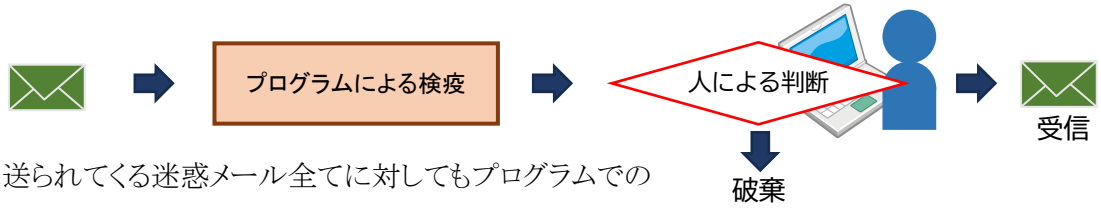
# 悪意のメール送信者に騙されない為に

## メールが手元に届く前に、ビジュアルで「いる」「いらない」を切り分けられる

情報セキュリティ脅威の多くは、メールを通じたマルウェアの仕込まれた添付ファイルの配布や、マルウェアを感染させる目的で作成された WEB サイトへのアクセスです。

### ❑ 一般的なメール受信処理

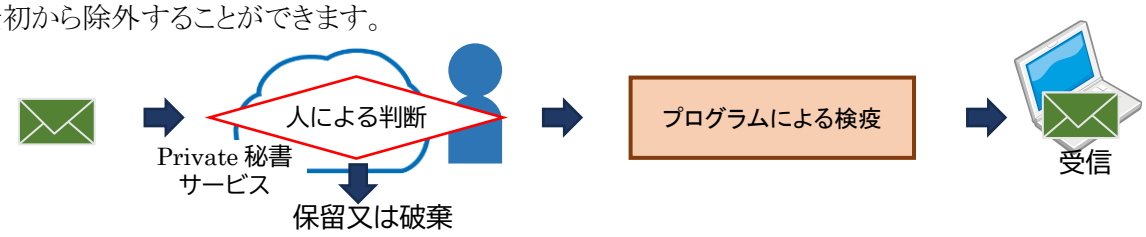
誰が送ったメールでも一旦は受け取る必要があり、ウィルス対策プログラムでメールを検疫した後、受信者の手元へ届きます。手口の巧妙さから、プログラムでは完全に脅威を取り除くことができない場合もある事から、最後に受信者自身に「受け入れる」か「拒否する」かの判断が要求されます。




大量に送られてくる迷惑メール全てに対してもプログラムでの検疫は働き、最終的に受信者の手元まで届きます。

### ❑ Private 秘書サービスを使ったメール受信処理

Private 秘書サービス は、最初に人による判断をし、「いる」メールだけを受け取り、「いらない」メールは、最初から除外することができます。



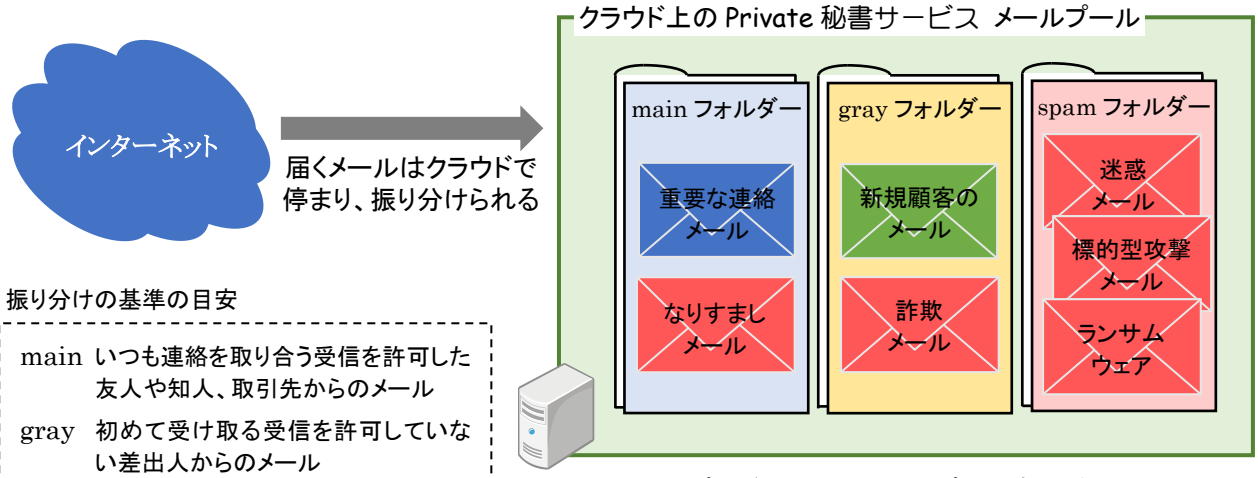

「Private 秘書サービス」は、メールを取捨する為に必要となる、様々な情報と手段を提供します。

### ❑ Private 秘書サービスを利用することで

インターネットから届くメールには危険なものがたくさんあります。
Private 秘書サービスは、これらの脅威を察知してビジュアル的に利用者の視覚へ訴えます。
専門的な知識のない利用者であっても、「緑:信頼されている」「赤:信頼されていない」から容易に注意喚起され、インターネットの先にいる悪意の攻撃者の罠にかからずに、本当に必要なメールだけを取捨して PC やモバイルで安全にメールを受け取る手助けをします。

まずは、緑 と 赤 の表示を手掛かりに、判断に困ったらアドバイザー(後述)の詳細画面で送信元アドレスや送信元 Hostを細かく吟味することで、騙されることの無い安心できるメール受信環境をご利用下さい。

# 1. メールはクラウドで停まり、内容に応じて 3 種類に振り分けられる

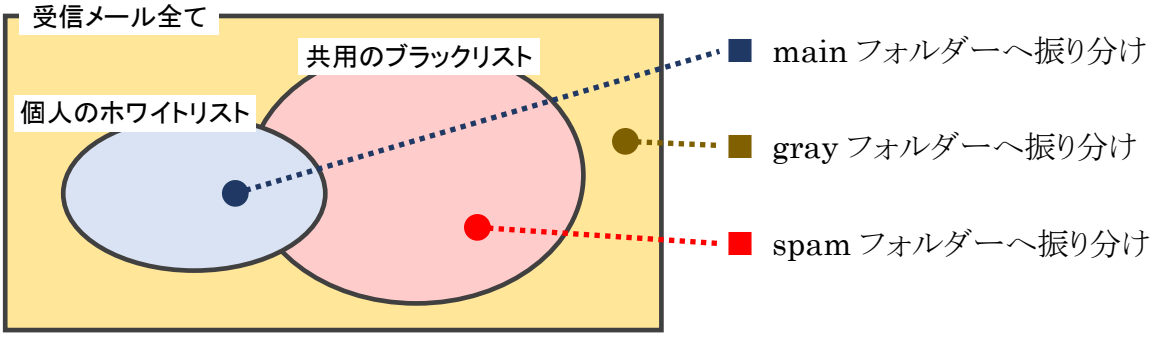



振り分けの基準の目安

| | |
|---|---|
| main | いつも連絡を取り合う受信を許可した友人や知人、取引先からのメール |
| gray | 初めて受け取る受信を許可していない差出人からのメール |
| spam | 危険なハイパーリンクを含む注意が必要なメールや迷惑メール |

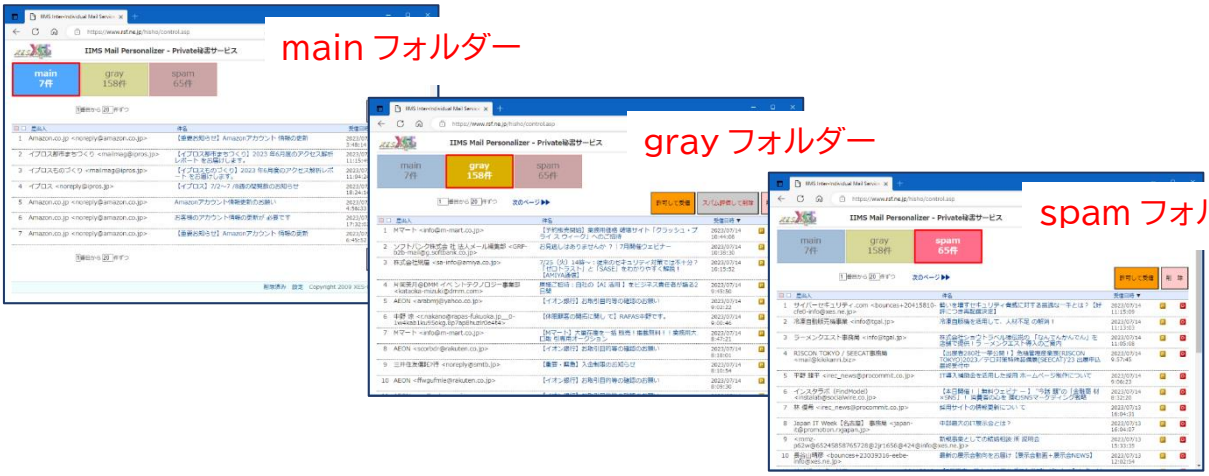
gray フォルダーや spam フォルダーに振り分けられたメールを受信許可して受信すると、次回からは main フォルダーへ届きます。

## 利用者共用のブラックリストと、個人のホワイトリストを使って、届くメールを自動振り分け




個人のホワイトリストは、自分が受信許可した差出人（From）アドレスのリストです。
共用のブラックリストは、利用者が協力して登録をしている、悪質なハイパーリンク先アドレスのリストです。
インターネットから届いたメールは、まず最初に個人のホワイトリストと照合され、ヒットしたメールは main フォルダーへ振り分けられます。ヒットしなかったメールは、次に共用のブラックリストと照合され、ヒットしたメールは spam フォルダーへ、ヒットしなかったメールは gray フォルダーへ振り分けられます。

以下は、受信メールが各フォルダーへ振り分けられている状態の画面です。



利用者は、まず main フォルダーをチェック、次に gray フォルダーをチェック、余裕があれば spam フォルダーもチェックし、本文を確認して必要なメールだけを選択して受信操作をします。
メール本文の閲覧は、WEB サイトへのハイパーリンクとファイルのダウンロードリンクが無効となった、安全な環境が提供され、閲覧操作からマルウェアへの感染などの心配はありません。

## 2. 危険なハイパーリンクには、警告がでる

メール本文に記載の、WEB ページへのハイパーリンクは、画面に表示されないものも含めて、全て抽出して表示することができます。

### ❑ 危険なハイパーリンクを含まないメールの場合


### ❑ 危険なハイパーリンクを含むメールの場合


main フォルダーでは、受信メールの本文中に危険なハイパーリンクを検出した場合、メールを開いた時点で「このメールには注意して下さい」と警告表示が出ます。

※ Private 秘書サービスの受信メール振り分け処理は、第一条件として受信メールの From 句に記載のメールアドレスが、「受信許可」に登録されたものを対象とします。次にブラックリストのチェックを行ないます。
その結果、ブラックリストにヒットしても、自分にとって必要なものは、「受信許可」として登録することで main フォルダーに必ず振り分けることができます。

# 3. メールの受信ルートと、受信メールに対する利用者全体の挙動を学習し、届くメールを評価してアドバイスを提示する

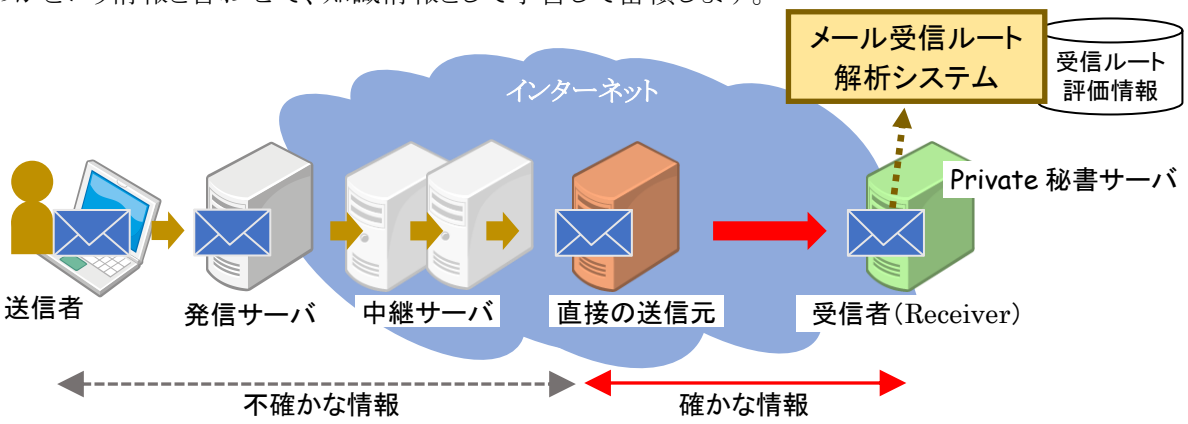
## ❑ main、gray、spam 振り分け方式の限界

main、gray、spam 振り分け方式は、「受信許可」のあるアドレスを詐称したなりすましメールが main フォルダーへ振り分けられてしまうことを防ぐことができません。また、WEB サイトへの外部リンクの記載のないメールは、警告を出すこともできません。

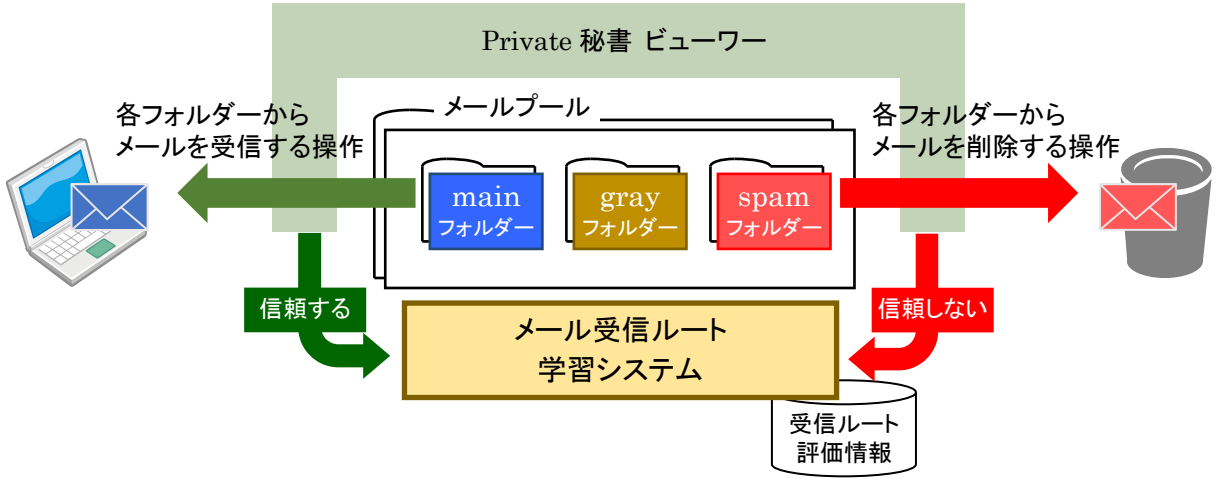
## ❑ メールの受信ルートを解析、利用者の挙動と合わせた情報として活用

インターネットから届くメールは、様々なサーバを経由して自システムに届きます。
受信したメールがどのサーバを経由して届けられたかは、メールヘッダーを解析することで情報を得られます。しかし、それは自サーバと直接通信をしたサーバまでで、それ以前のメール搬送ルートについては、容易にメールヘッダーの改ざんができることから、信用に値するものではありません。

Private 秘書サービスでは、直近の送信元サーバの情報を詳細に取得し、送信者（From や Sender）の情報と共に記録し、メールを受け取った本人が、そのメールに対して「受信」したのかあるいは「破棄」したのかという情報と合わせて、知識情報として学習して蓄積します。



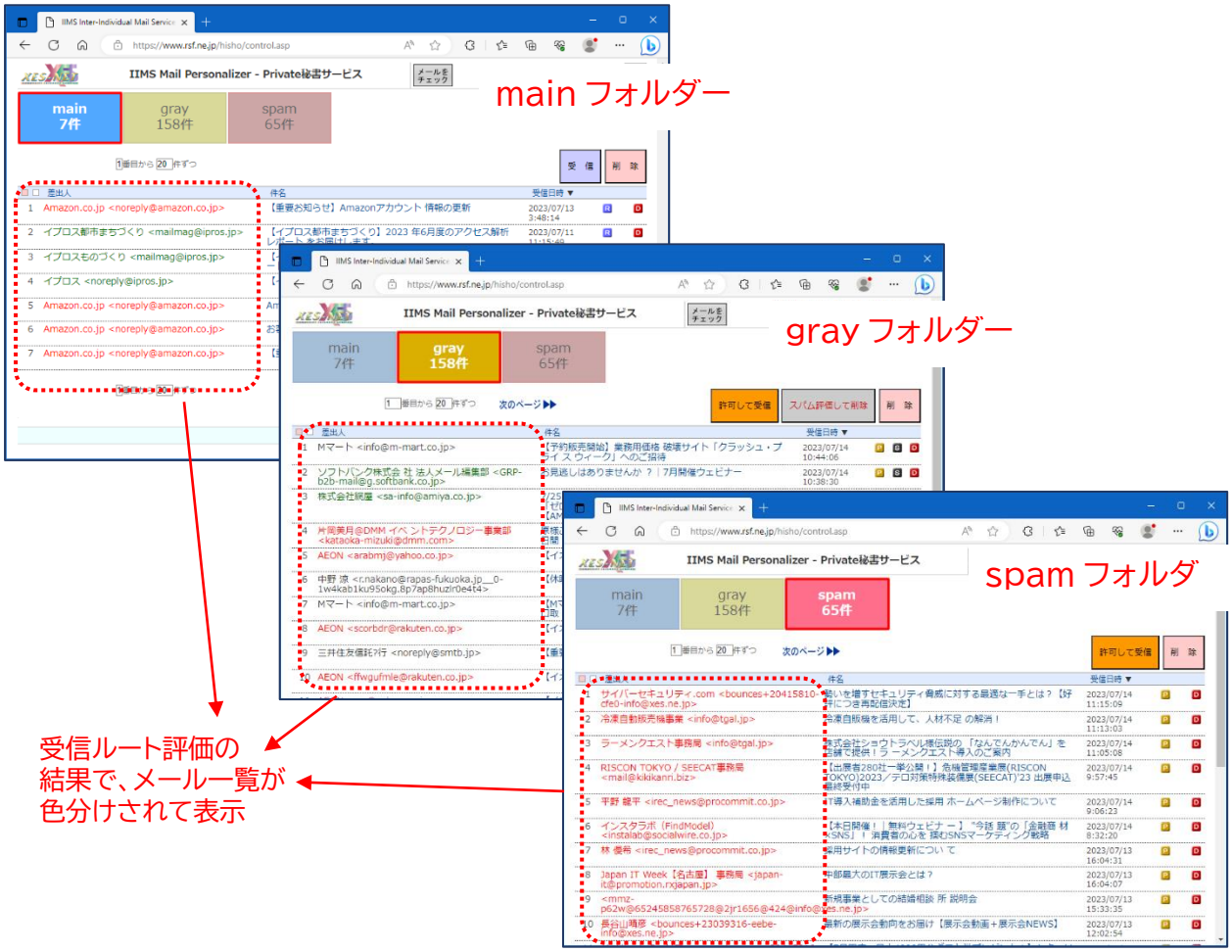

メールの受信ルート毎に、利用者の操作を学習して記録します。
自身の操作結果は全体にも反映され、他の利用者の情報とともに利用されます。



## ❑ 届いたメールを評価し、アドバイスを提示

蓄積した受信ルートの評価情報を使い、届いたメールを評価してアドバイスを提示します。
評価の内容は、直接送信してきたサーバの評価、送信者（Sender）の評価、差出人（From）の評価などを総合的に判断して、**「信頼できる」**、**「信頼できない」**の判断を下し、根拠となるスコアの詳細も提供します。
これにより、新しく届いたメールであっても、どのサーバから送られてきたのか、誰が送ったのかなど、既に受け取った実績のある先人の評価を生かすことで、問題のあるメールを容易に見つけ出す手助けをします。

以下は、**「メール受信ルート表示」**を有効にした場合の各フォルダーの画面です。



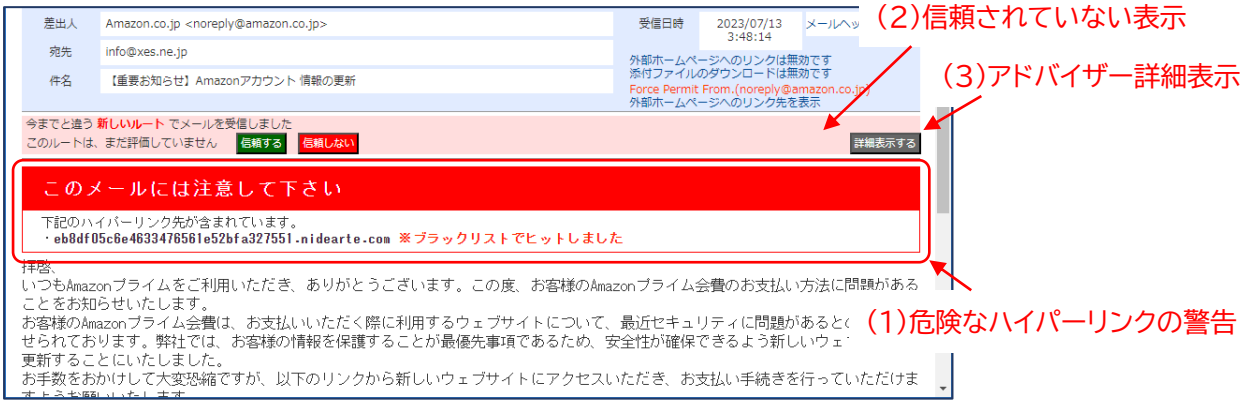

メールの差出人欄が、緑のメールは総合的に**「信頼されている」**と評価されたメールで、赤のメールが**「信頼されていない」**と評価されたメールになります。黒のメールは、まだ評価されていないか、評価の対象外のメールになります。

評価の基準は、自分の評価、共同利用者の評価の順で、Sender、From、中継 Host、Senderドメイン、Fromドメインの**「信頼されている」**、**「信頼されていない」**を数値化して評価の判断に用いています。
また、直接メールを送ってきている中継 Host については、受信の回数、DNS の正引き・逆引きの成否などを情報として開示しています。

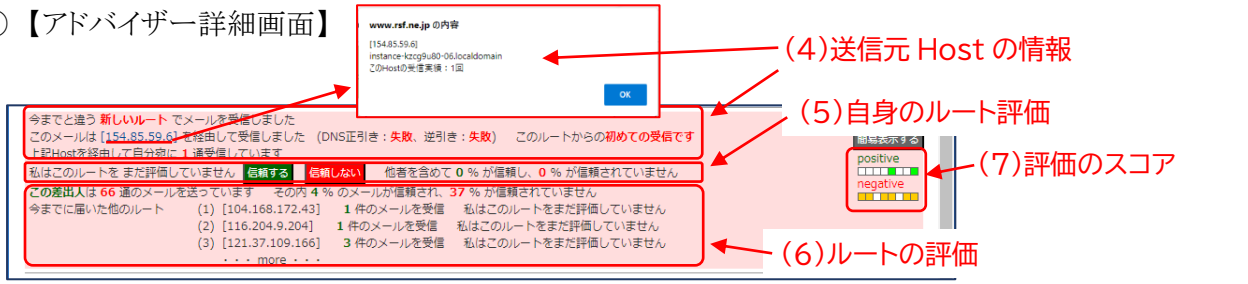
# 4. 届いたメールの「良し」、「悪し」を判断して、なりすましメールに騙されない

Private 秘書サービスの提供する様々なシグナルを確認しながら、危険なメールを洗い出します。

① 【メール詳細画面】




② 【アドバイザー詳細画面】




## (1) 危険なハイパーリンクの警告に注意する

「このメールには注意して下さい」と表示されたメールは、危険なハイパーリンクが含まれている場合があります。十分確認してから受信操作して下さい。

なお、ブラックリストは共有で運用されているものなので、自分にとって危険で無くともブラックリストに登録されている場合があります。

## (2) 信頼されていない表示

該当領域の赤表示は、アドバイザーによる「信頼されていない」と判断が下されたメールであることを示します。

## (3) アドバイザー詳細表示

クリックすると、「②アドバイザー詳細画面」が表示されます。

## (4) 送信元 Host の情報

メールを送信してきた SMTP サーバの情報を示します。IP アドレス、DNS 正引き・逆引きの結果が表示され、IP アドレスをクリックすると、対応するホスト名と受信回数が表示されます。

DNS 正引き・逆引きの結果が失敗となっている Host は注意が必要です。また、成功となっていてもホスト名が送信者とは関係のない海外のドメインであったり、不審なドメインである場合は注意が必要です。

## (5) 自身のルート評価

「信頼する」または「信頼しない」をクリックして、自分の評価を投票できます。
また、メールを受信・削除する操作をした場合も「信頼する」「信頼しない」評価が投票されます。

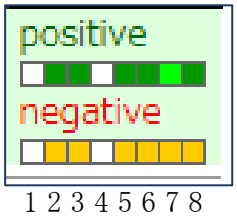
## (6) ルートの詳細評価

今までに受信したメールの件数と、信頼されている・いない割合が表示されます。
また、同じ送信者から別の Host を通じて受信している場合は、その IP アドレスが表示されます。既に受信実績のある IP アドレスとは全く違う IP アドレスが表示されている場合は注意が必要です。

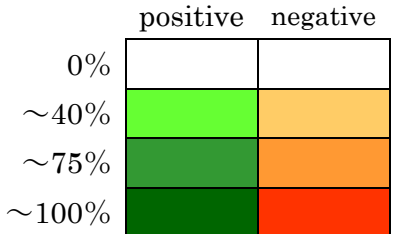
## (7) 評価のスコア (PC 版ビューワーのみ)

positive(信頼されている)と negative(信頼されていない)の各数値を以下のルートについて評価の度合いを計算し、色を付けて表示します。

スコア表示例




信頼度




1 Sender(実送信者)から自分宛の信頼度
2 From(差出人)から自分宛
3 Host(メールサーバ)から自分宛
4 Sender(実送信者)から全体宛
5 From(差出人)から全体宛
6 Host(メールサーバ)から全体宛
7 Sender(実送信者)ドメインから全体宛
8 From(差出人)ドメインから全体宛

評価の重み大 ↓ 小

白が 0%で、数値が大きくなるほど色が濃くなり、ビジュアル的に確認ができます。
また、マウスをスコアに合わせると、詳細な数値が表示されます。

「(5) 自身のルート評価」でカウントされた数値が最も優先されます。自身でまだ評価をしていない場合は、システムを利用する別の利用者の評価の総意を基に数値が決まります。
「1 Sender(実送信者)から自分宛」から順に positive と negative の数値を比較し、最終的にこのメールを「信頼できる」か「信頼できない」の判断が下され、システムからのアドバイスとして提示されます。
「信頼できない」と判断された場合は、「(2) 信頼されていない表示」の様な赤表示となります。

以上の各項目を参考に、メールの「良し」、「悪し」を判断する手助けとして下さい。

## ❑ 注意するメールの例

### ① メール本文から判断して、送信元のアドレスがおかしい


DNS の正引きが成功している為、送信者は正規の手順でメールを送信してきていると確認できます。しかし、メール本文から推察して、送信者メールアドレスのドメインが、「.cn：中国」はあり得ないと判断できます。

以下は、三菱 UFJ 銀行からの本物のメールで、DNS 参照、メールアドレスなど違和感がありません。


外部リンクにも、特にもおかしなものは含まれていません。

② なりすましたアドレスからのだますメール


送信元アドレスは「info@Amazon.co.jp」となっていますが、DNS の正引き、逆引き共に「失敗」となっています。これは、メールを送信してきた Host（173.82.212.131）が、mail0.Amazon.co.jp を騙ってメールを送信した為で、実際にこの Host は Amazon.co.jp のものでは無いと推察できます。
この様に、送信元のアドレスが、ネットショップや銀行、クレジットカード会社などであっても、そのメールを送信してきた Host が正規のものか不正なものかで、受信メールの真贋を判断することができるのです。

また、外部リンクには「www.amazon-jp.zydmrou.cn」が含まれています。本メールは HTML 形式なので、メール本文を閲覧しただけでは、クリックすると何処へつながるのかを確認することは容易ではありません。また、「www.amazon-jp.zydmrou.cn」は一見すると Amazon のメールアドレスであると取り違えてしまう心配もあります。

## ❑ Private 秘書サービスを利用することで ～ 再確認 ～

インターネットから届くメールには危険なものがたくさんあります。
Private 秘書サービスは、これらの脅威を察知してビジュアル的に利用者の視覚へ訴えます。
専門的な知識のない利用者であっても、「緑：信頼されている」「赤：信頼されていない」から容易に注意喚起され、インターネットの先にいる悪意の攻撃者の罠にかからずに、本当に必要なメールだけを取捨して PC やモバイルで安全にメールを受け取る手助けをします。

まずは、緑 と 赤 の表示を手掛かりに、判断に困ったらアドバイザーの詳細画面で送信元アドレスや送信元 Hostを細かく吟味することで、騙されることの無い安心できるメール受信環境をご利用下さい。

https://www.hisho.ne.jp/

特定非営利活動法人
インターネットビジネス研究所
XES-NET https://www.ib-r.com
〒178-0063 東京都練馬区東大泉 4-17-9
mailto:info@ib-r.com

2023/7/20 版