 (Build 14.0.8089.0726) で取得しています。

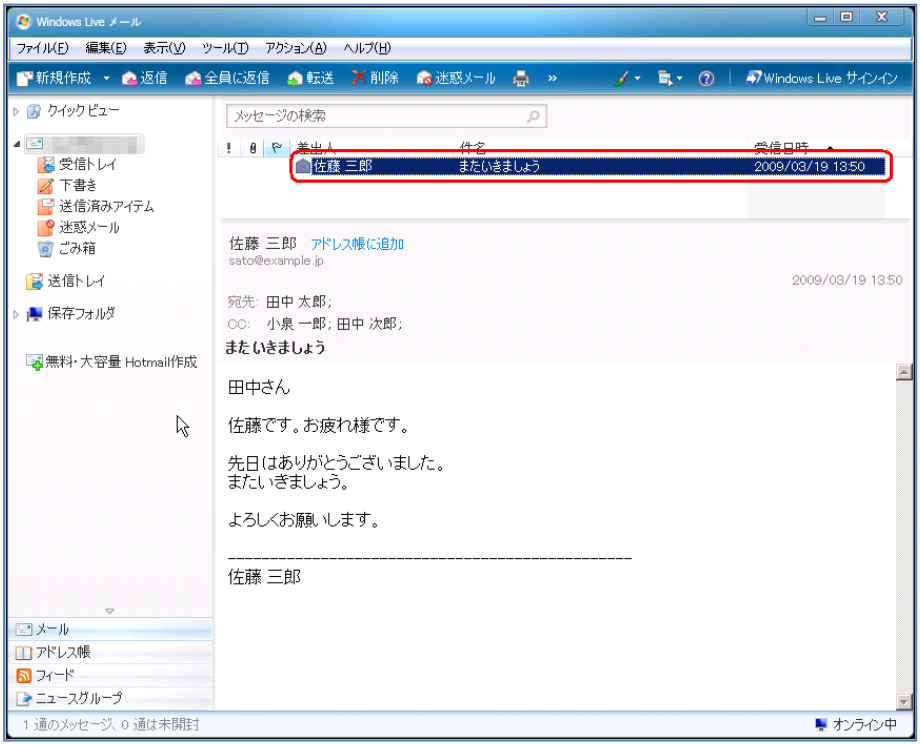
- 表示項目に「宛先」が追加される。



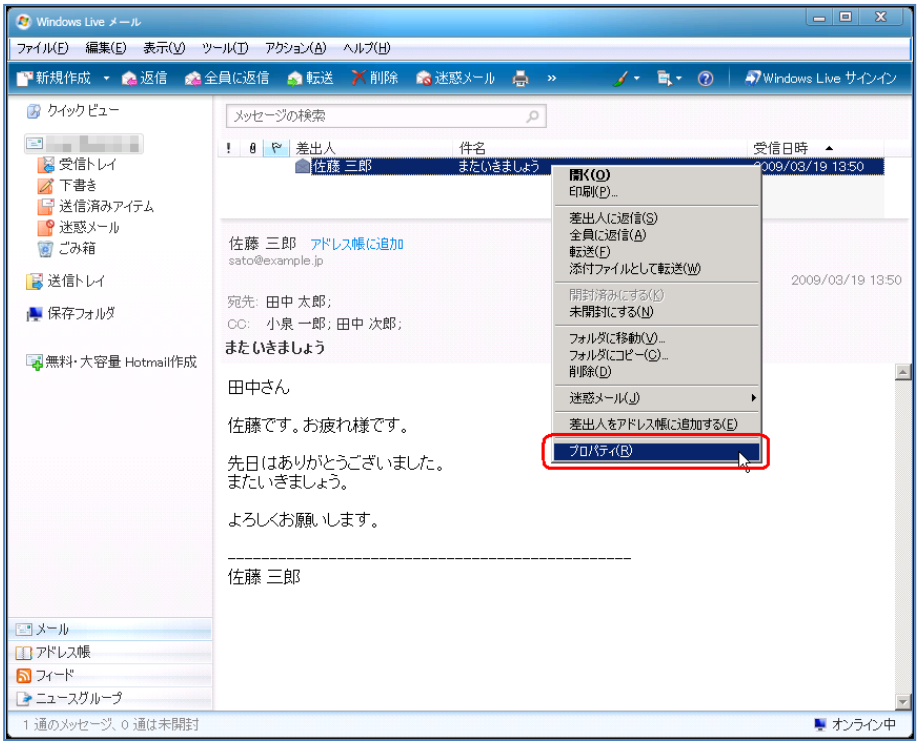
※この画像は Windows Live Mail Version 2009 (Build 14.0.8089.0726) で取得しています。

メールヘッダ情報の確認方法

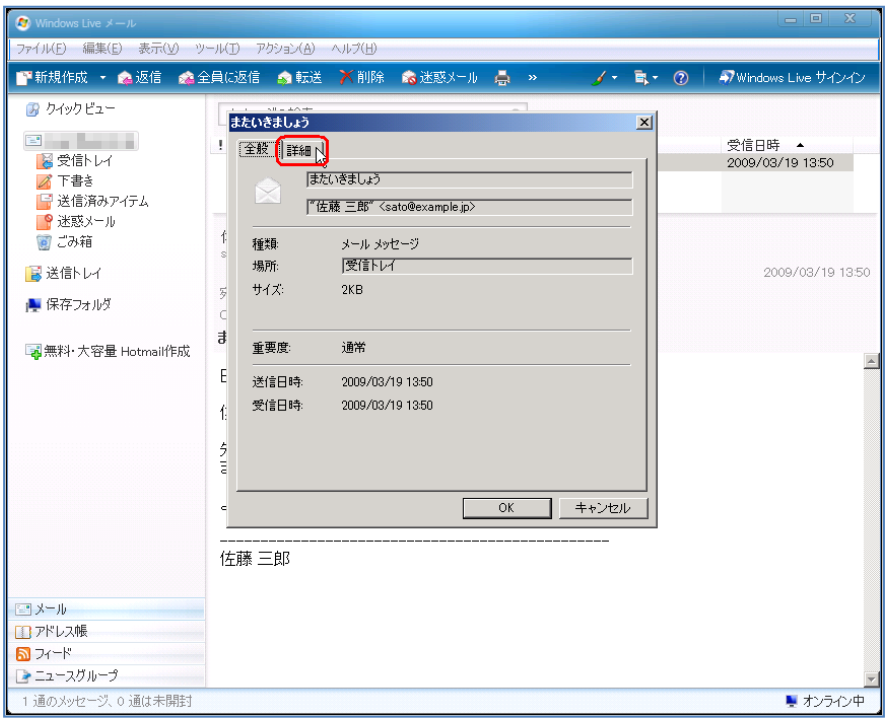
- メールを選択する。



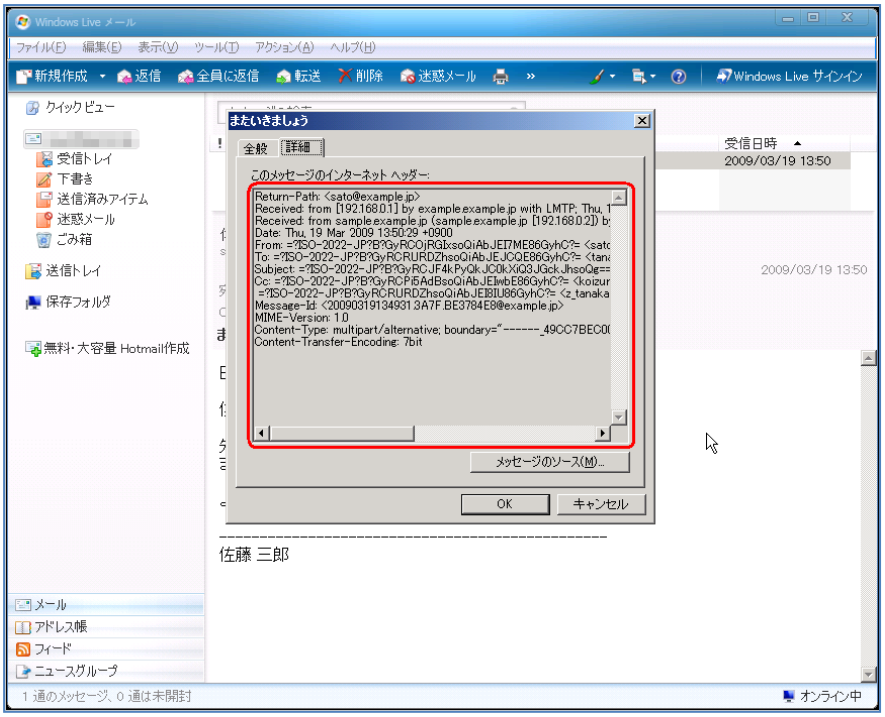
- 右クリックし、「プロパティ」を選択する。



- Subject(件名)ウインドウの「詳細」タブを選択する。



- 「このメッセージのインターネットヘッダ」にヘッダが表示される。

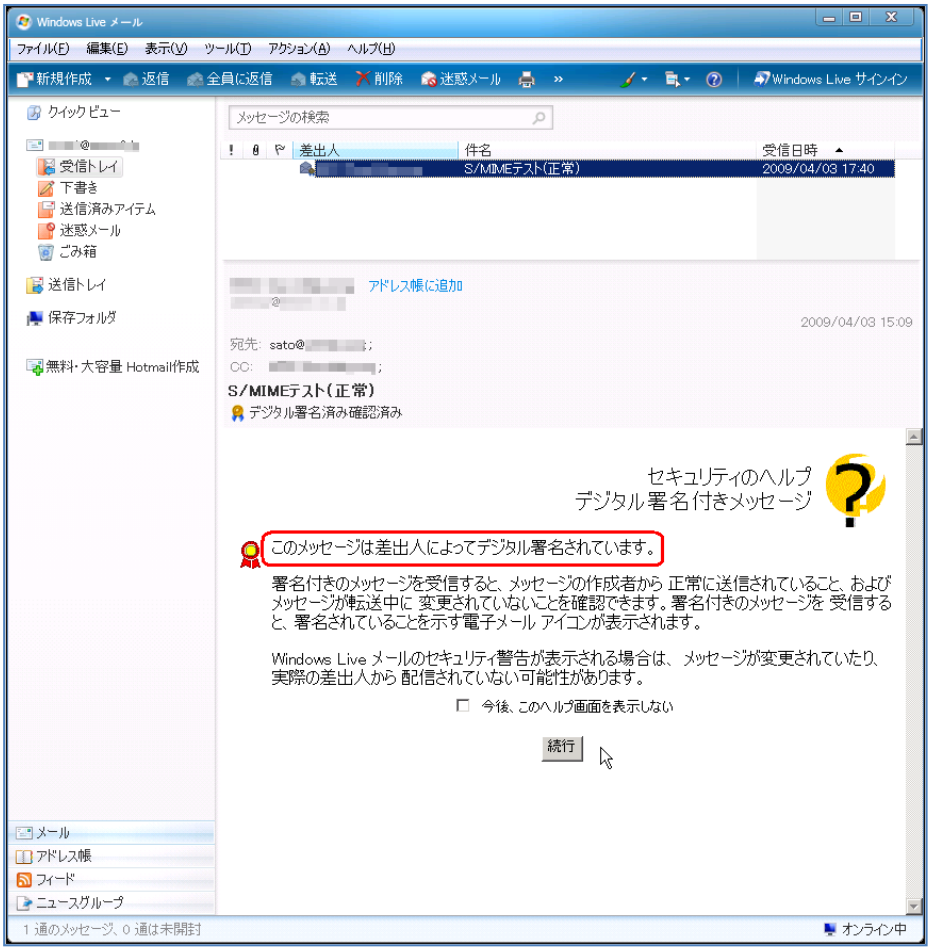


メールアドレスの表示形式の設定

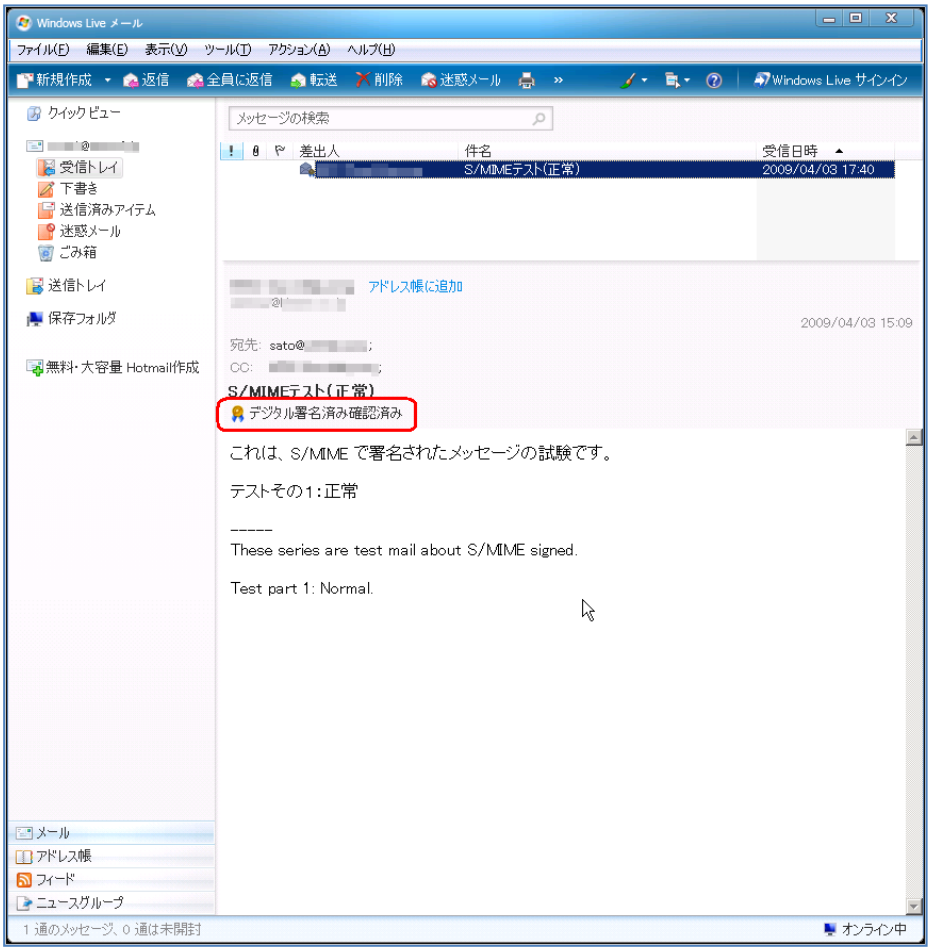
Microsoft Windows Live Mail のメールアドレスの表示形式は、標準で「表示名」と「メールアドレス」の両方を表示します。特別な設定は必要ありません。

S/MIME による署名メールの表示例

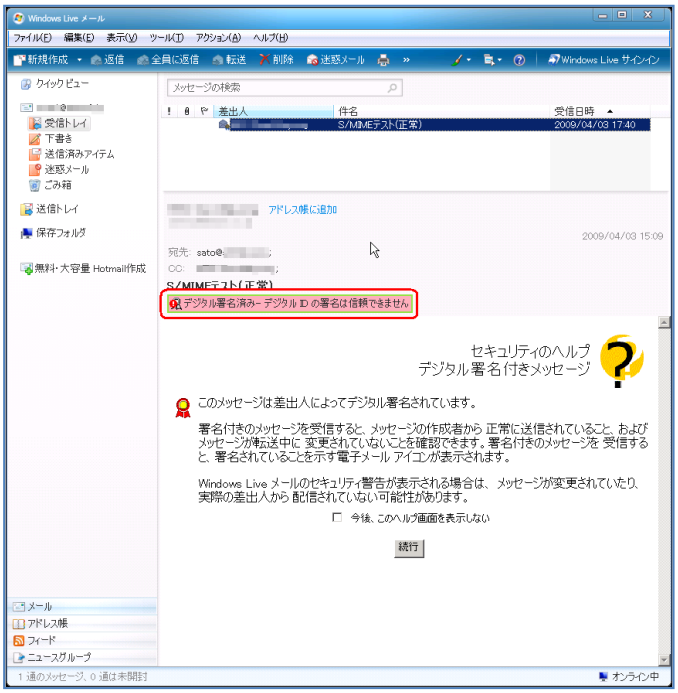
- S/MIME で署名されたメッセージが問題なく検証された場合
    1. デジタル署名されている旨表示される。



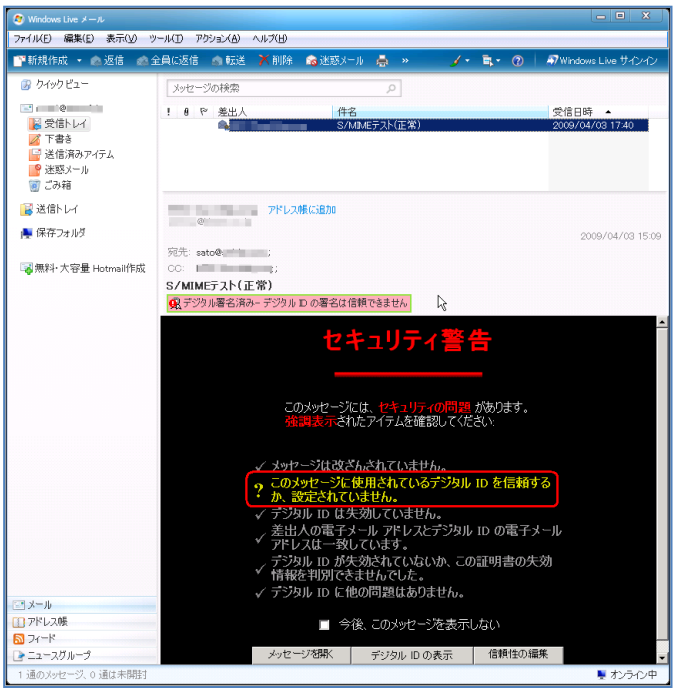
2. 「続行」ボタンを押すと、メール本文が表示される。
デジタル署名が正常な場合、サブジェクトの下部に「デジタル署名済み - 確認済み」と表示される。



- S/MIME で署名されたメッセージの証明書が検証できない場合
  1. デジタル署名されている旨表示される。
     証明書を検証出来ない場合、サブジェクトの下部に「デジタル署名済み - デジタル ID の署名は信頼できません」と表示される。

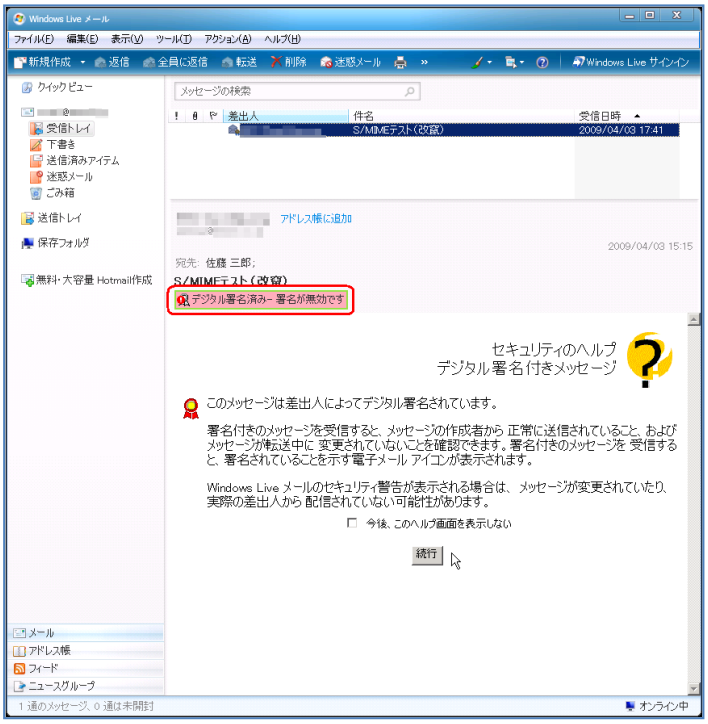


  2. 「続行」ボタンを押すと、セキュリティ警告のメッセージが表示される。
     証明書を検証出来ない場合、強調表示されている部分に「このメッセージに使用されているデジタル ID を信頼するか、設定されていません。」と表示される。

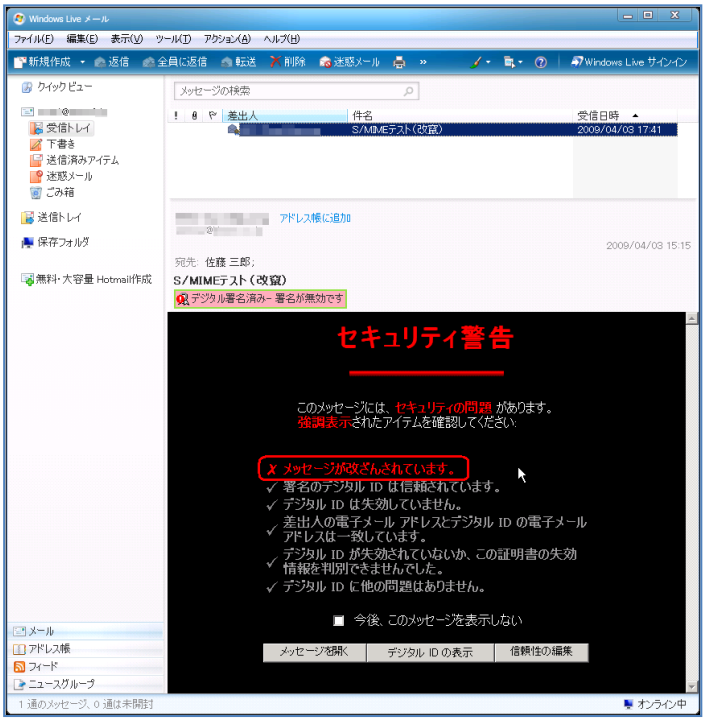


- S/MIME で署名されたメッセージが改ざんされている場合

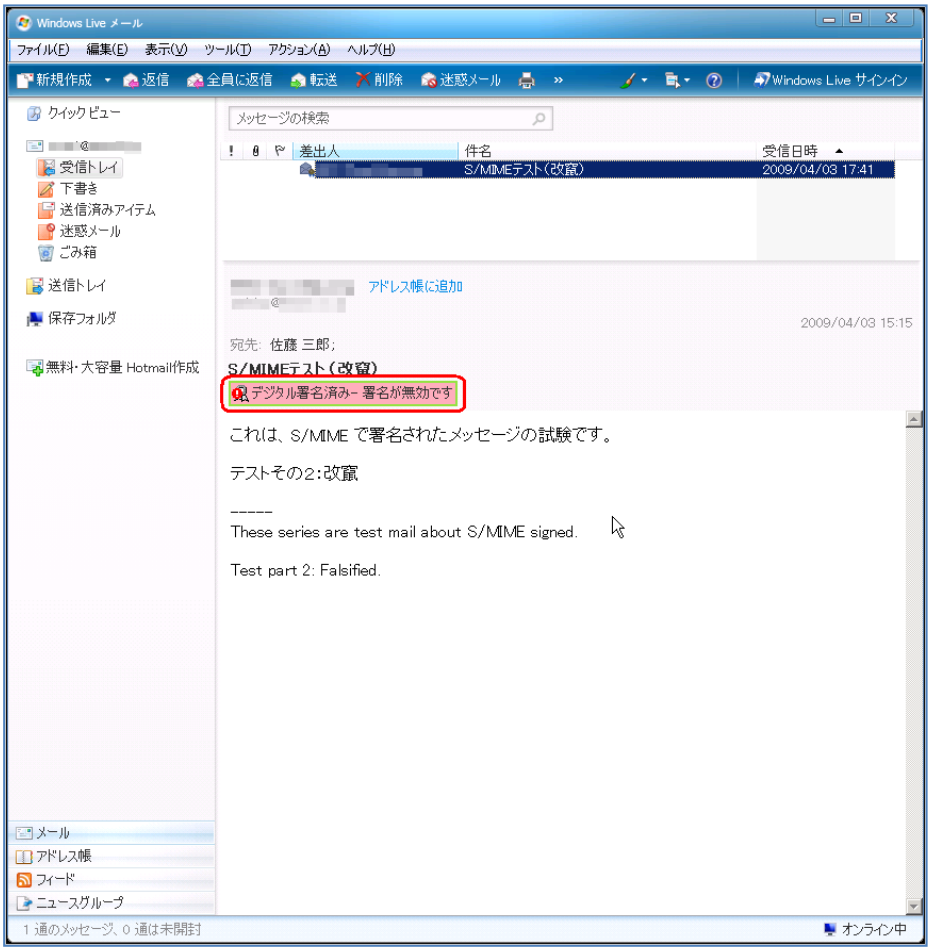
1. デジタル署名されている旨表示される。
メッセージが改ざんされている場合、サブジェクトの下部に「デジタル署名済み - 署名が無効です」と表示される。



2. 「続行」ボタンを押すと、セキュリティ警告のメッセージが表示される。
メッセージが改ざんされている場合、強調表示されている部分に「メッセージが改竄されています。」と表示される。



3. 「メッセージを開く」を選択すると、メッセージが表示される。
メッセージが改ざんされている場合、サブジェクトの下部に「デジタル署名済み - 署名が無効です」と表示される。

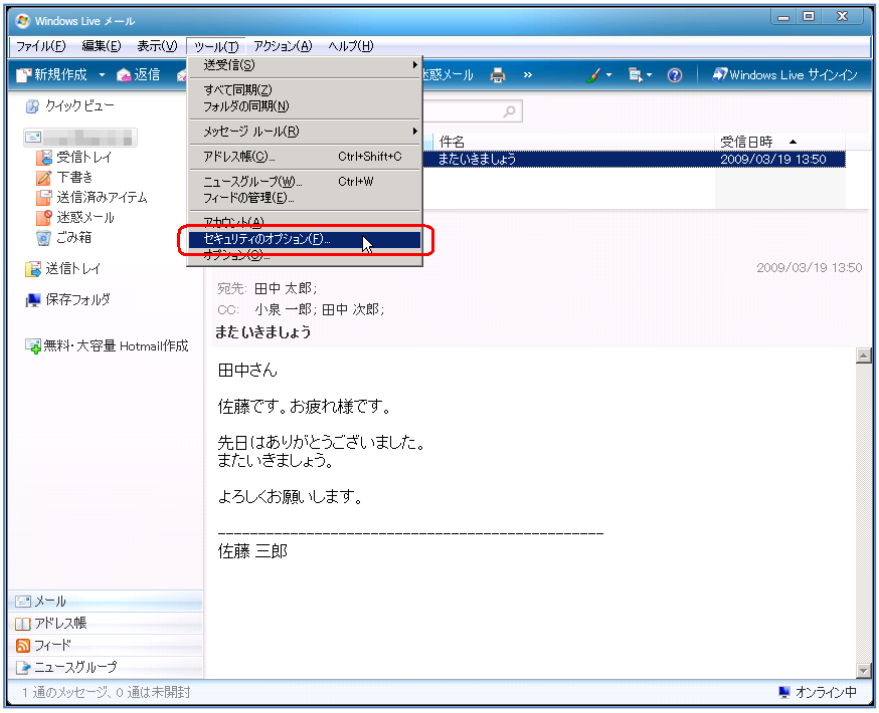


PGP 対応

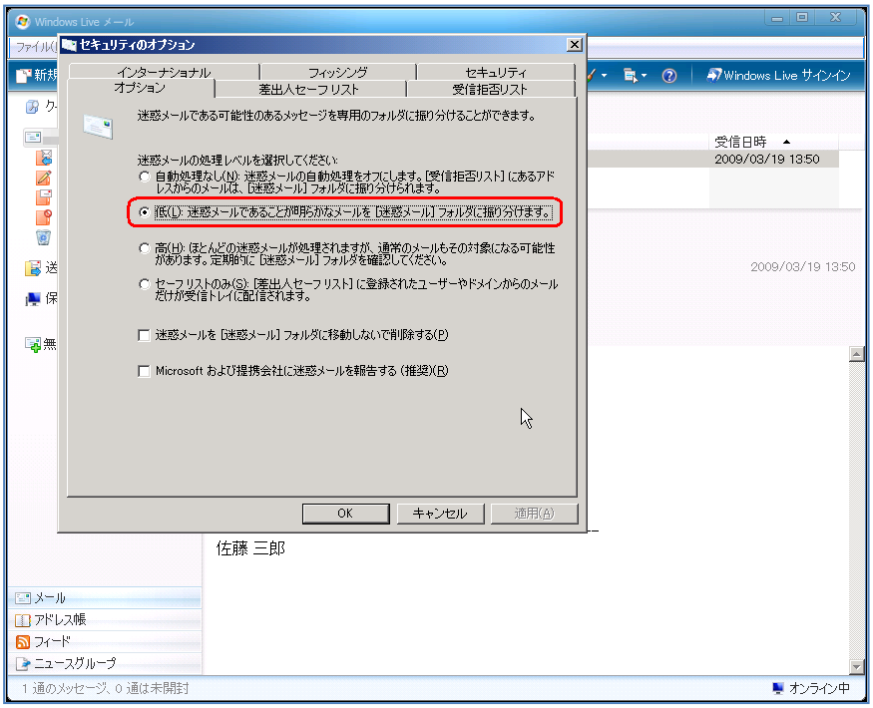
Microsoft Windows Live Mail は、標準で PGP をサポートしていません。

迷惑メールフィルタの設定

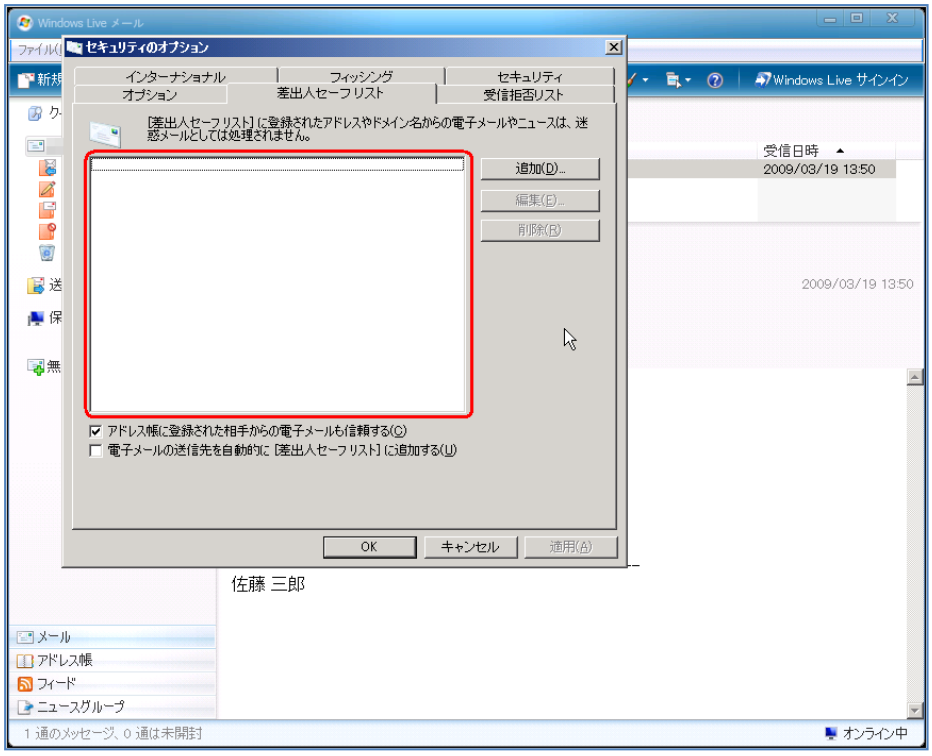
- メニューの「ツール」から「セキュリティのオプション」を選択する。



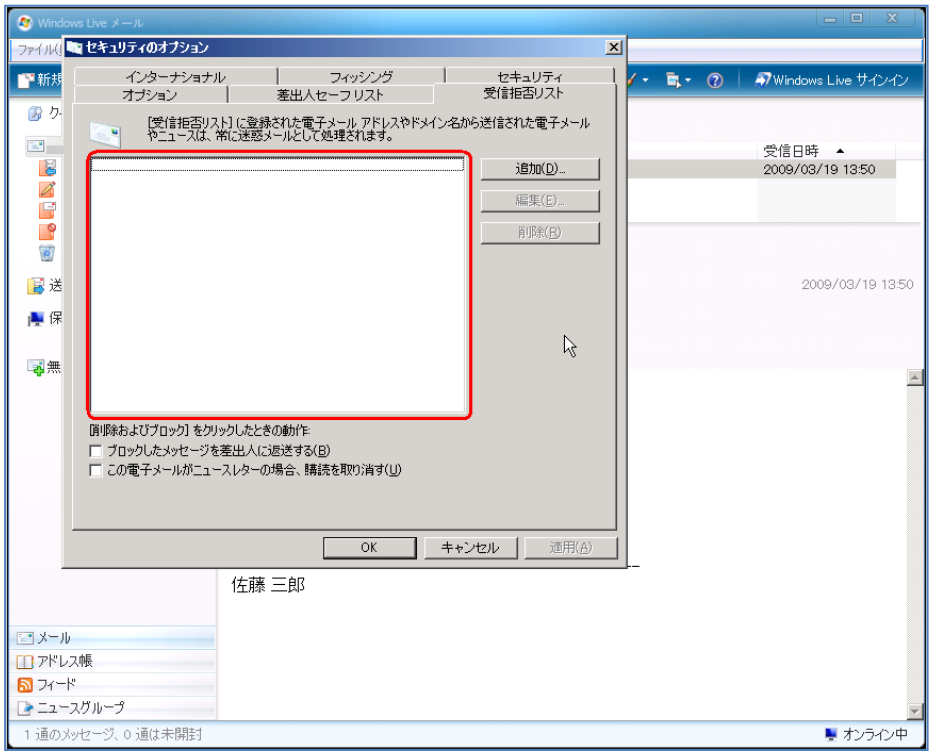
- 「セキュリティのオプション」ウインドウの「オプション」タブを選択する。
必要に応じて、迷惑メールの処理レベルを選択してください。 ここでは、「低：迷惑メールであることが明らかなメールを「迷惑メール」フォルダに振り分けます。」を選択。



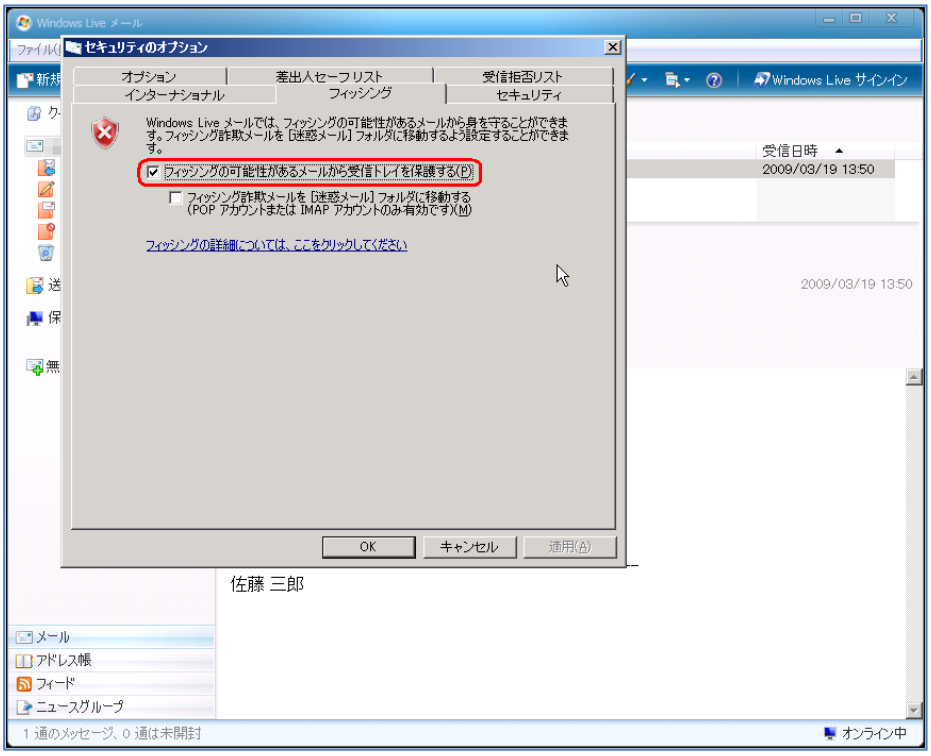
- 「差出人セーフリスト」タブを選択する。
  必要に応じて、迷惑メール処理を行わない差出人メールアドレスを登録して下さい。



- 「受信拒否リスト」タブを選択する。
  必要に応じて、受信拒否を行うメールアドレスを登録して下さい。

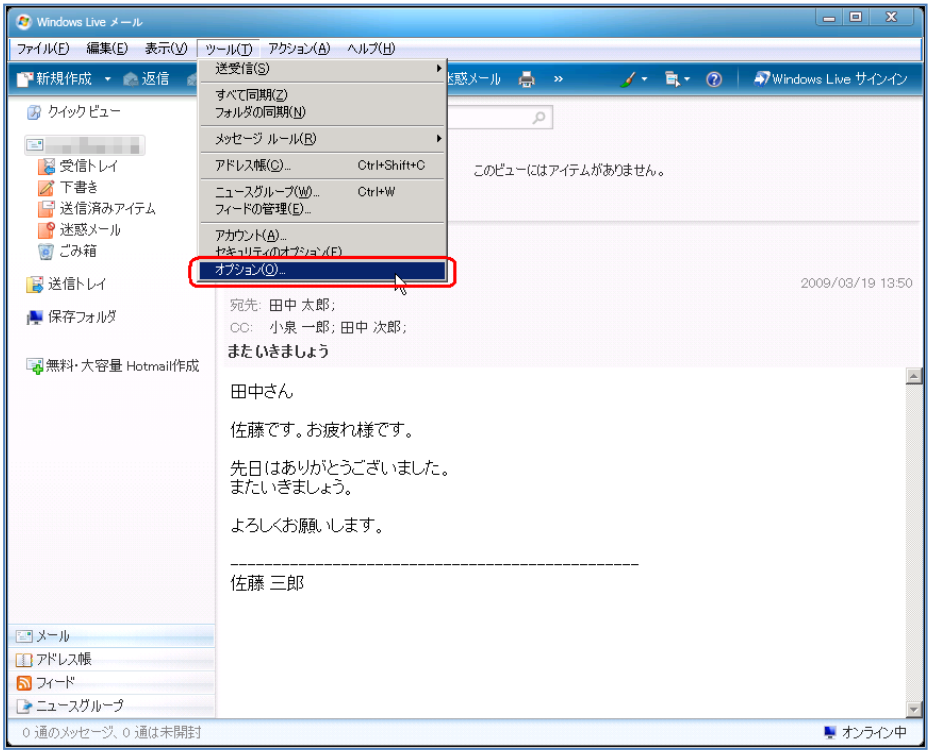


- 「フィッシング」タブを選択する。
  「フィッシングの可能性があるメールから受信トレイを保護する」がチェックされていることを確認して下さい。

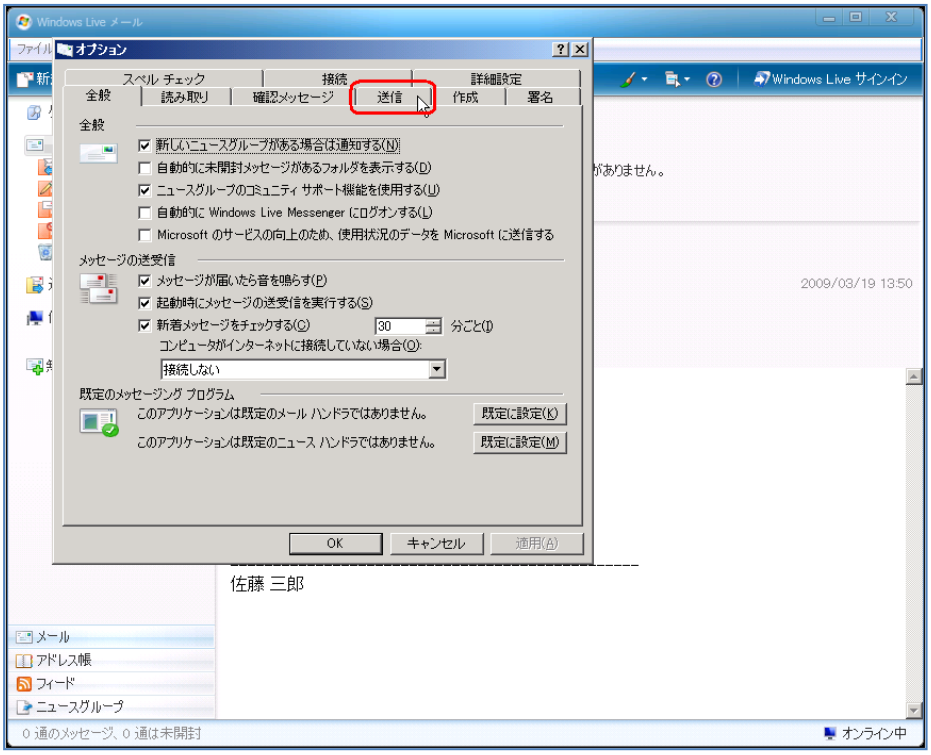


メール送信フォーマットに関する設定

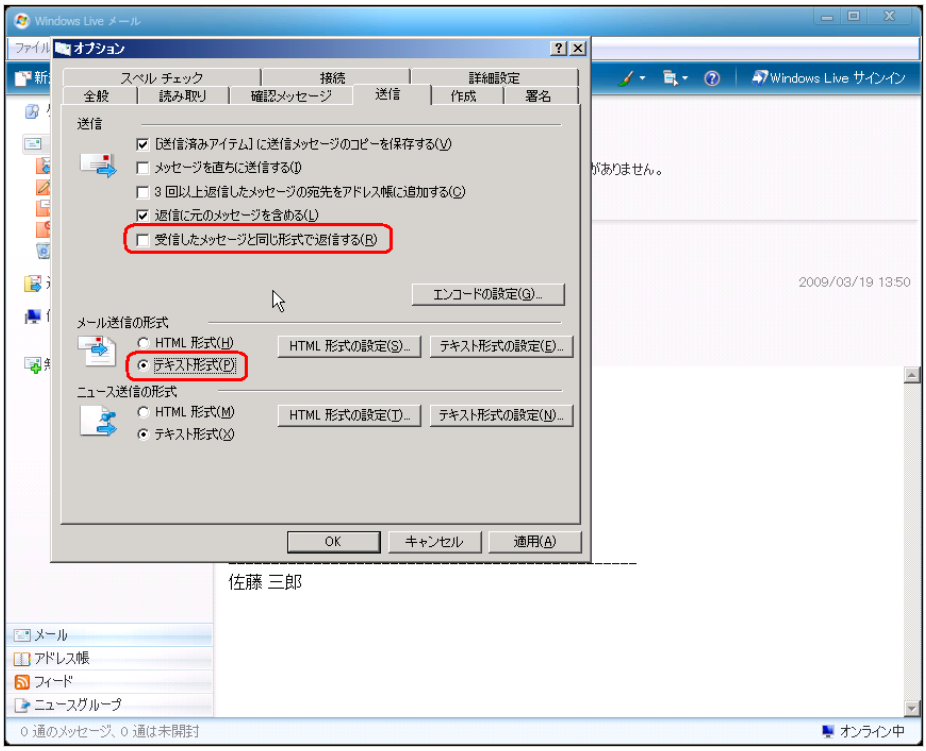
- メニューの「ツール」から「オプション」を選択する。



- 「オプション」ウインドウの「送信」タブを選択する。

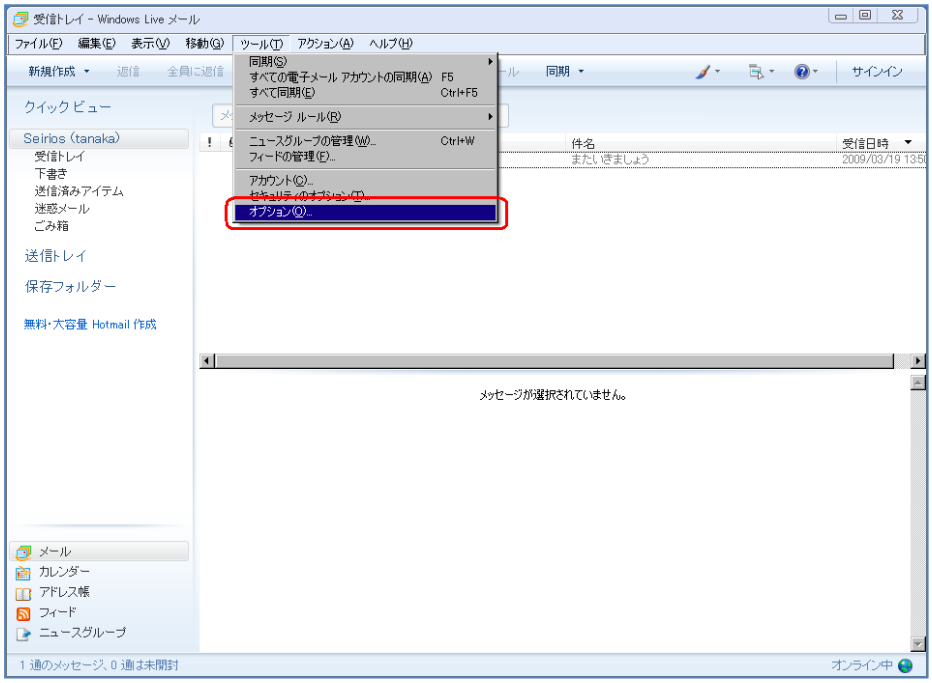


- 「受信したメッセージと同じ形式で返信する」のチェックを外し、「メール送信の形式」を「テキスト形式」にする。



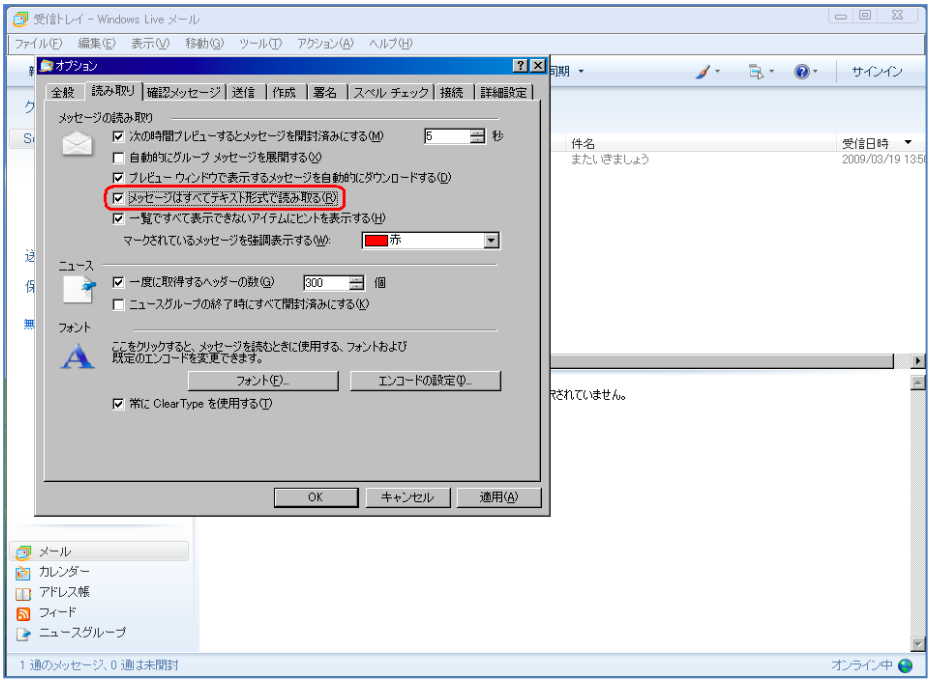
HTML メールの表示に関する設定

- メニューの「ツール」から「オプション」を選択する。



※この画像は Windows Live Mail Version 2009 (Build 14.0.8089.0726) で取得しています。

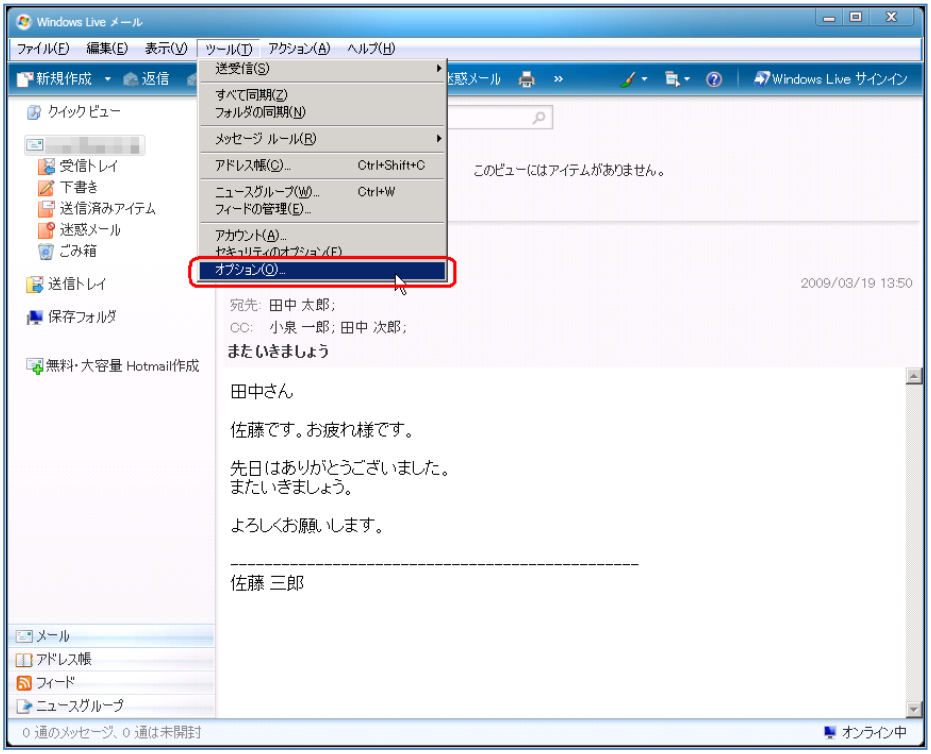
- 「オプション」ウインドウの「読み取り」タブを選択し、「メッセージはすべてテキスト形式で読み取る」のチェックを有効にする。



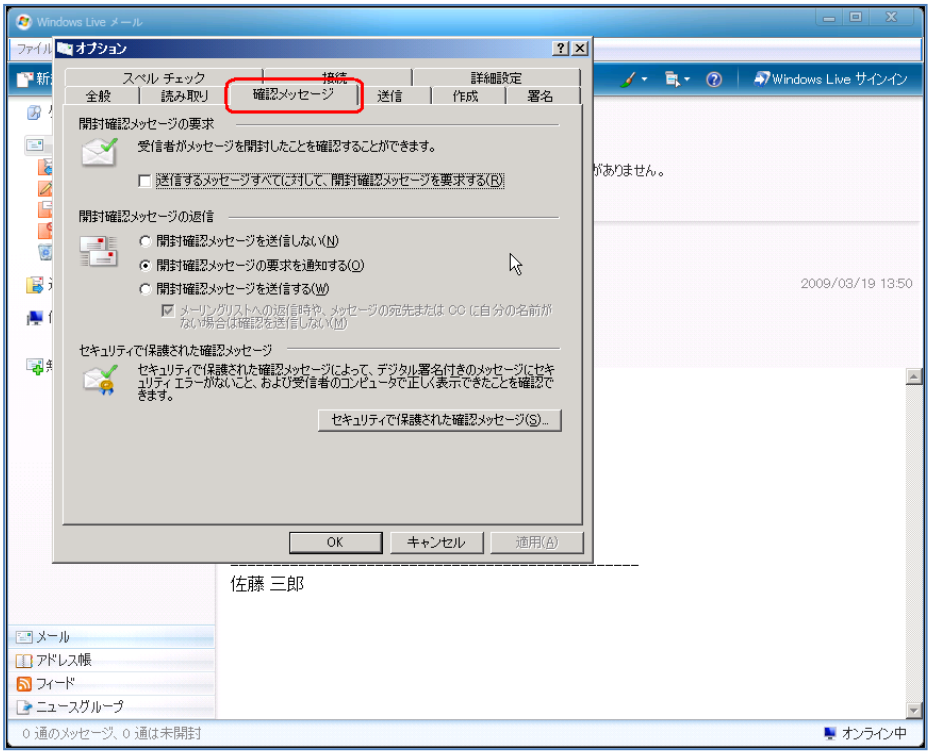
※この画像は Windows Live Mail Version 2009 (Build 14.0.8089.0726) で取得しています。

開封確認機能に関する設定

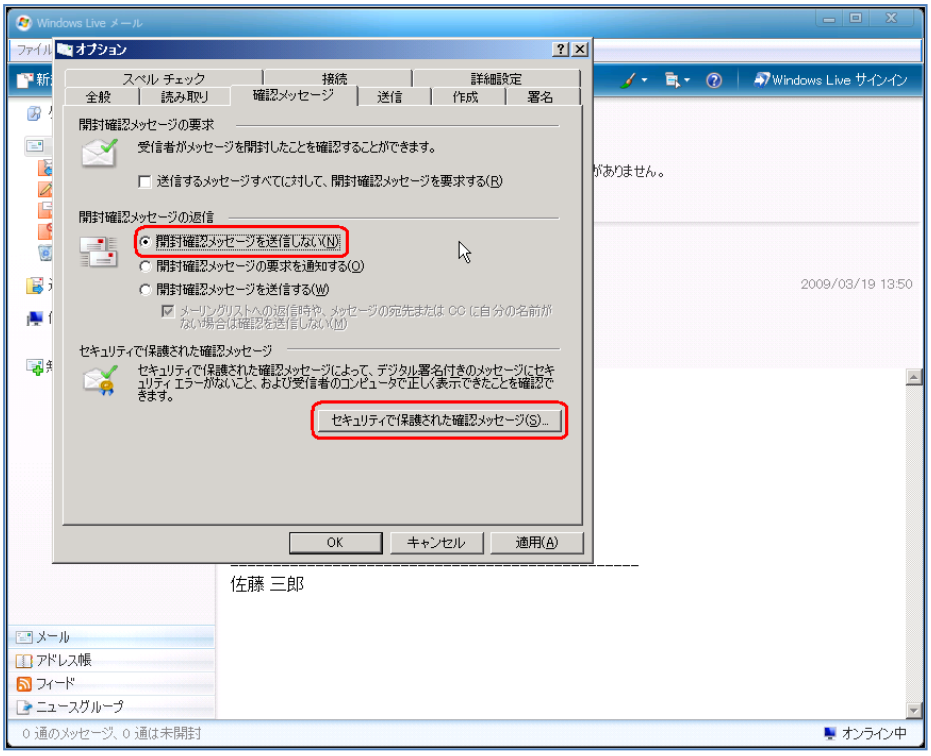
- メニューの「ツール」から「オプション」を選択する。



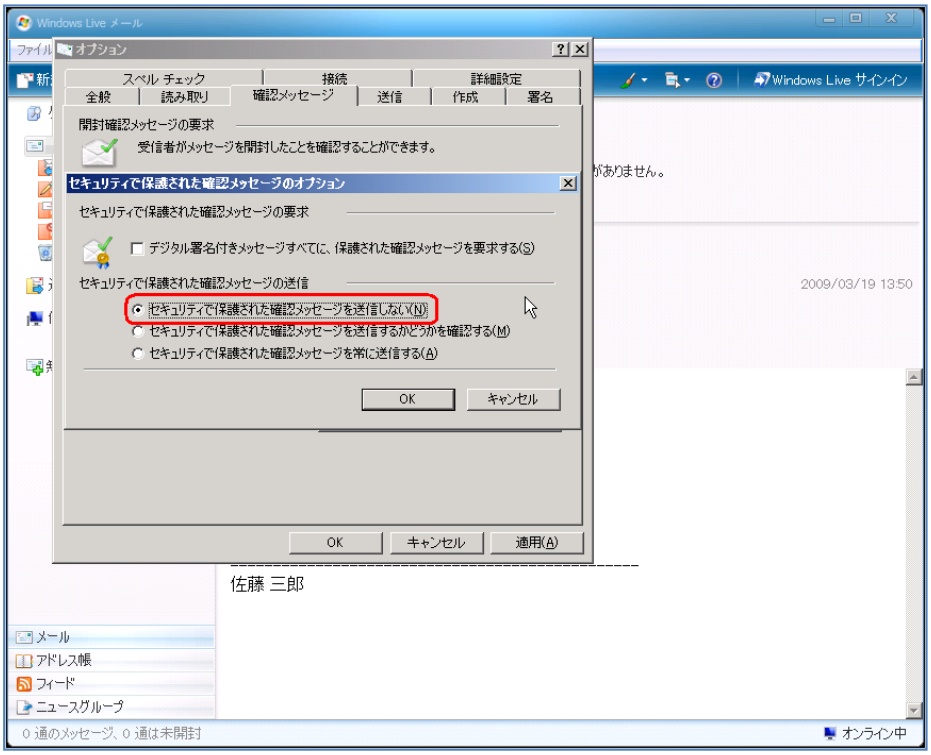
- 「オプション」ウインドウの「確認メッセージ」タブを選択する。



- 「開封確認メッセージを送信しない」をチェックし、「セキュリティで保護された確認メッセージ」を選択する。



- 「セキュリティで保護された確認メッセージを送信しない」をチェックする。

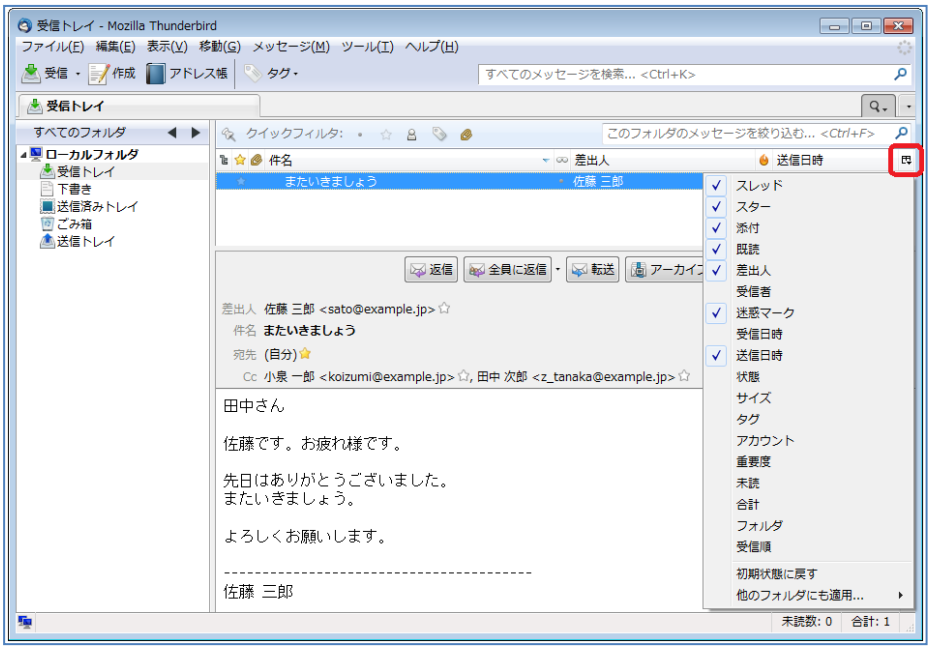


4.7 Mozilla Thundarbird の設定

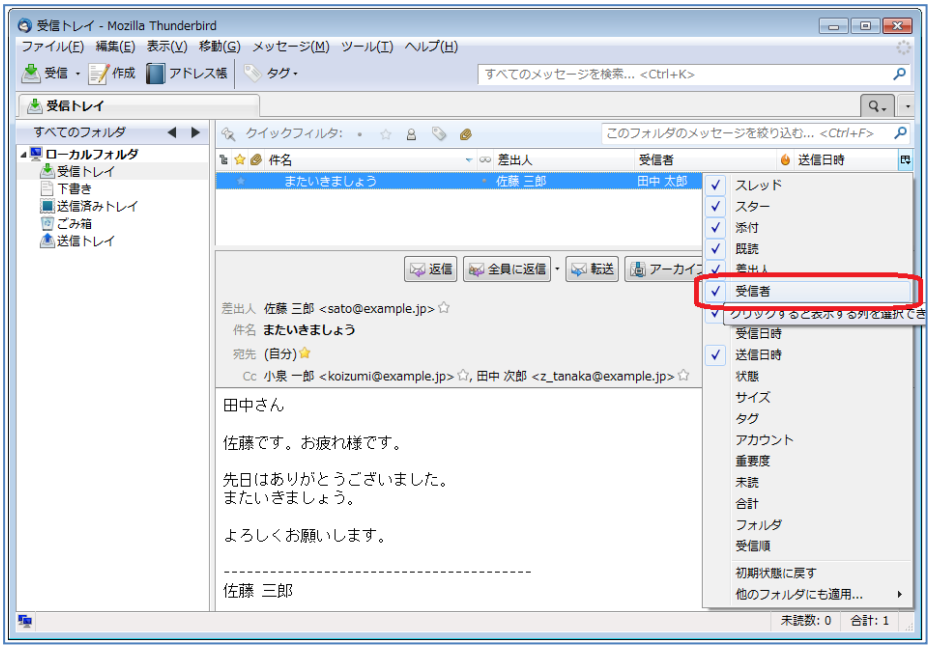
4.7.1 各設定

メール一覧で表示される情報の拡充

- 表示項目の右端にあるアイコンをクリックする。

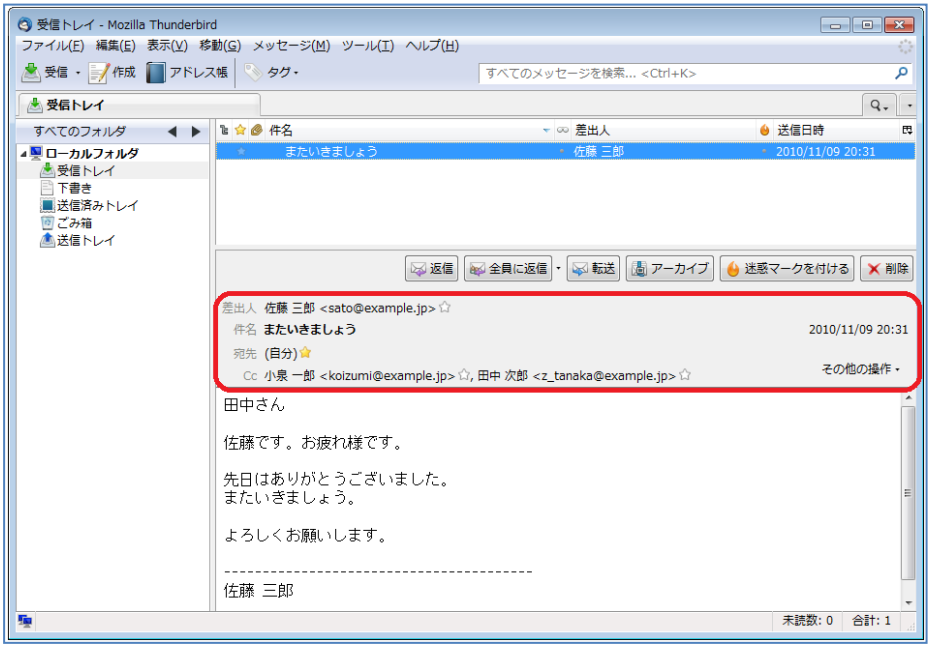


- 「受信者」を有効にすることで、表示項目に「受信者」が追加される。

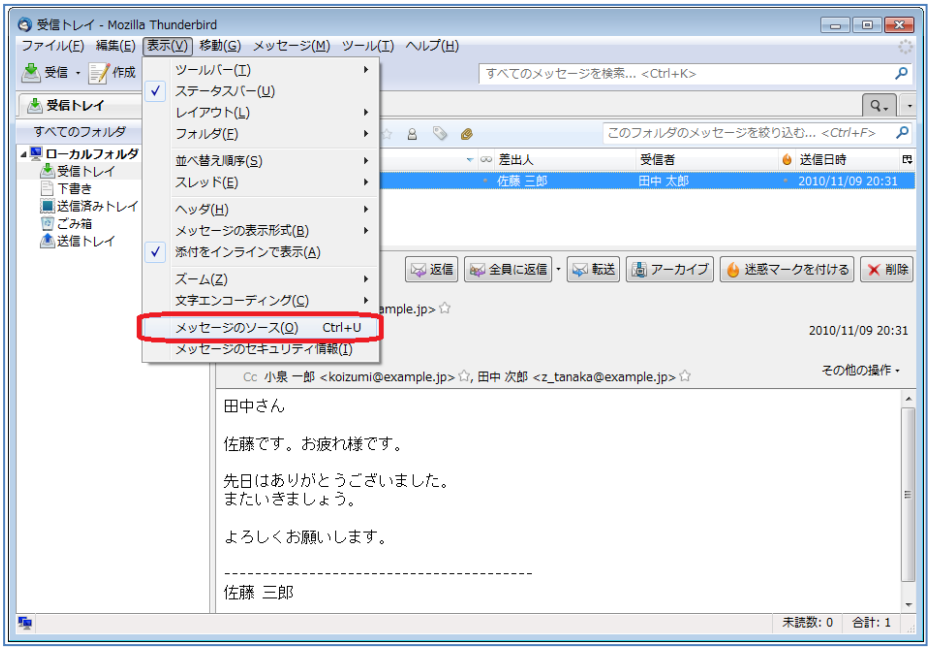


メールヘッダ情報の確認方法

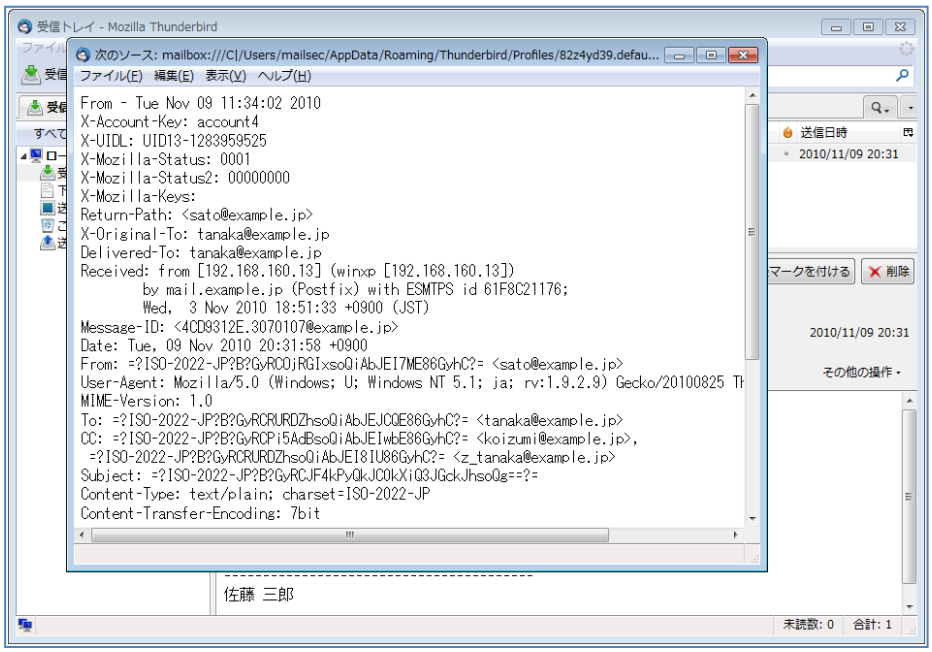
- メールを選択する。



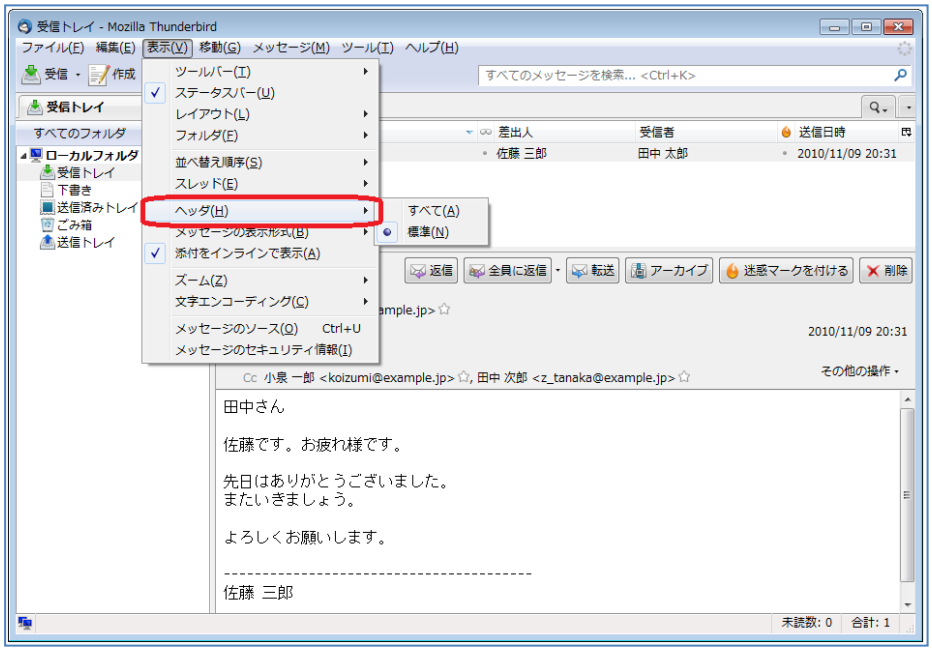
- メニューの「表示」から「メッセージのソース」を選択する。



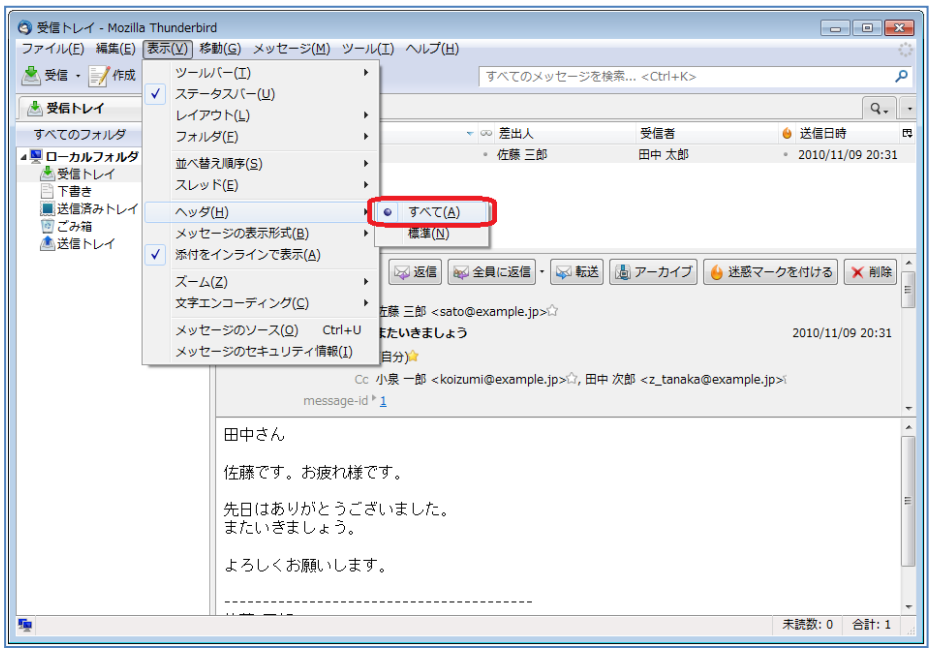
- 別ウインドウが開き、メッセージのソースが表示される。



- また、以下の手順を実行することでメール本文にメールヘッダ情報を表示します。
メール本文にメニューの「表示」から「ヘッダ」を選択する。



- 「すべて」を選択することで、メールヘッダ情報が表示される。

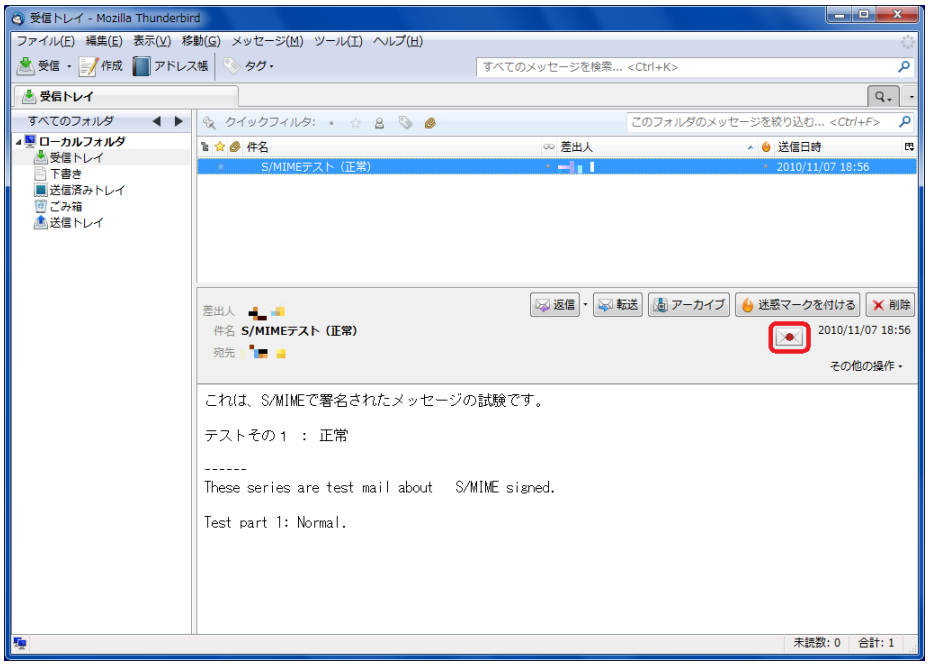


メールアドレスの表示形式の設定

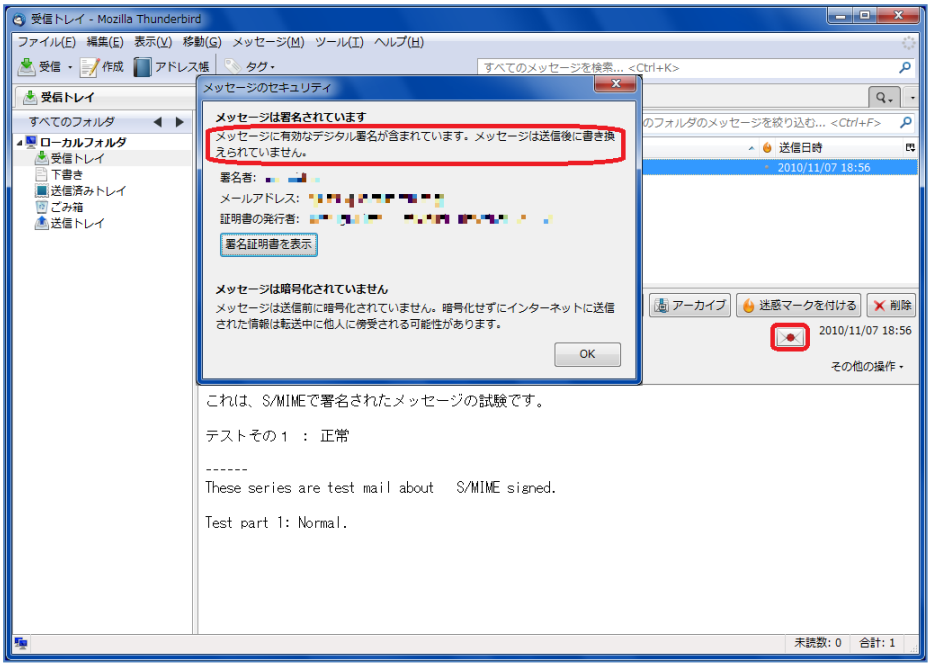
Mozilla Thunderbird は標準で差出人の情報を「表示名」と「メールアドレス」の両方を表示します。特別な設定は必要ありません。

S/MIME による署名メールの表示例

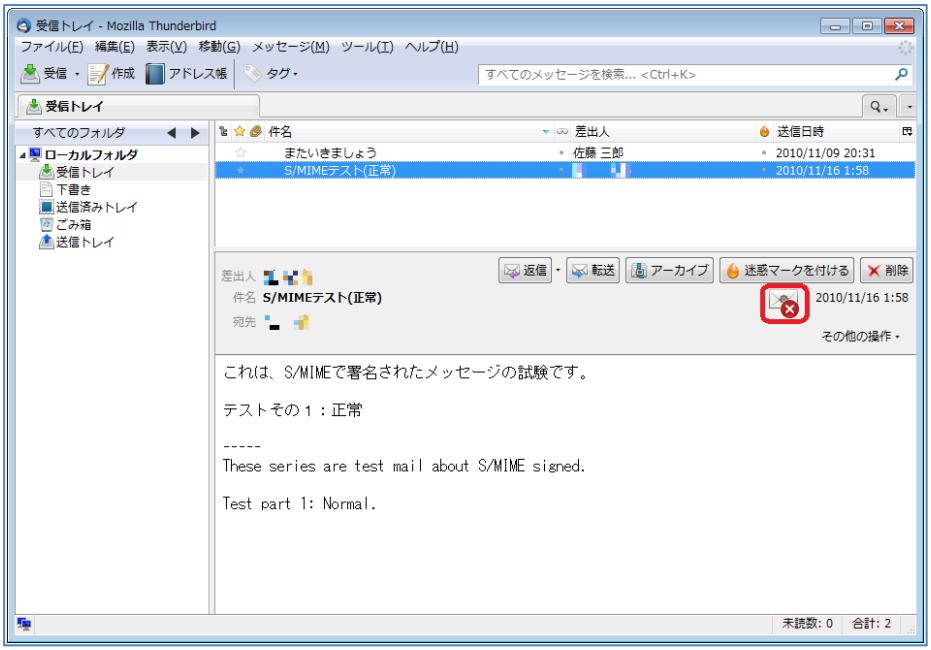
- S/MIME で署名されたメッセージが問題なく検証された場合
  1. メッセージが表示され、右側に正常を意味するアイコンが表示される。



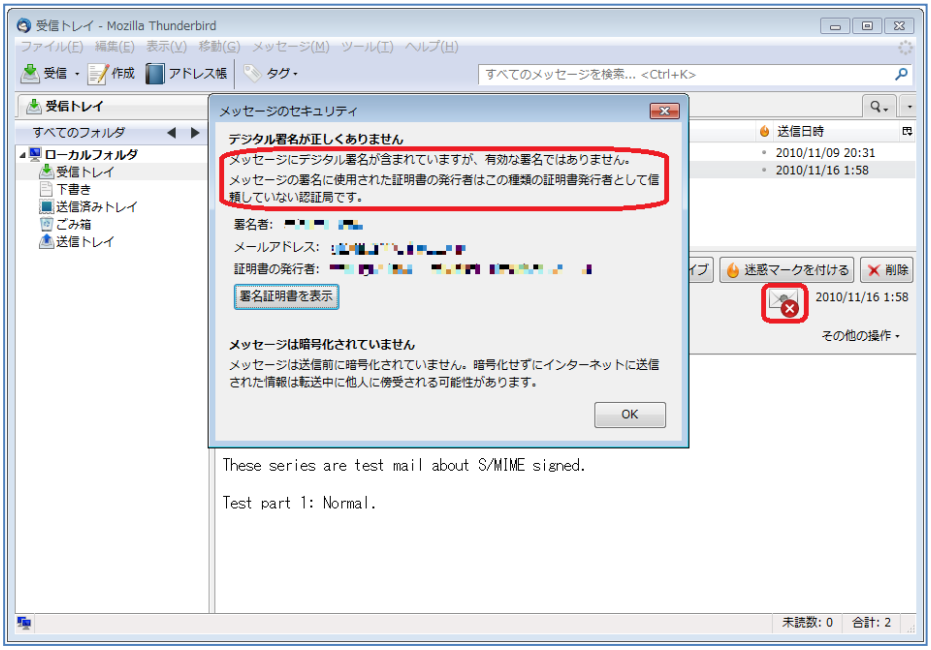
  2. 正常を意味する「封筒」型のアイコンをクリックすると「メッセージのセキュリティ」ウインドウが開く。
     デジタル署名が正常な場合、「メッセージに有効なデジタル署名が含まれています。メッセージは送信後に書き換えられていません。」と表示される。



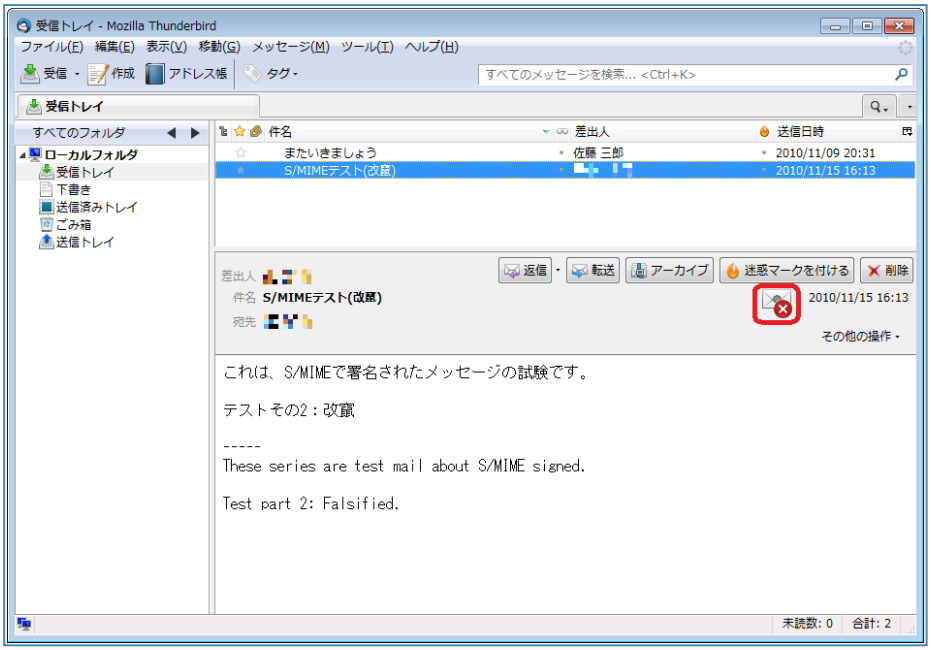
- S/MIME で署名されたメッセージの証明書が検証できない場合
  1. メッセージが表示され、右側に異常を意味するアイコンが表示される。



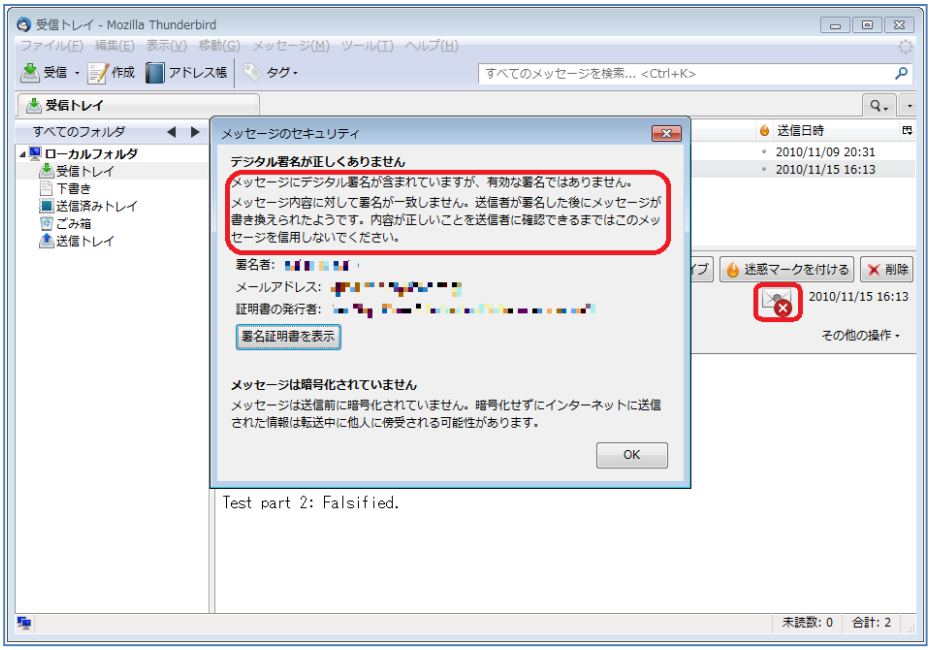
  2. 異常を意味する「封筒」型のアイコンをクリックすると「メッセージのセキュリティ」ウインドウが開く。
     証明書を検証出来ない場合、「メッセージにデジタル署名が含まれていますが、有効な署名ではありません。メッセージの署名に使用された証明書の発行者はこの種類の証明書発行者として信頼していない認証局です。」と表示される。



- S/MIME で署名されたメッセージが改ざんされている場合
  1. メッセージが表示され、右側に異常を意味するアイコンが表示される。



  2. 異常を意味する「封筒」型のアイコンをクリックすると「メッセージのセキュリティ」ウインドウが開く。
     メッセージが改ざんされている場合、「メッセージにデジタル署名が含まれていますが、有効な署名ではありません。メッセージ内容に対して署名が一致しません。送信者が署名した後にメッセージが書き換えられたようです。内容が正しいことを送信者に確認できるまではこのメッセージを信用しないでください。」と表示される。

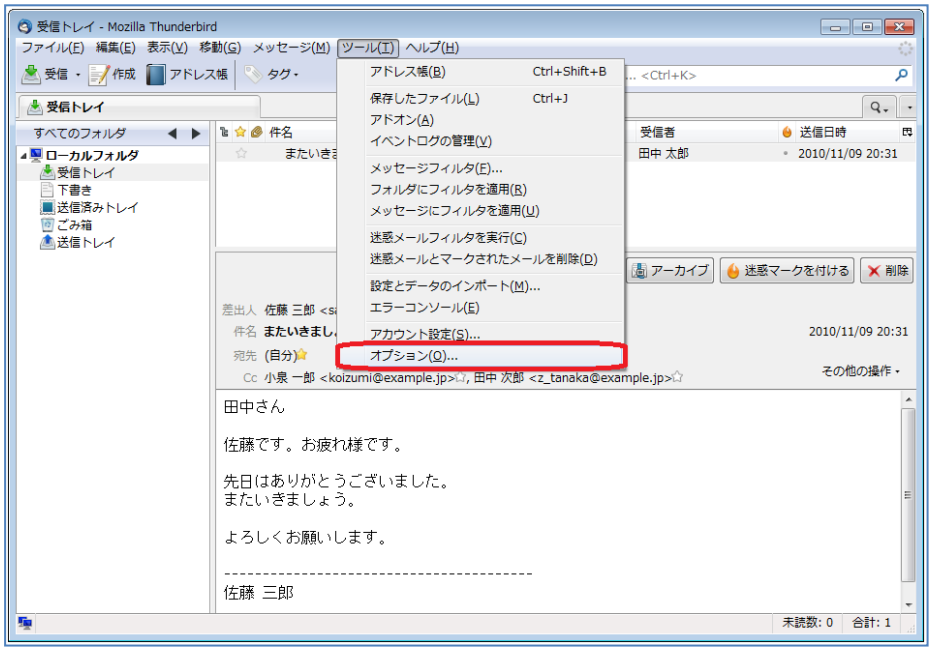


PGP/GPG 対応

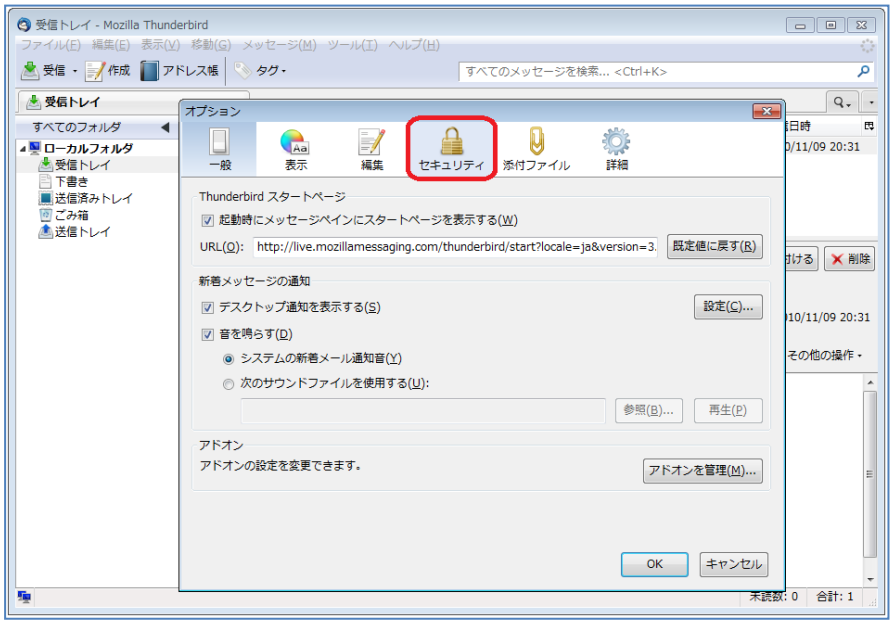
Mozilla Thunderbird は、PGP/GPG をサポートしていません。

迷惑メールフィルタの設定

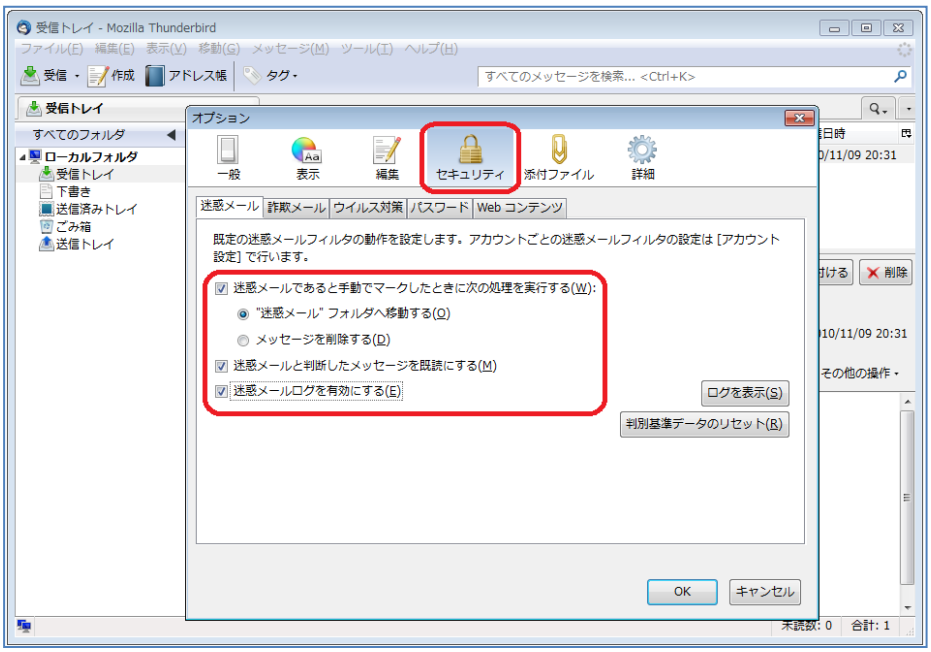
- メニューの「ツール」から「オプション」を選択する。



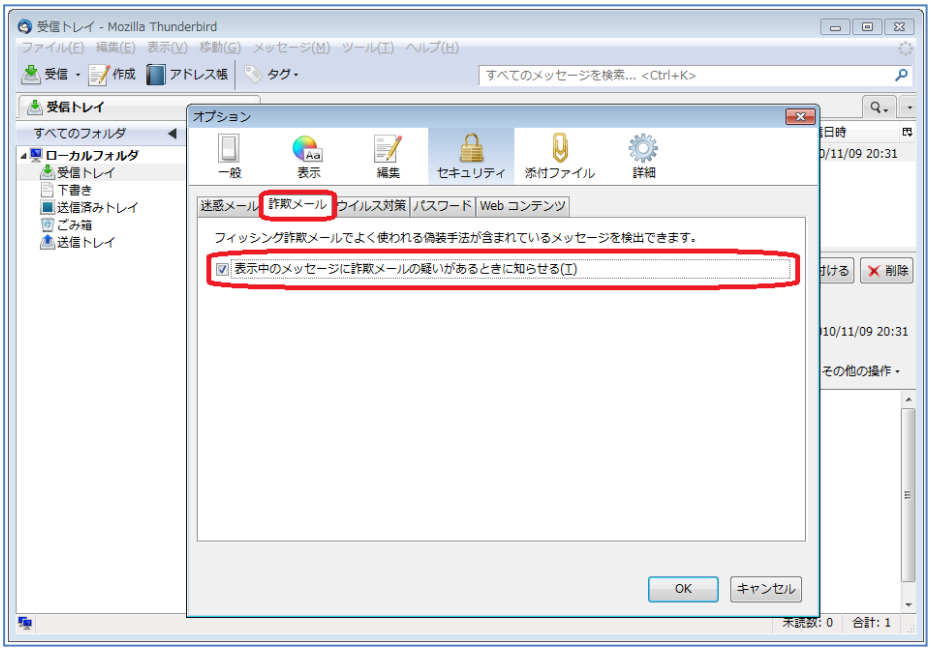
- 「オプション」ウインドウの「セキュリティ」を選択する。



- 「迷惑メール」タブを選択し、全ての項目のチェックを有効にする。

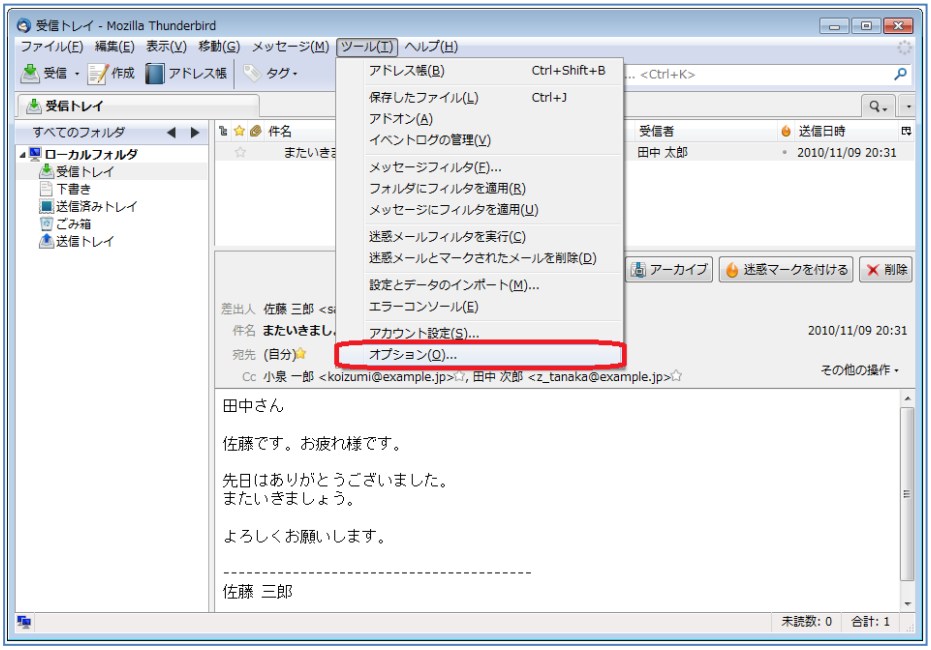


- 「詐欺メール」タブを選択し、「表示中のメッセージに詐欺メールの疑いがあるときに知らせる」のチェックを有効にする。

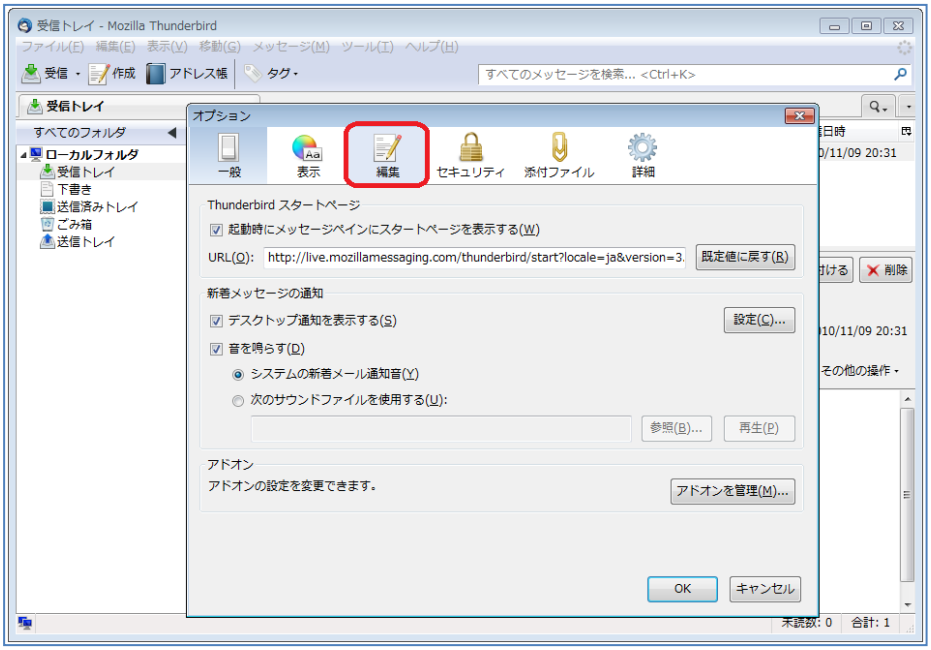


メール送信フォーマットに関する設定

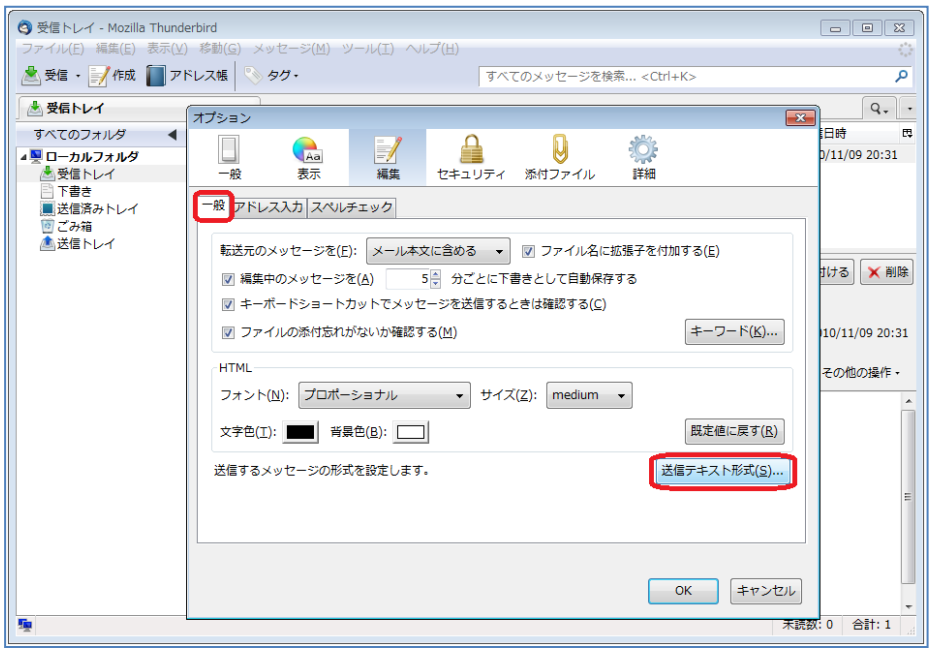
- メニューの「ツール」から「オプション」を選択する。



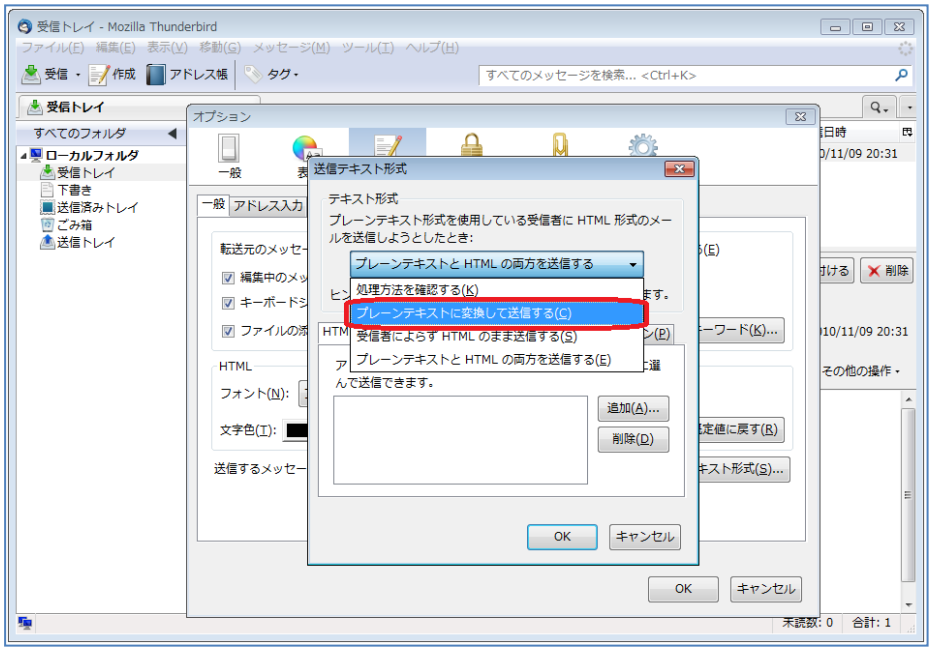
- 「オプション」ウインドウの「編集」を選択する。



- 「一般」タブの「送信テキスト形式」ボタンを押す。

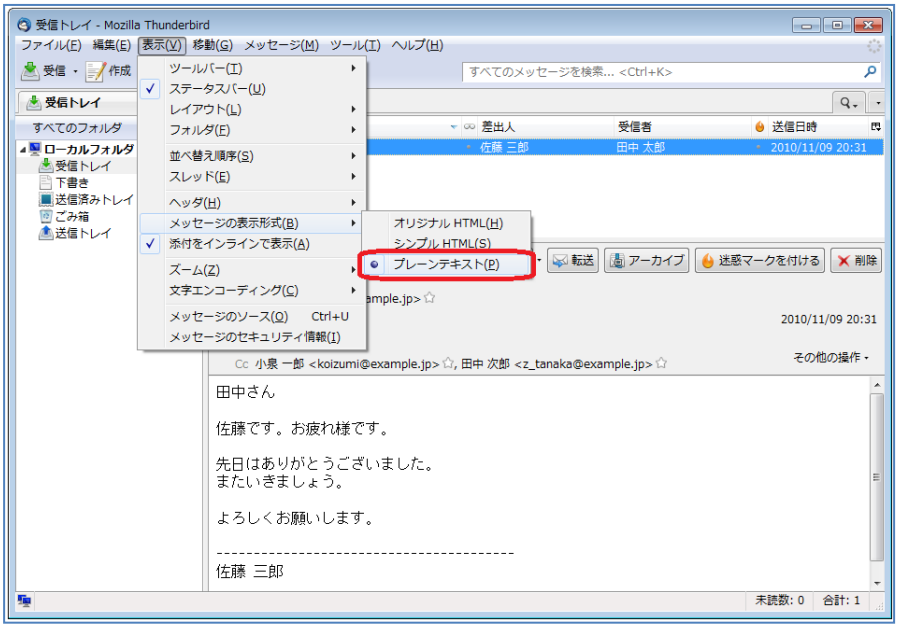


- 「テキスト形式」内のプルダウンメニューから、「プレーンテキストに変換して送信する」を選択する。



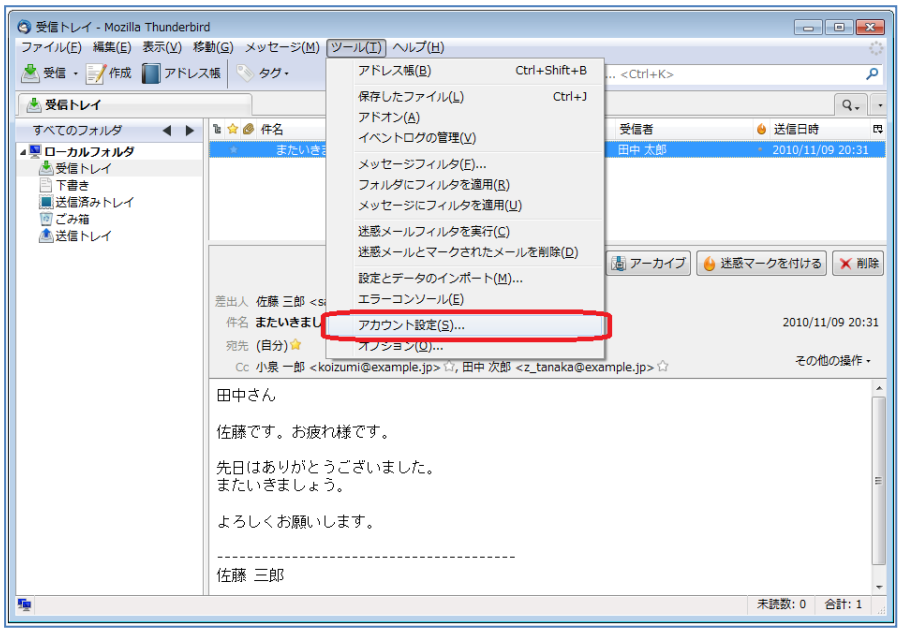
HTML メールの表示に関する設定

- メニューの「表示」から「メッセージの表示形式」を選択し、「プレーンテキスト」を選択する。

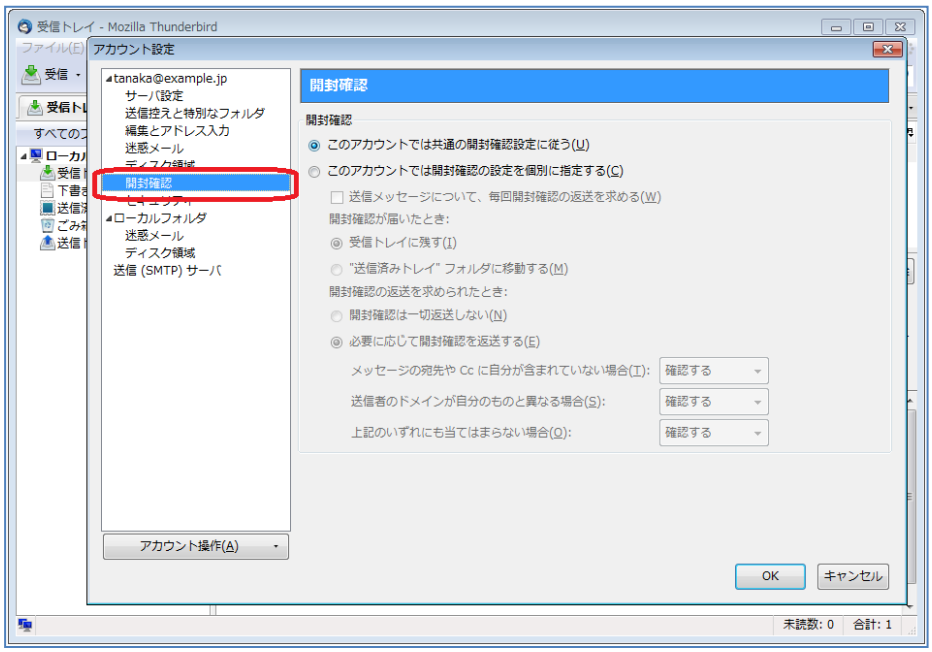


開封確認機能に関する設定

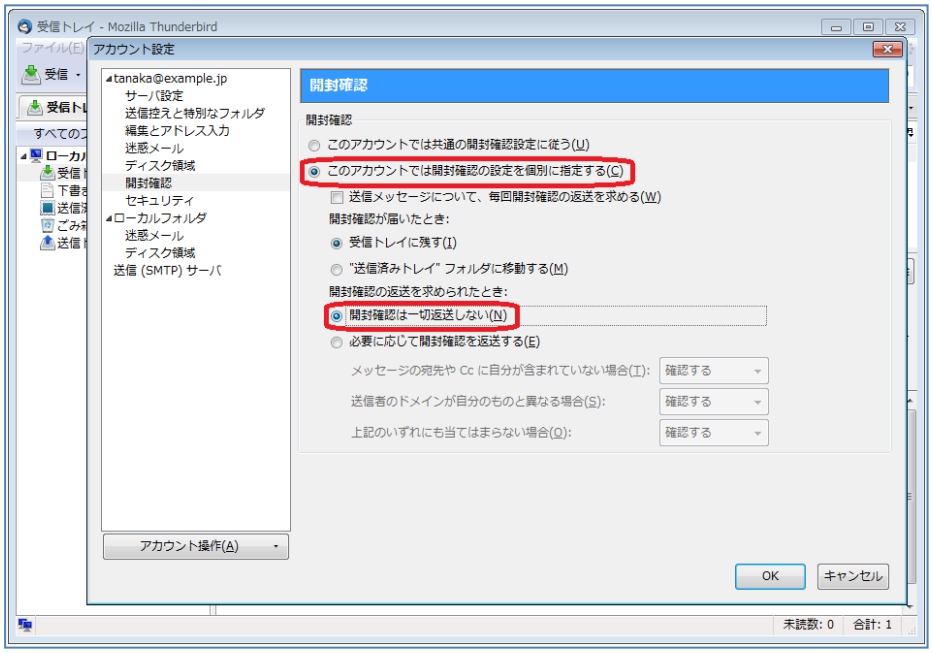
- メニューの「ツール」から「アカウント設定」を選択する。



- 「アカウント設定」ウインドウの左枠から「開封確認」を選択する。



- 「開封確認」内の「このアカウントでは開封確認の設定を個別に指定する」にチェックを有効にし、「開封確認は一切返送しない」のチェックを有効にする。



4.8 Gmail の設定

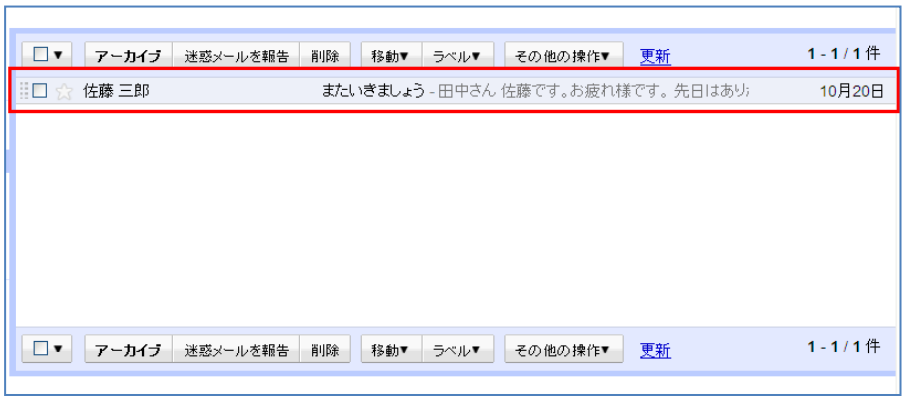
4.8.1 各設定

メール一覧で表示される情報の拡充

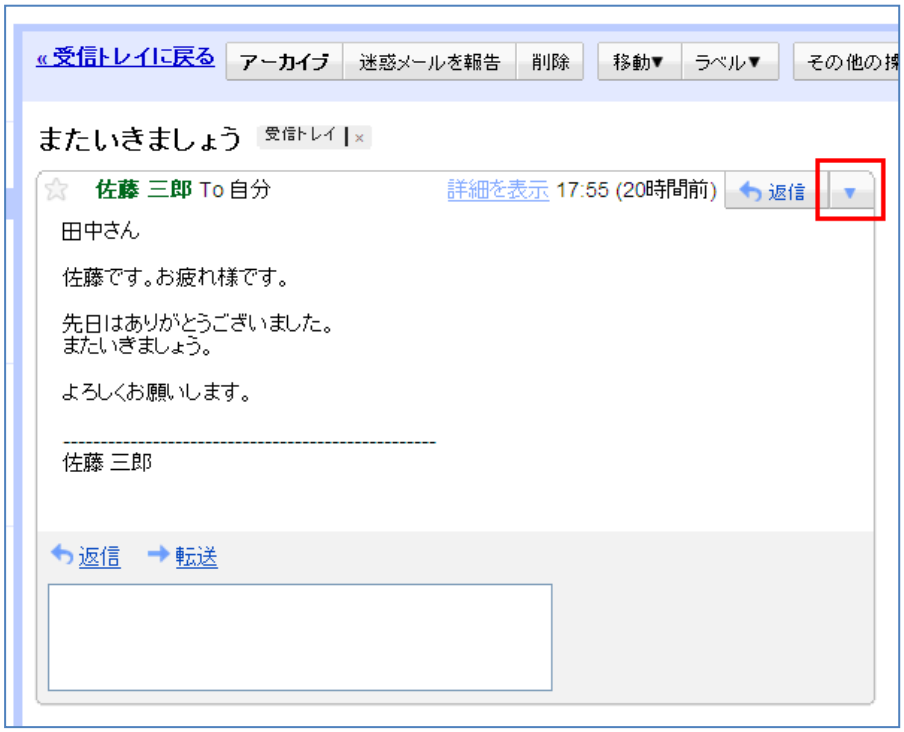
Gmail は、メール一覧で表示される情報を拡充することはできないため、設定はありません。

メールヘッダ情報の確認方法

- メールを選択する。

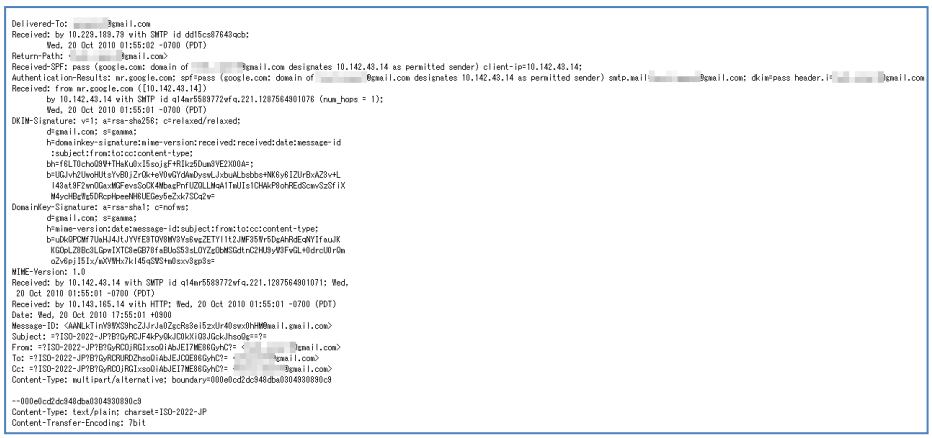


- ウインドウ枠の右上にある下向きの矢印（▼）を選択する。



- 「メッセージのソースを表示」を選択する。

- メールのヘッダ情報が別ウインドウで表示される。

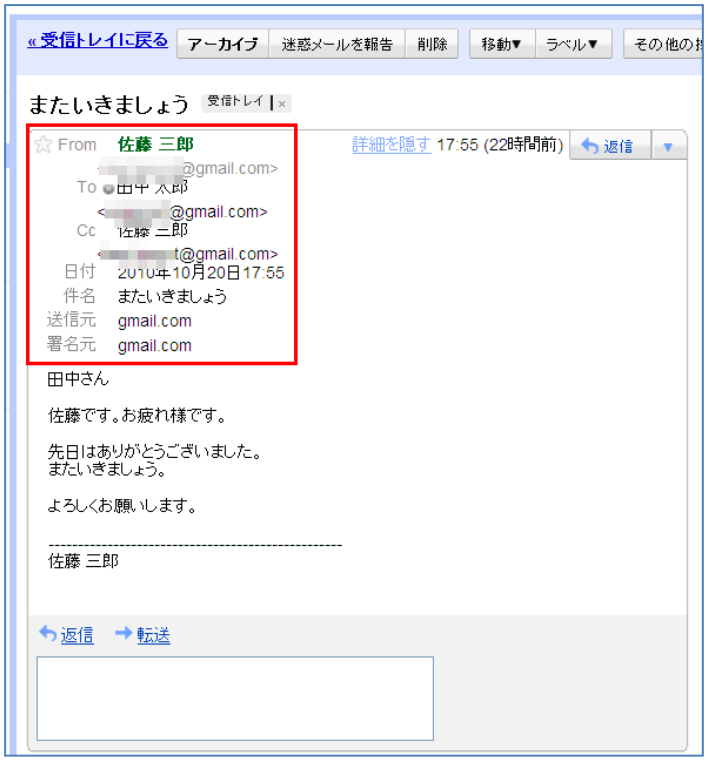


メールアドレスの表示形式の設定

Gmail は、メールアドレスの表示形式を設定することはできません。
※メール本文を表示し、「詳細を表示」を選択することで詳細なメール情報を表示することは可能です。

- メールを選択し、「詳細を表示」を選択する。

- メールの詳細情報が表示される。



S/MIME による署名メールの表示例

Gmail は、S/MIME をサポートしていません。

PGP/GPG 対応

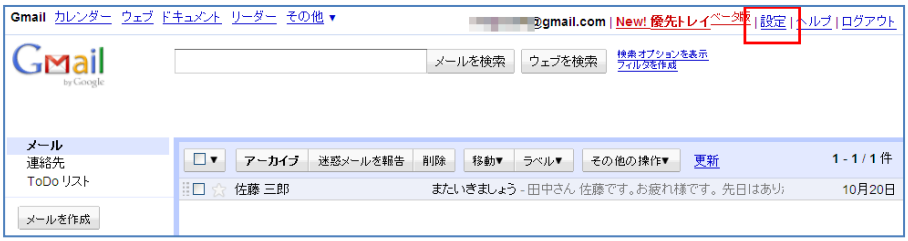
Gmail は、PGP/GPG をサポートしていません。

迷惑メールフィルタの設定

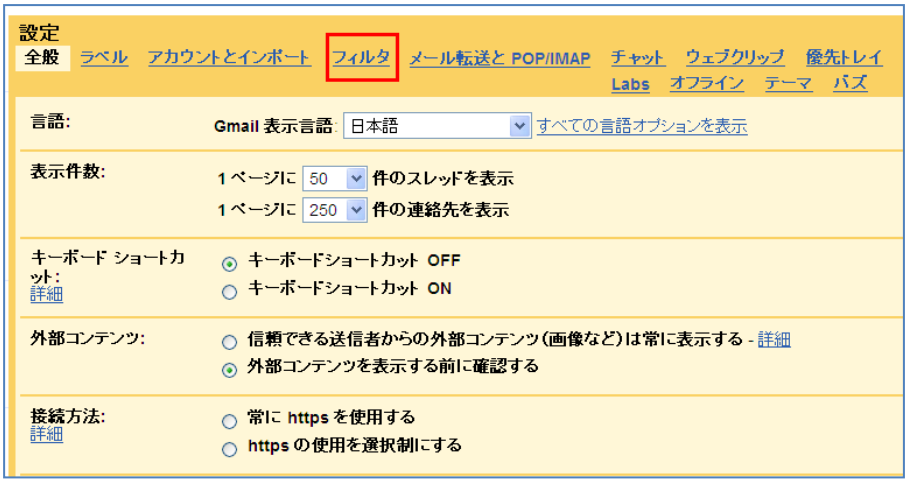
Gmail は、標準で迷惑メールフィルタ機能をサポートしていますが、機能の詳細を設定することはできません。
特定のメールアドレスを迷惑メールフィルタの対象から除外するホワイトリスト機能が提供されていますので、必要に応じて設定してください。

※ホワイトリスト機能は、送信元や宛先、件名やキーワードなどのフィルタ条件を指定することで、指定した条件に合致した受信メールを迷惑メールから除外することが可能である。
今回は送信元メールアドレスが「XXXXXXXXX@gmail.com」の場合に、迷惑メールフィルタから外す手順を紹介する。

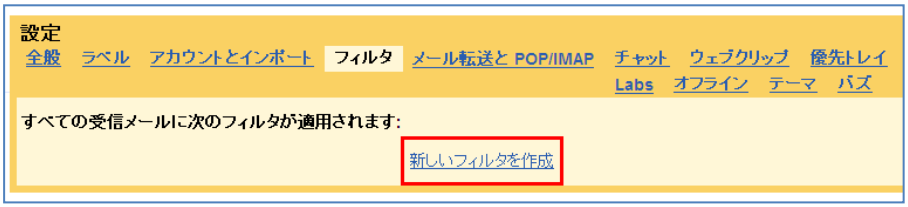
- 「設定」を選択する。



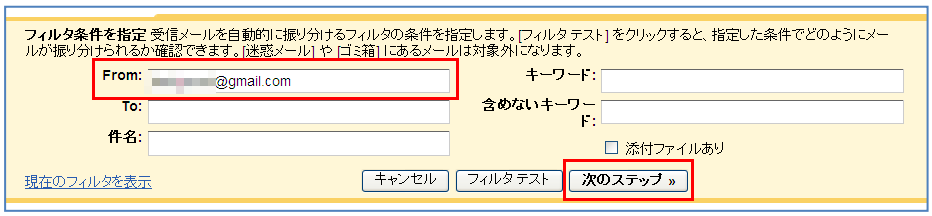
- 「フィルタ」を選択する。



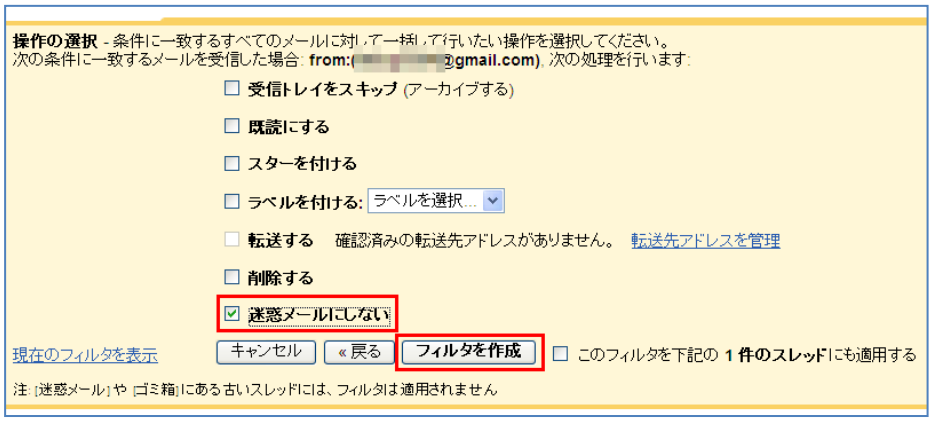
- 「新しいフィルタを作成」を選択する。



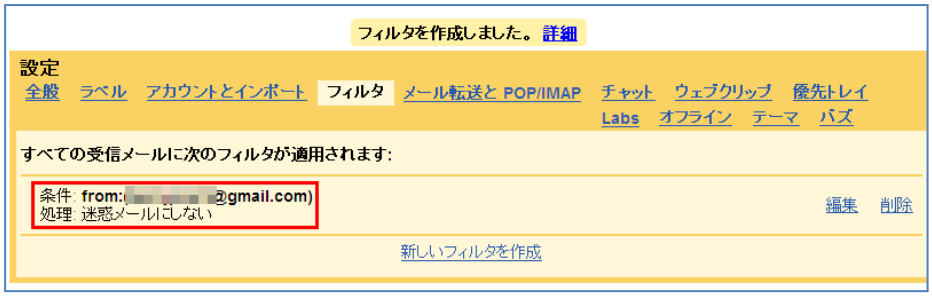
- 「From:」にフィルタするメールアドレスを入力し、「次のステップ」を選択する。



- 「迷惑メールにしない」にチェックし、「フィルタを作成」を選択する。

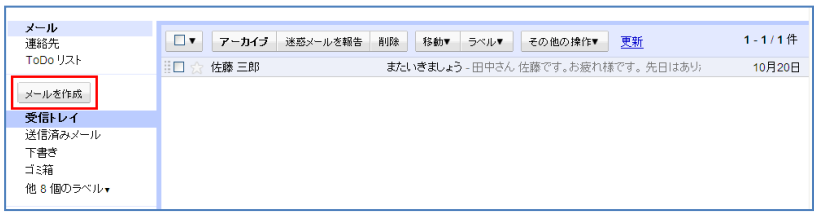


- 指定したフィルタが適用される。

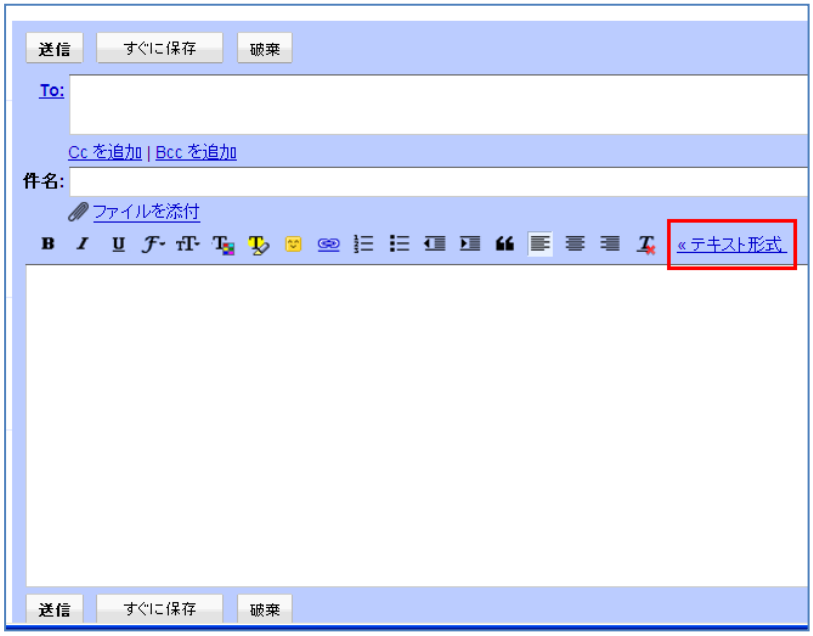


メール送信フォーマットに関する設定

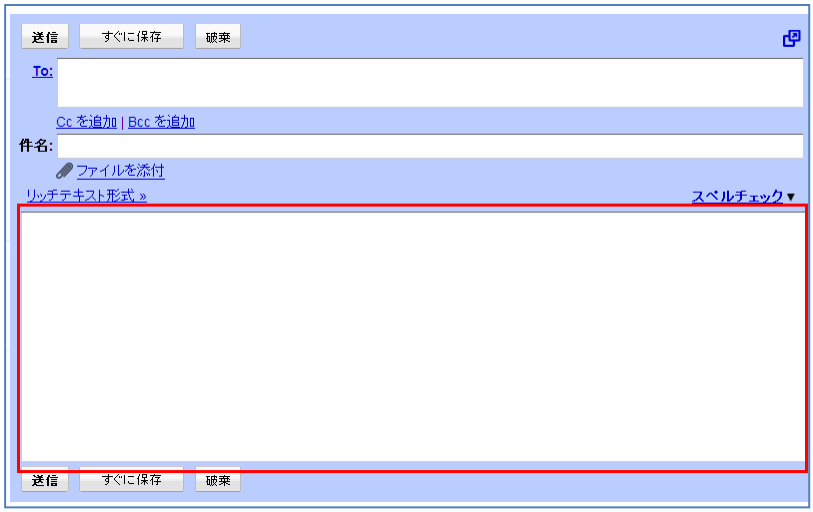
- 「メールを作成」を選択する。



- 「テキスト形式」を選択する。



- メール送信フォーマットがテキスト形式に変更される。

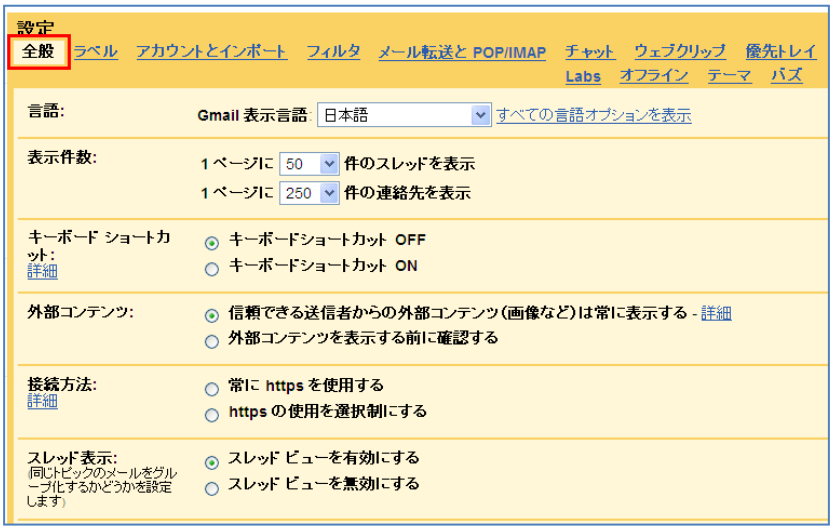


HTML メールの表示に関する設定

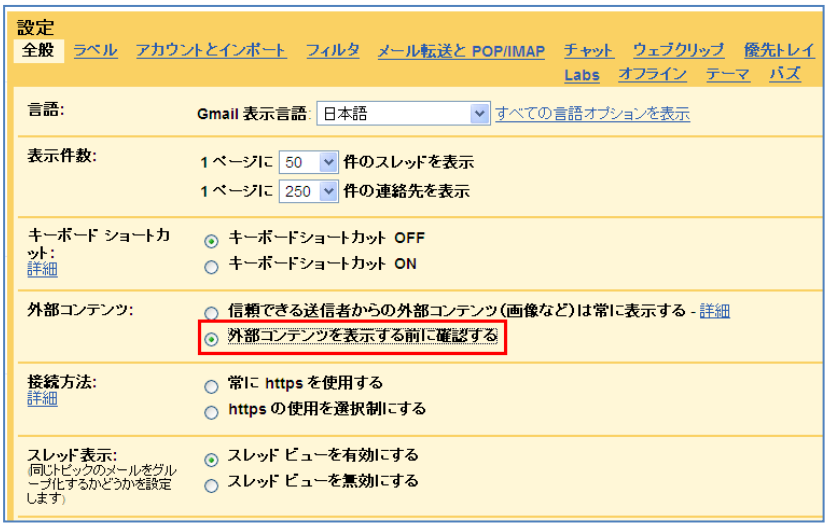
Gmail は、受信した HTML メールをテキスト形式で表示することができません。
ただし、リモート画像を表示する前に確認することは可能です。

- 「設定」を選択する。

- 「全般」を選択する。



- 「外部コンテンツを表示する前に確認する」にチェックを入れる。



開封確認機能に関する設定

Gmail は、開封確認機能を持っていないため、設定はありません。

4.9 Yahoo! メールの設定

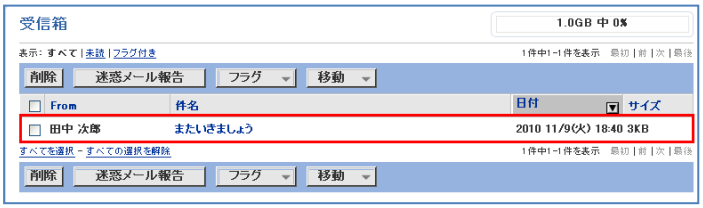
4.9.1 各設定

メール一覧で表示される情報の拡充

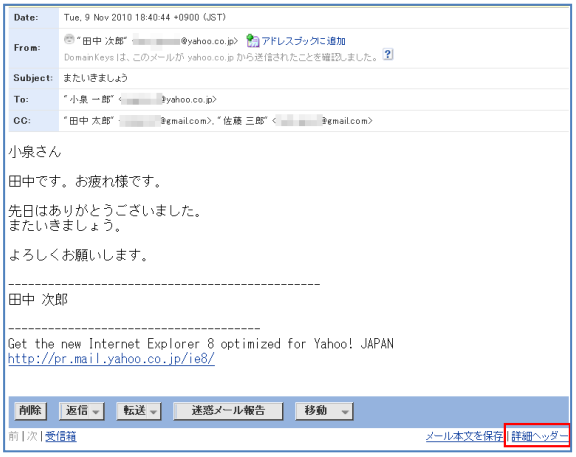
Yahoo! mail は、メール一覧で表示される情報を拡充することはできないため、設定はありません。

メールヘッダ情報の確認方法

- メールを選択する。



- ウインドウ枠右下の「詳細ヘッダ」を選択する。

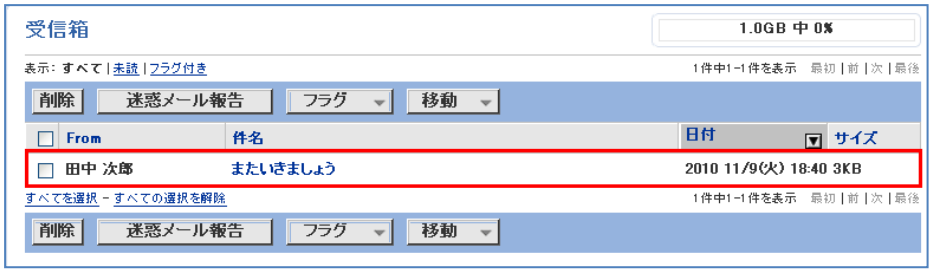


- メールのヘッダ情報が別ウインドウで表示される。

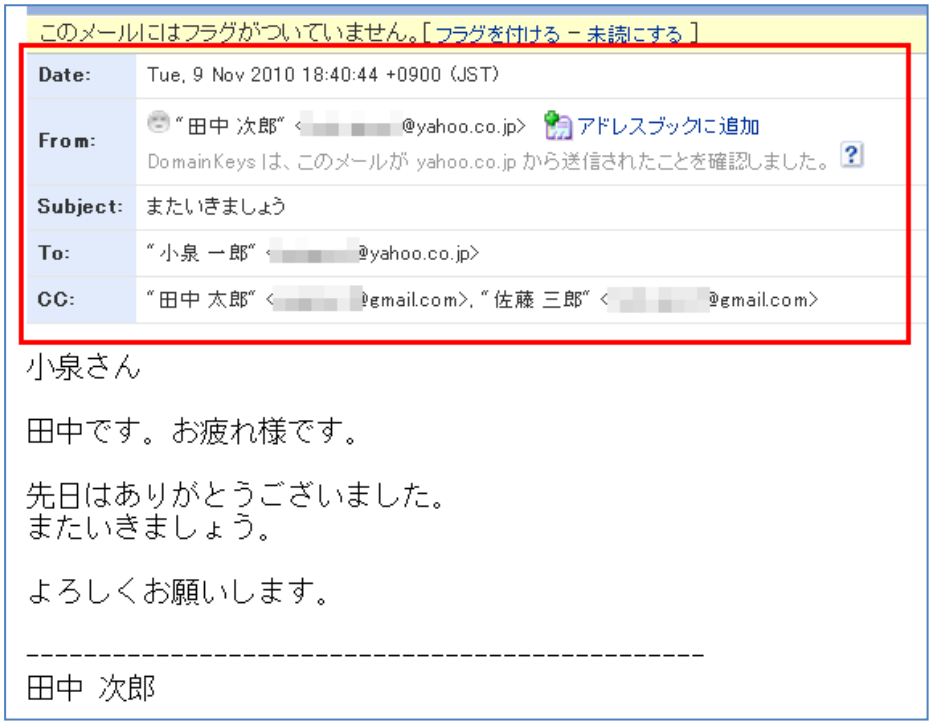
メールアドレスの表示形式の設定

Yahoo! mail は、メールアドレスの表示形式を設定することはできません。
※メール本文を表示し、「詳細を表示」をクリックすることで詳細なメール情報を表示することは可能です。

- メールを選択する。



- メールの詳細情報が表示される。



S/MIME による署名メールの表示例

Yahoo! mail は、S/MIME をサポートしていません。

PGP/GPG 対応

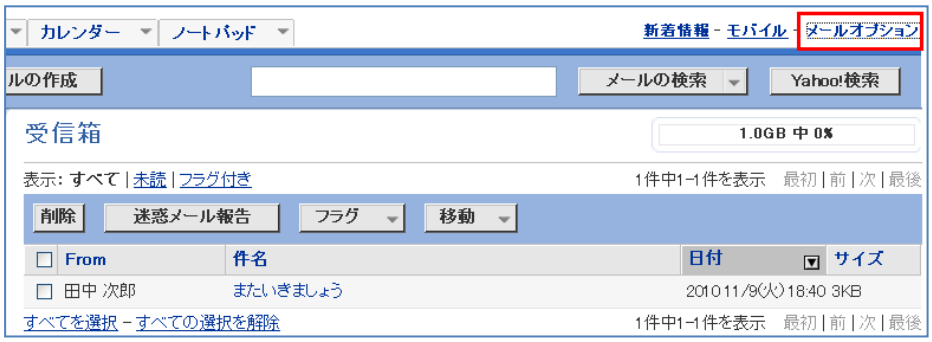
Yahoo! mail は、PGP/GPG をサポートしていません。

迷惑メールフィルタの設定

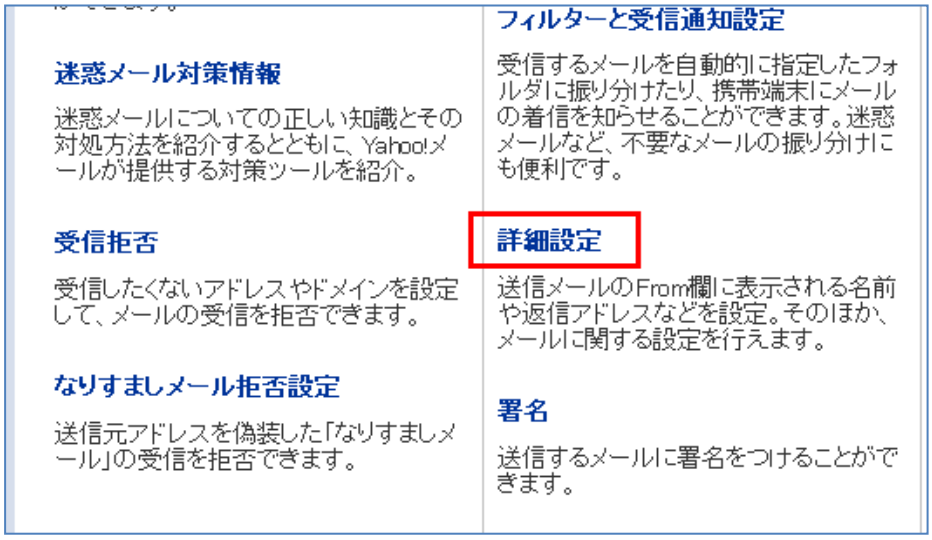
Yahoo! mail は、標準で迷惑メールフィルタ機能をサポートしていますが、機能の詳細を設定することは出来ません。

メール送信フォーマットに関する設定

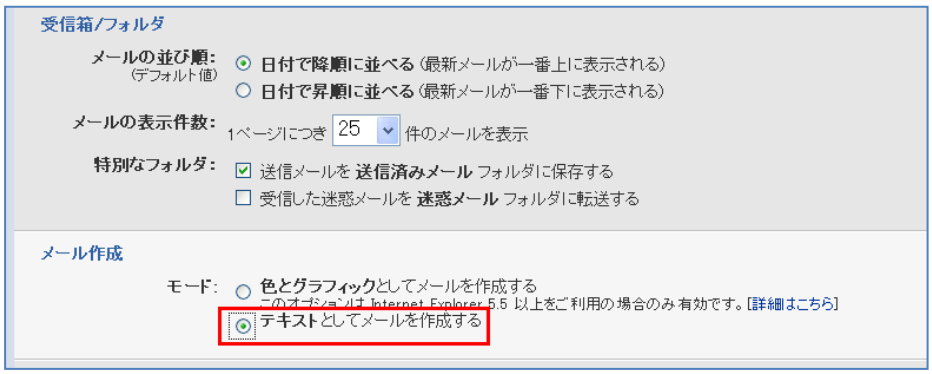
- 「メールオプション」を選択する。



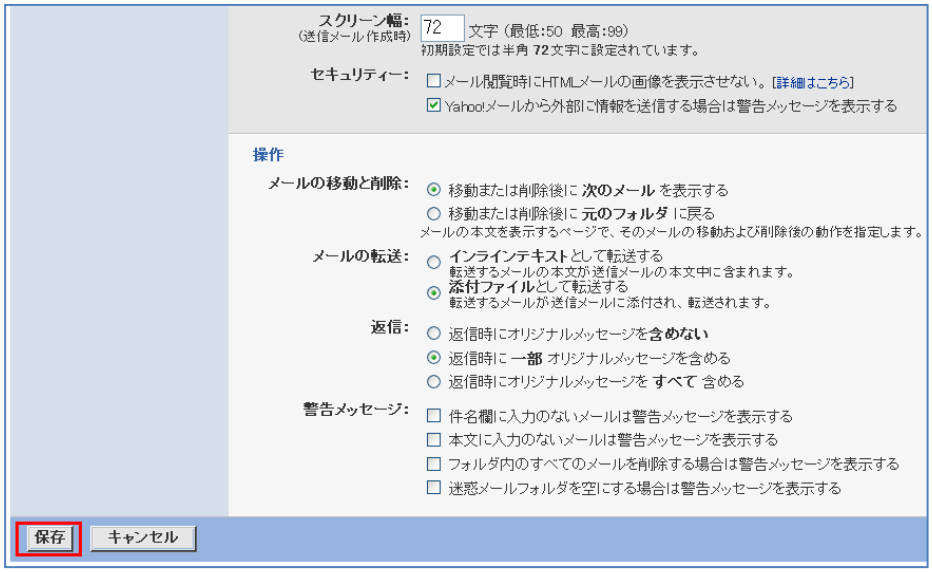
- 「詳細設定」を選択する。



- 「テキストとしてメールを作成する」にチェックを入れる。



- 「保存」を選択する。

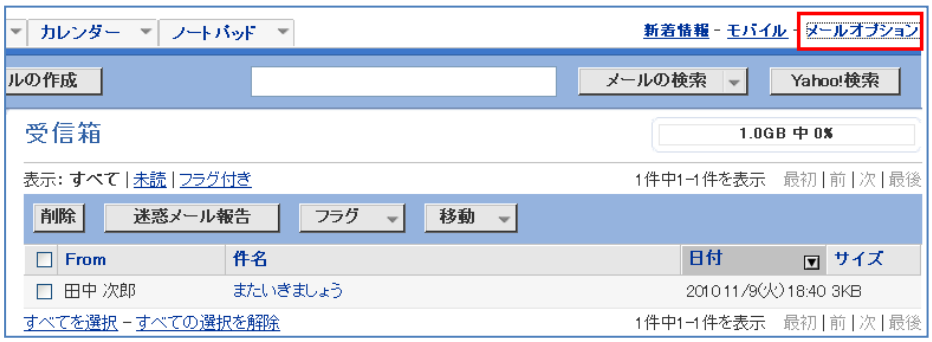


- 「設定が変更されました」のメッセージが表示される。

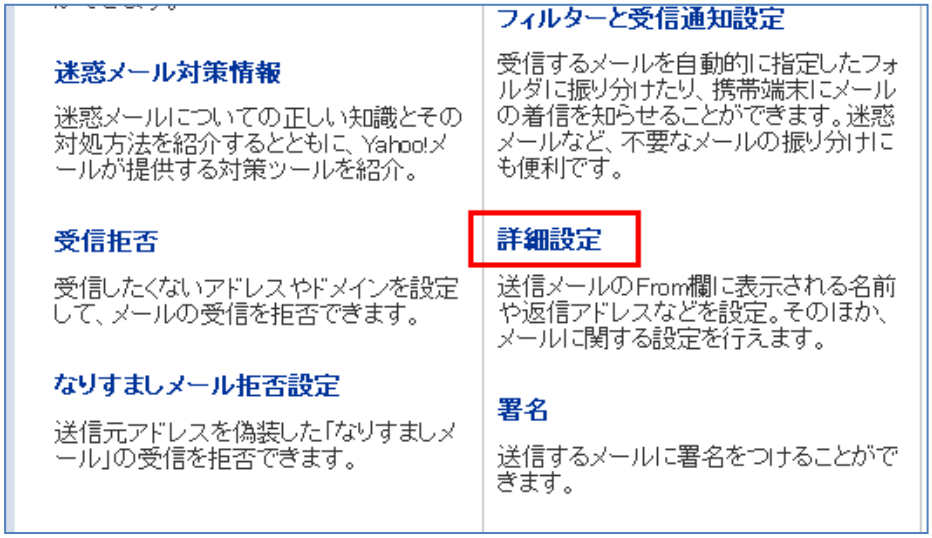
HTML メールの表示に関する設定

Yahoo! mail は、受信した HTML メールをテキスト形式で表示することができません。
ただし、画像を表示させないようにすることは可能です。

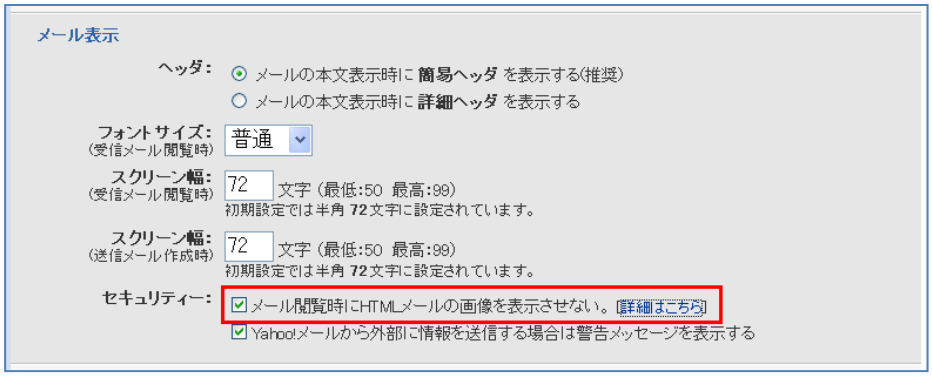
- 「メールオプション」を選択する。



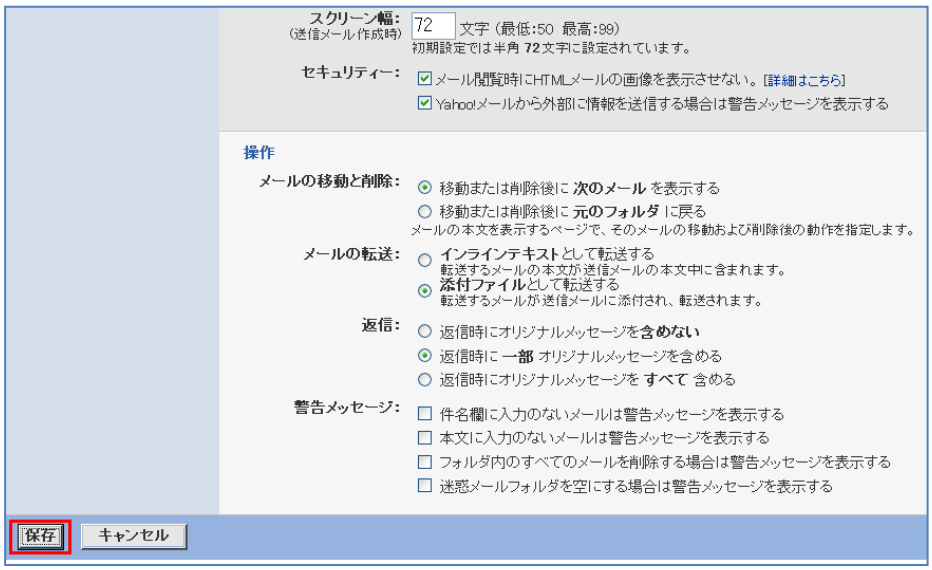
- 「詳細設定」を選択する。



- 「メール閲覧時に HTML メールの画像を表示させない」にチェックを入れる。



- 「保存」を選択する。



- 「設定が変更されました」のメッセージが表示される。

開封確認機能に関する設定

Yahoo! mail は、開封確認機能をサポートしていません。

5 用語説明

IMAP
インターネットメッセージアクセスプロトコル(Internet Message Access Protocol)は、メールサーバから電子メールを受信したり、メールサーバ上でメールを操作したりするプロトコル。主に利用される IMAP4 rev1 では、クライアントとサーバ間の通信に 143/tcp が使用され、RFC3501 にて規定されている。

MDA
メール配送エージェント(Mail Delivery Agent)は、メール転送エージェント(MTA)によって振り分けられた電子メールを別の MTA に送信したり、受信者のメールボックスに配送する機能。

MTA
メール転送エージェント(Mail Transfer Agent)は、電子メールを宛先アドレスに配送する機能のことであり、メールサーバ機能のなかで中心的な機能を持つ。

MUA
メールユーザエージェント(Mail User Agent)は、電子メールを読み書き、メールサーバへの送信、メールサーバからの受信等を行うソフトウェア。いわゆる電子メールソフト(もしくはメールクライアント)のこと。

OP25B
アウトバウンドポート 25 ブロッキング(Outbound Port 25 Blocking)は、迷惑メール送信者が増えたことに対して ISP 側で採用された対策で、ISP がユーザに割り当てた IP アドレスから ISP 外部への SMTP 通信を遮断する。SMTP 通信が TCP の 25 番ポートを利用するため、この名称が使用されている。

PGP
プリティーグッドプライバシー(Pretty Good Privacy)は、Philip Zimmermann が開発、公開した暗号ソフトウェア。公開鍵暗号方式を採用しており、電子メールの暗号化、電子署名を行うことが可能である。

POP before SMTP
ポップビフォアエスエムティーピー(POP before SMTP)は、SMTP 認証が策定される以前に策定されたメール送信者の認証に利用される仕組みで、SMTP によるメール送信の前に POP の認証機能を利用してユーザ認証を行う。

POP/POP3
ポストオフィスプロトコル(Post Office Protocol)は、メールサーバから電子メールを受信するためのプロトコル。現在は、改良された POP3（POP version3） が主に使用されている。通常、クライアントとサーバ間の通信には 110/tcp が使用され、RFC1939 にて規定されている。

S/MIME
エスマイム(Secure Multipurpose Internet Mail Extensions)は、電子メールの暗号化と電子署名に関する国際規格である。公開鍵暗号方式を採用しており、電子メールの暗号化、電子署名を行うことが可能である。

SMTP
簡易メール転送プロトコル(Simple Mail Transfer Protocol)は、電子メールを転送するプロトコル。通常、クライアントとサーバ間の通信には 25/tcp が使用され、RFC5321 にて規定されている。

SMTP 認証

SMTP 認証は、SMTP を利用したメール配送を行う際に、送信者がそのメールサーバを利用する権限があるかの認証機能を追加した仕様。

SSL/TLS

SSL はセキュアソケットレイヤー(Secure Sockets Layer)の略であり、TLS はトランスポート層セキュリティ(Transport Layer Security)の略である。
SSL 及び TLS は、安全性を要求される通信を行う場合に利用するためのプロトコルである。
SSL はもともと、Web における通信の安全性の確保のためにネットスケープコミュニケーションズ社によって開発されたものである。その後、IETF による標準化作業が行われ、SSL の後継として RFC2246 として TLS1.0 が公開された。
なお、現在では、TLS1.2(RFC5246) となっている。

開封確認

開封確認(Disposition Notification)は、送信した電子メールが受信者に届いたかどうかを確認できる機能。RFC3798 にて規定されており、この機能を利用したメールが到着しても「開封確認を送り返す必要は無い」となっている。