

**E-Post Secure Handler**  
**(インバウンドメール承認機能)**  
**ユーザーズガイド**

(第1. 03C 版)

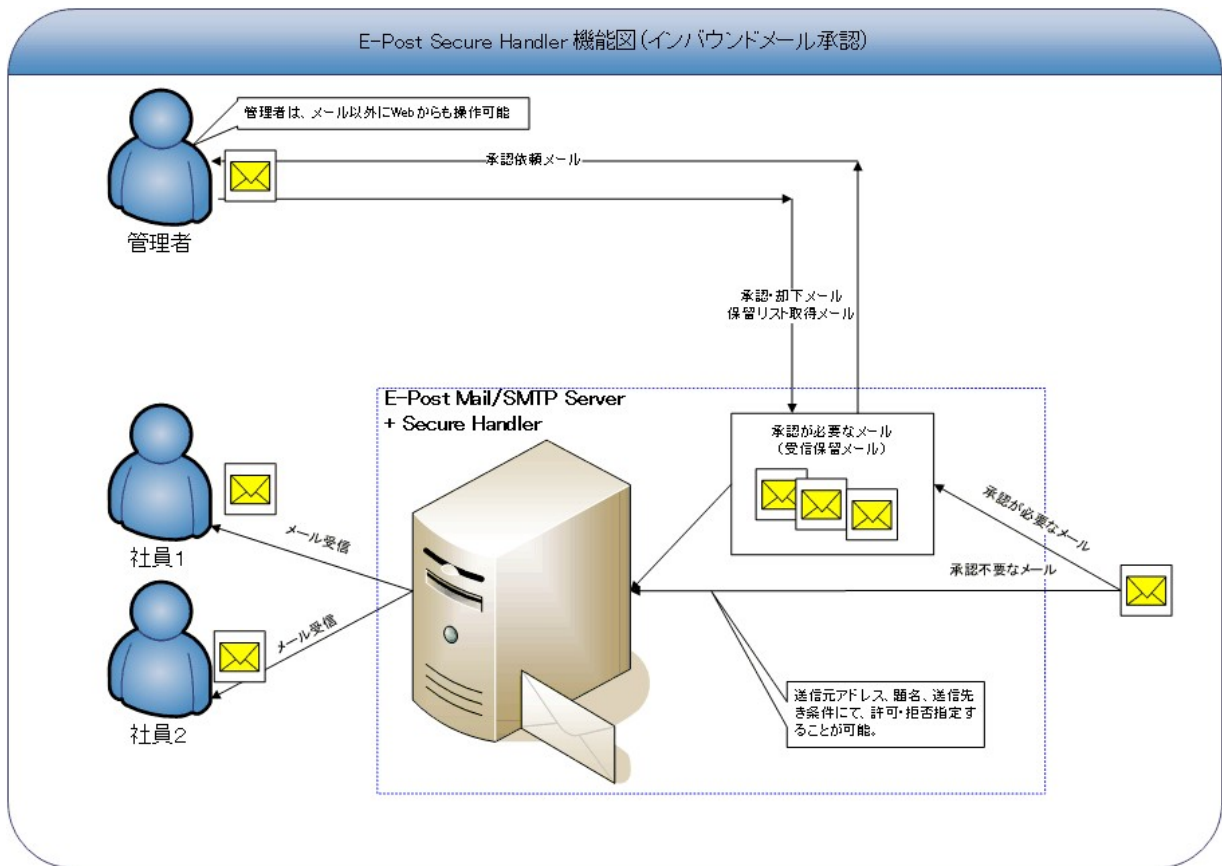
## はじめに

このたびは、「E-Post Secure Handler (インバウンドメール承認機能)」をお買い上げいただきまして誠に有難うございました。

「E-Post Secure Handler (インバウンドメール承認機能)」は、外部ドメインから届けられたメールを一時スプールし管理者が、スプール中のメールの安全確認を行い内部ドメイン宛へ安全なメールを受信することを目的としたメールゲートウェイ機能を付加します。

継続して運用することにより、許可した送信元のメールは次回以降、自動的に受信(通過)し、拒否した送信元のメールは次回以降、自動的に受信拒否されますので、よりスムーズで安全なメール環境が時間と共に構築されていきます。  
踏み台対策、スパム対策、ランサムウェア(マルウェア)対策等にご利用ください。

## E-Post Secure Handler 機能(インバウンドメール承認)



**注意** 本マニュアルは、お買い上げいただいた製品をお使いになるコンピュータにインストールする方法や、「E-Post Secure Handler」の各設定について説明をしています。本マニュアルに掲載されていない「E-Post Secure Handler」の機能については、オンラインヘルプおよびインターネットサイトを、ご参照ください。

### 本ガイドをお読みになる前に

本ガイドをお読みになる前に、お使いのコンピュータで Windows Server 2008 (R2), Windows Server 2012 (R2), Windows Server 2016 のいずれかが正常に動作し、TCP/IP プロトコルが正しく機能していることをご確認ください。

Microsoft, Windows, Windows NT は、米国 Microsoft Corporation の商標です。

本マニュアルの内容の一部または全部を無断掲載することをお断りします。

本マニュアルの内容については、機能向上のため、予告なく変更することがあります。

## ソフトウェア使用許諾契約書

重要:本ソフトウェアは、以下条項にご同意いただいた場合にのみご使用いただけます。

本ソフトウェアを使用された場合は下記条項にご同意いただけましたものとさせていただきますので、下記条項を充分お読みの上ご使用ください。

本ソフトウェアは、著作権法および著作権に関する条約をはじめ、その他の無体財産権に関する法律ならびに条約によって保護されています。本ソフトウェアは許諾されるもので、販売されるものではありません。

### 第1条 ライセンスの許諾

1. お客様は、発行された1ライセンスにつき、ご使用になるコンピュータのOS1台に対し、本ソフトウェアのコピーをインストールし使用する権利を許諾します。

### 第2条 複製の禁止

1. お客様は、バックアップの目的で本ソフトウェアの複製物を1個に限り作成することができます。
2. お客様は、本ソフトウェアの複製を前項以外の目的で行うことは出来ません。お客様が本条項に違反した場合、お客様の作成した複製品の所有権は、イー・ポストに帰属するものとし、イー・ポストは即時全複製品の引渡しをお客様に対して要求することができます。

### 第3条 譲渡、貸与の禁止

1. お客様はイー・ポストの書面による事前の承認なしに、第1条に規定するライセンスの許諾を、譲渡(売買、贈与、交換)または貸与等の方法で第三者に提供することは出来ません。
2. お客様は本製品のレンタル、擬似レンタル行為、中古品取引を行うことは出来ません。

### 第4条 反社会的勢力との取引排除

1. 弊社は、自ら及び自らの役員・従業員が、反社会的勢力(暴力団、暴力団員、暴力団準構成員、暴力団関係企業・団体、総会屋、社会運動等標ぼうゴロ、その他反社会的勢力。以下総称して「反社会的勢力」という)でないことを保証するとともに、これらの反社会的勢力との関係を一切持たないことを保証します。
2. 弊社は、お客様が次の各号の一に該当する場合、催告することなく本契約を解除することができるものとします。なお、当該契約解除により損害が生じた場合であっても、お客様がその責を負うものとします。
  - (1)お客様またはお客様の役員・従業員が、反社会的勢力である場合。
  - (2)お客様またはお客様の役員・従業員が、反社会的勢力との関係を有していると認められる場合。
  - (3)お客様またはお客様の役員・従業員が、反社会的勢力に対して資金等を提供し、または便宜を供給するなど、反社会的勢力の運営維持に協力・関与していることが認められる場合。
3. 弊社は、前項各号を確認することを目的としてお客様の調査を行うことができるものとします。なお、弊社から調査を求められた場合、お客様はこれに協力するものとします。
4. お客様は、第2項各号のいずれかに該当し、またはそのおそれがあることが判明した場合、ただちにその旨を弊社に通知しなければならないものとします。

### 第5条 賠償請求

1. お客様が第2条または第3条に違反して本ソフトウェアの複製または譲渡、貸与等を行った場合、イー・ポストはお客様に対し、損害賠償として、本ソフトウェアの希望小売価格に複製回数に乗じて得た額の3倍に相当する金額を請求できるものとします。

### 第6条 期間

1. 本契約は本ソフトウェアをはじめてインストールしたときから効力を生ずるものとします。
2. お客様は、イー・ポストから提供された本ソフトウェア、説明書を含むイー・ポストからの提供物および複製物をすべて破棄し、その旨を証明する文書をイー・ポストに送付することにより本契約を終了させることができるものとします。

### 第7条 バージョンアップ

1. イー・ポストはお客様に予告無しに改良の為に本ソフトウェアの変更を行うことがあります。
2. イー・ポストは本ソフトウェアを改良した新しいバージョンのソフトウェア(以下「新バージョン」という)をお客様に対して有償または無償にて提供することができます。

3. バージョンアップキットの提供を受けたお客様は、本ソフトウェアライセンスの許諾その他の権利を失い、新バージョンについて新しい契約による権利を取得するものとします。

#### **第8条 免責**

1. イー・ポストは本ソフトウェアの使用により生じた損害に関していかなる責任も負わないものとします。

#### **第9条 サポートの期間**

1. 本製品の販売終了から1年経過した後は本ソフトウェアに関するイー・ポストのサポートは終了するものとします。
2. 新バージョンが発売された場合、本ソフトウェアは特別な理由により継続される場合を除き販売終了となります。本ソフトウェアに関するサポートも同様に販売終了から1年経過した後に終了するものとします。
3. 前2項の規定にかかわらず、サポートの終了後もイー・ポストの指定した受付期間内に限り、お客様は第6条のバージョンアップのサービスを受けることが出来るものとします。

#### **第10条 ソフトウェアの変更の禁止**

1. お客様は、いかなる理由があっても本ソフトウェアの変更、改作、リバースエンジニアリング、逆コンパイル、逆アセンブルその他を行うことは出来ません。

#### **第11条 管轄裁判所**

1. お客様及びイー・ポストは本契約に関連して発生した紛争については東京地方裁判所を第一審の管轄裁判所とすることに合意します。

## 使用環境

Windows Server 2008 (R2)/2012 (R2)/2016

E-POST メールサーバまたは、E-POST SMTP サーバがインストールされている必要があります。

推奨するハードウェアスペック

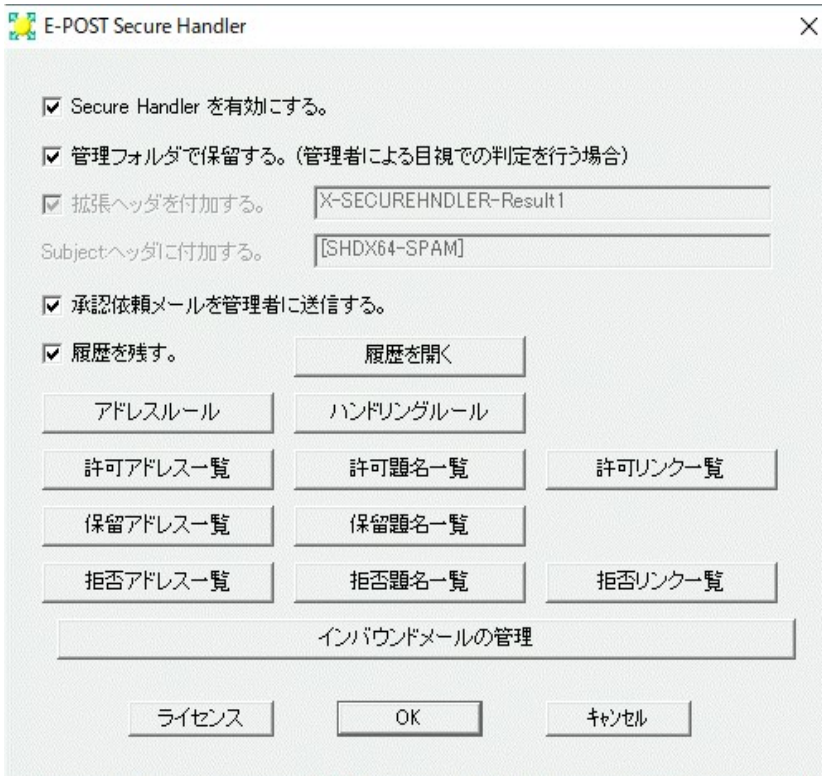
- CPU Xeon Core 相当 2GHz 以上
- MEM 8GB 以上
- HDD 60GB 以上

本プログラムは、Intel(および互換 CPU)用です。

## E-Post Secure Handler (インバウンドメール承認)機能の設定



インストールが完了するとデスクトップ上に設定アイコンが表示されるので、マウスでインバウンドメール承認機能を有効とする為に初期設定を行います。



### Secure Handler を有効にする。

インバウンドメール承認を有効にする場合、チェックボックスをオンにします。

### 管理フォルダで保留する。(管理者による目視での判定を行う場合)

セキュアハンドによる保留条件に合致したインバウンドメール承認を管理者が目視で行う場合、チェックします。

### 拡張ヘッダを付加する。

管理者が目視で行わず、セキュアハンドによる判定を任意の拡張ヘッダとして追加する場合、チェックし追加する拡張ヘッダ名を項目として指定します。

### Subject:ヘッダに付加する。

管理者が目視で行わず、セキュアハンドによる判定を任意の文字列(例:SPAM や JUNK)として SUBJECT(題名)メールヘッダの先頭に記載する場合項目として指定します。

### 承認依頼メールを管理者に送信する。

ご使用のメーラにてインバウンドメールの受信の許可や拒否を行う際の承認依頼を生成したい場合、チェックボックスをオンにします。

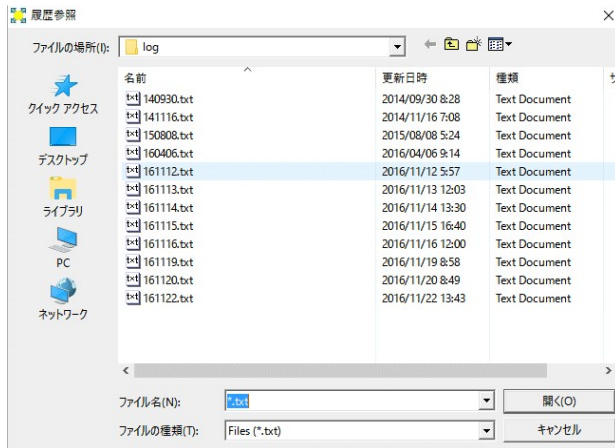
オフでは、承認依頼のメールは生成されません。ブラウザでのみ管理する際に、依頼メールの生成を抑止します。

### 履歴を残す。

インバウンドメールの受信の許可や拒否を行った履歴(ログ)を残したい場合、チェックボックスをオンにします。

### 履歴を開く

履歴内容を参照する場合クリックすると履歴一覧が表示されます。



## アドレスルール

ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、reciver.dat という承認発生条件を設定するファイルを表示します。

3行目の管理者アドレスを適正なアドレスに設定します。他項目は特別な事情がない限り、変更しないでください。

1行目:送信元アドレスのホワイトリストファイルが指定されています。

2行目:送信元アドレスのブラックリストファイルが指定されています。

3行目:題名でのハンドリングルール(以下)ファイルと管理者アドレスが指定されています。

**管理者アドレスは、E-Post Secure Handler を組込む Mail/SMTP サーバを通過するアドレス(内部ドメインのアドレス)を指定します。**

外部ドメインでのアドレス指定は出来ません。



## ハンドリングルール

ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、reciverkey.dat という承認発生条件(主に題名キーワード)を設定するファイルを表示します。

特別な事情がない限り、記述済みの最初から2行分(white=... および black=...)は変更しないでください。

1行目:題名のホワイトリストファイルが指定されています。

2行目:題名のブラックリストファイルが指定されています。

3行目以降:承認対象となる題名や送信先などの条件を列挙します。

ここで指定した条件に一致したメールが承認対象のメールとして保留されることになります。



## 【設定できる条件】

設定条件には、ワイルドカード“\*”での指定が可能です。

ワイルドカードが含まれない指定文字列は完全一致となるので注意が必要です。

### [to0=非保留送信先]について

エンベロープの送信先(同報の場合、最初のアドレス)に、ここで定義した文字列が含まれていないとき、インバウンドメール承認を実施します。

### [to1=保留送信先]について

エンベロープの送信先(同報の場合、最初のアドレス)に、ここで定義した文字列が含まれているとき、インバウンドメール承認を実施します。

### [cc0=非保留送信先]について

エンベロープの送信先(同報の場合、2つ目以降のアドレス)に、ここで定義した文字列が含まれないとき、インバウンドメール承認を実施します。

### [cc1=保留送信先]について

エンベロープの送信先(同報の場合、2つ目以降のアドレス)に、ここで定義した文字列が含まれているとき、インバウンドメール承認を実施します。

### [envf0=非保留送信元]について

エンベロープの送信元に、ここで定義した文字列が含まれないとき、インバウンドメール承認を実施します。

### [envf1=保留送信元]について

エンベロープの送信元に、ここで定義した文字列が含まれているとき、インバウンドメール承認を実施します。

### [date0=非保留日付]について

Date:ヘッダにここで定義した文字列が含まれないとき、インバウンドメール承認を実施します。

### [date1=保留日付]について

Date:ヘッダにここで定義した文字列が含まれるとき、インバウンドメール承認を実施します。

### [from0=非保留送信元]について

From:ヘッダにここで定義した文字列が含まれないとき、インバウンドメール承認を実施します。

### [from1=保留送信元]について

From:ヘッダにここで定義した文字列が含まれるとき、インバウンドメール承認を実施します。

### [sub0=非保留題名]について

Subject:ヘッダにここで定義した文字列が含まれないとき、インバウンドメール承認を実施します。

※保管文字コードはデフォルトは SHIFT-JIS コードです。(admiappr.ini 内の code=設定が反映されます。)

### [sub1=保留題名]について

Subject:ヘッダにここで定義した文字列が含まれるとき、インバウンドメール承認を実施します。

※保管文字コードはデフォルトは SHIFT-JIS コードです。(admiappr.ini 内の code=設定が反映されます。)

## 【設定例】

Date ヘッダの時差が“+0900”以外を保留し承認対象とする場合。(みなし、国外のクライアントから送信されているメールを保留承認)

date0=\*+0900\*

特定のメールアドレス宛が含まれるメール保留し承認対象とする場合。(特定内部アカウント宛のメールを保留承認)

to1=hogehoge@xxx.co.jp

cc1=hogehoge@xxx.co.jp

特定の表題が含まれるメール保留し承認対象とする場合。(詐欺メールの可能性のあるメールを保留承認)

sub1=\*請求\*

## 許可アドレス一覧

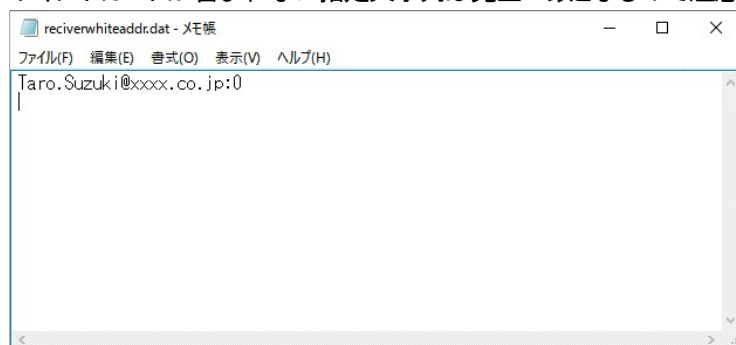
ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、reciverwhiteaddr.dat という承認許可された、エンベロープの送信元が保存されるファイルを表示します。

送信元のホワイトリストテーブルとして機能します。

設定条件には、ワイルドカード“\*”での指定が可能です。



ワイルドカードが含まれない指定文字列は完全一致となるので注意が必要です。



### 保留アドレス一覧

ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、receivergrayaddr.dat という WEB 管理で操作された承認許可回数を超えるまでの「許可アドレス一覧」へ登録が保留されている、エンベロープの送信元が保存されるファイルを表示します。

保留内容は、〈アドレス〉×〈カウント数〉が含まれます。

許可回数は、admiappr.ini 中の「ホワイトリストへの登録までの許可設定回数(グレーリストでの保持回数)whitecount=〈許可が必要な回数〉」に設定された値になります。

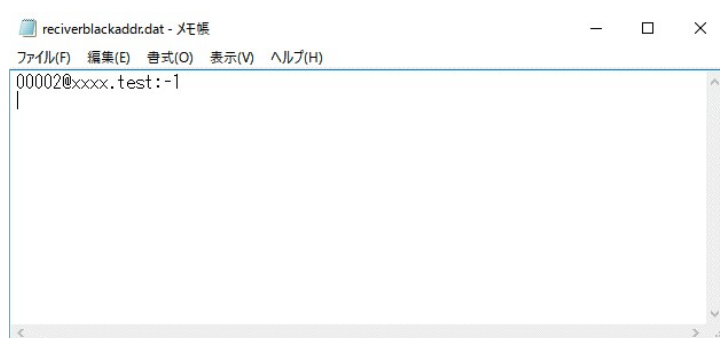
### 拒否アドレス一覧

ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、receiverblackaddr.dat という承認拒否された、エンベロープの送信元が保存されるファイルを表示します。

送信元のブラックリストテーブルとして機能します。

設定条件には、ワイルドカード“\*”での指定が可能です。

ワイルドカードが含まれない指定文字列は完全一致となるので注意が必要です。



### 許可題名一覧

ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、receiverwhiteword.dat という承認許可された、メールの題名が保存されるファイルを表示します。

題名のホワイトリストテーブルとして機能します。

設定条件には、ワイルドカード“\*”での指定が可能です。

ワイルドカードが含まれない指定文字列は完全一致となるので注意が必要です。

※保管文字コードはデフォルトは SHIFT-JIS コードです。(admiappr.ini 内の code=設定が反映されます。)



## 保留題名一覧

ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、recivergrayword.dat という WEB 管理で操作された承認許可回数を超えるまでの「許可題名一覧」へ登録が保留されている、エンベロープの送信元が保存されるファイルを表示します。

保留内容は、〈題名〉〈カウント数〉が含まれます。

許可回数は、admiappr.ini 中の「ホワイリストへの登録までの許可設定回数(グレーリストでの保持回数)whitecount=〈許可が必要な回数〉」に設定された値になります。

※保管文字コードはデフォルトは SHIFT-JIS コードです。(admiappr.ini 内の code=設定が反映されます。)

## 拒否題名一覧

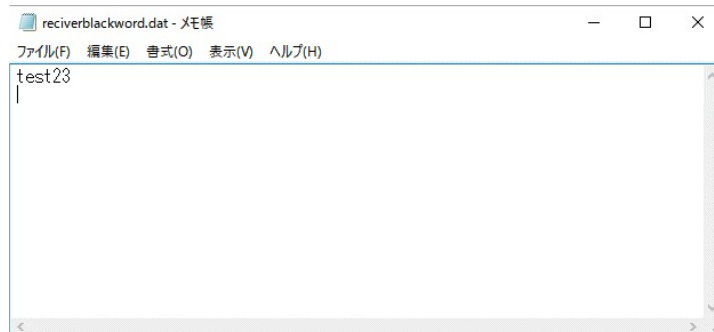
ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、reciverblackword.dat という承認拒否された、メールの題名が保存されるファイルを表示します。

題名のブラックリストテーブルとして機能します。

設定条件には、ワイルドカード“\*”での指定が可能です。

ワイルドカードが含まれない指定文字列は完全一致となるので注意が必要です。

※保管文字コードはデフォルトは SHIFT-JIS コードです。(admiappr.ini 内の code=設定が反映されます。)



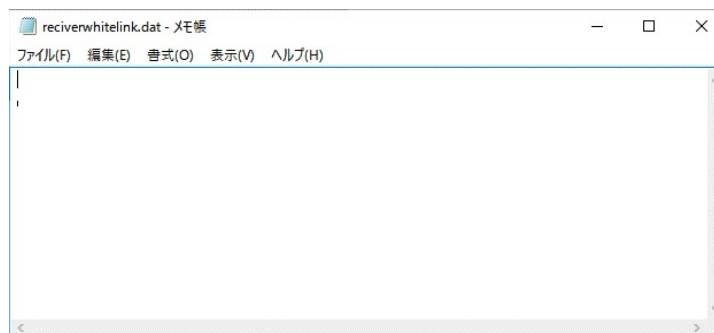
## 許可リンク一覧

ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、reciverwhitelink.dat という、メール本文中に記載されたスパムにしないリンクを保存するファイルを表示します。

本文内のリンクのホワイリストテーブルとして機能します。

設定条件には、ワイルドカード“\*”での指定が可能です。

ワイルドカードが含まれない指定文字列は完全一致となるので注意が必要です。



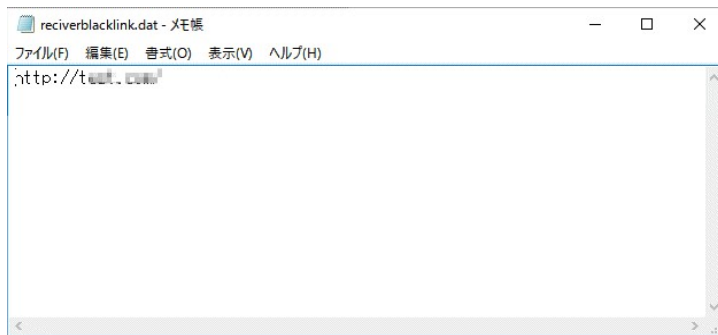
## 拒否リンク一覧

ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、reciverblacklink.dat という、メール本文中に記載されたスパムにしたいリンクを保存するファイルを表示します。

本文内のリンクのブラックリストテーブルとして機能します。

設定条件には、ワイルドカード“\*”での指定が可能です。

ワイルドカードが含まれない指定文字列は完全一致となるので注意が必要です。



以上の設定が終わったら[OK]ボタンを押して設定を保存します。

「Secure Handler を有効にする。」や「承認依頼メールを管理者に送信する。」の変更を行った場合は、[E-Post Mail Control]を起動し、[サービス]タブの EPSTRS について停止→開始を行うと機能が反映されます。

## ブラウザからの操作

### WEB サーバ(IIS7)での設定

IIS の Web サーバに付属の CGI,HTML ファイルを設定することで、インバウンドメール承認がブラウザからの操作を行うことができます。

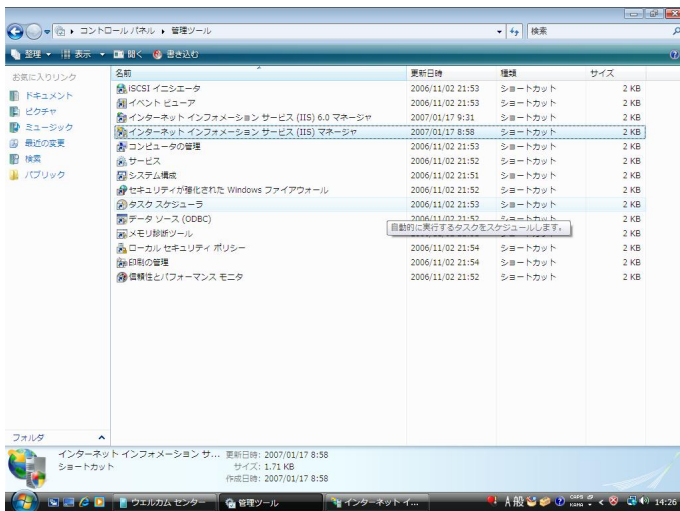
ブラウザからの操作では、拒否したメールはバックアップされ、何らかの理由で回復したい場合にも対処できる機能が用意されています。

### IIS 7 での設定

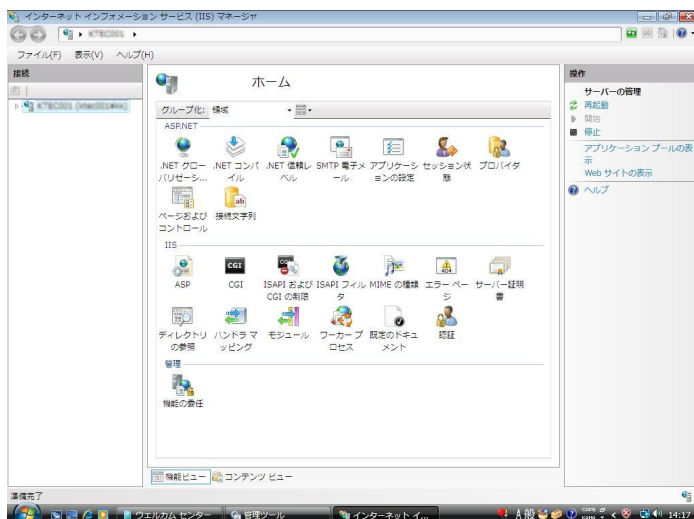
注意)

IIS 7 で利用する場合は、以下の設定を行い拡張子“.exe”が CGI として実行可能となるように設定を行う必要があります。

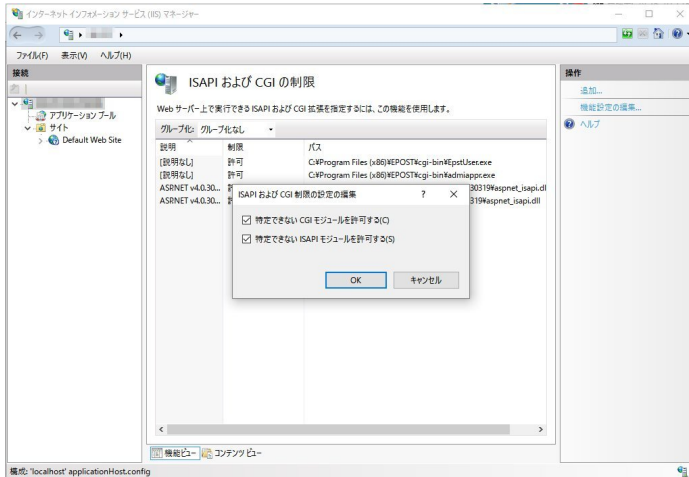
インターネットインフォメーションサービス(IIS)マネージャを起動します。



コントロールパネル ⇒ 管理ツール ⇒ インターネットインフォメーションサービス(IIS)マネージャ



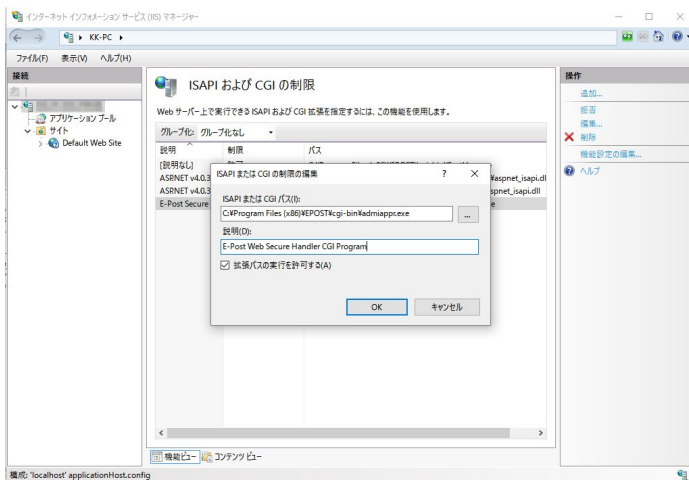
## ISAPI および CGI の制限への設定



### 機能設定の編集

⇒特定できない CGI モジュールを許可する=チェック

⇒特定できない ISAPI モジュールを許可する=チェック

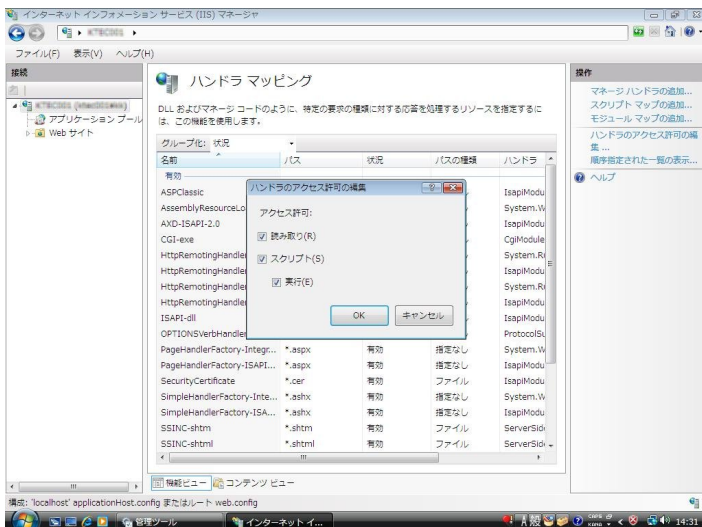


### 追加

⇒ISAPI または CGI の制限の編集="c:\program files\epost\cgi-bin\admiappr.exe" (CGI を指定)

⇒説明=E-POST Web Secure Handler Manager CGI Program

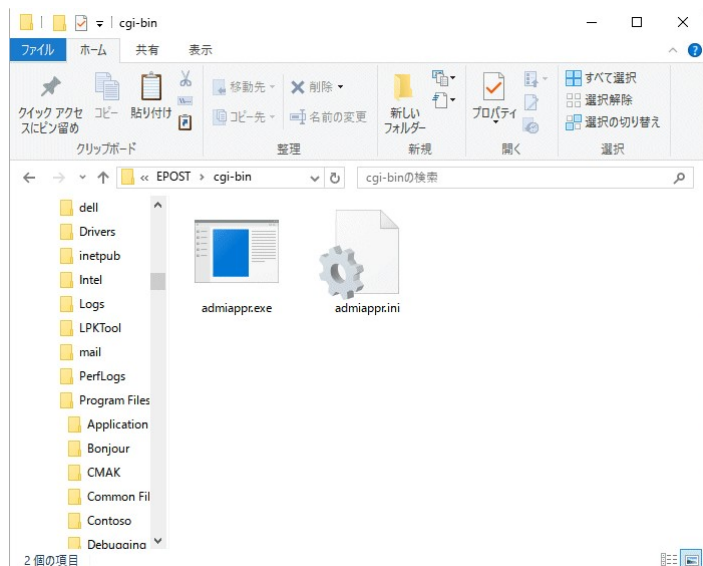
⇒拡張パスの実行を許可する



## ハンドラマッピングへの設定

CGI-exe ハンドラアクセスの許可の編集=実行をチェック  
 以上を設定すると、CGIが動作可能になります。

「仮想ディレクトリ」"cgi-bin"が無い場合は、実フォルダを"c:\program files¥epost¥cgi-bin"として作成します。  
 既に「仮想ディレクトリ」"cgi-bin"が存在する場合は、"C:\Program Files¥EPOST¥cgi-bin"の内容を  
 (admiappr.exe/admiappr.ini)をコピーします。



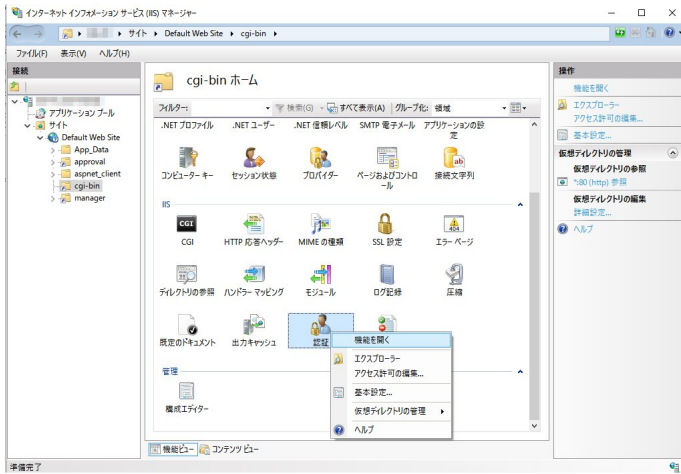
保存後、"admiappr.ini"ファイルをメモ帳などで開き、以下の2項目を実際にHTMLが保管されているフォルダ位置及び  
 仮想フォルダ名に変更して保存してください。



—— admiappr.ini の変更 ——

'承認管理 UR  
 urlpath=/approval/  
 'HTML フォルダ  
 html=C:\Program files¥EPOST¥admiappr¥

設定した CGI(admiappr.exe)には、「インターネットサービスマネージャ(IIS)」より  
 => 表示ツリーから仮想フォルダ"CGI-BIN"フォルダを選択します。



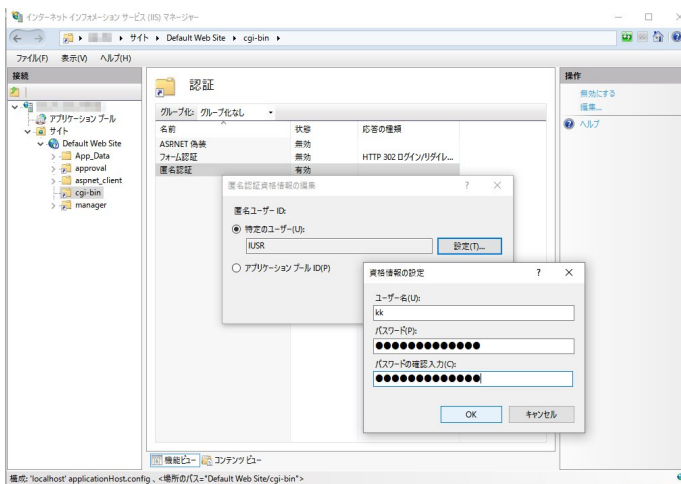
⇒ 認証

⇒ 匿名認証

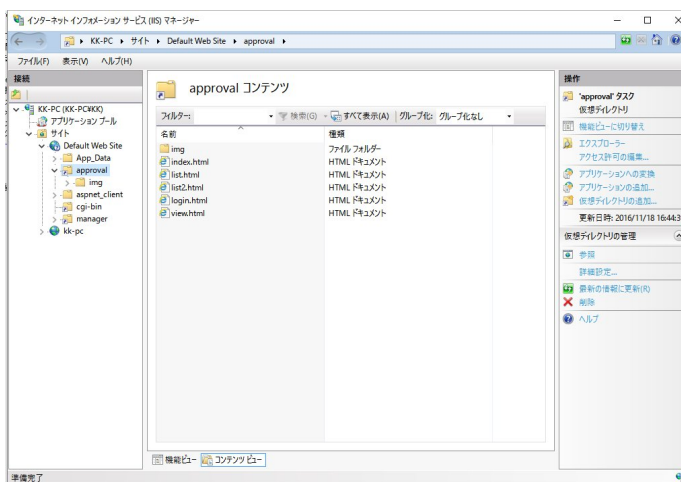
⇒ 編集

⇒ 特定のユーザー

⇒ Administrator 権限を持つユーザーアカウントを定義しておきます。



「インターネットサービスマネージャ(IIS)」にて、ルート下に「仮想ディレクトリ」"approval"を作成し、「c:\program files\post\admiappr%」を割当て、該当の WEB サイトを起動してください。



最後にブラウザより、<http://localhost/approval/> へ接続し、操作画面が表示されれば設定完了です

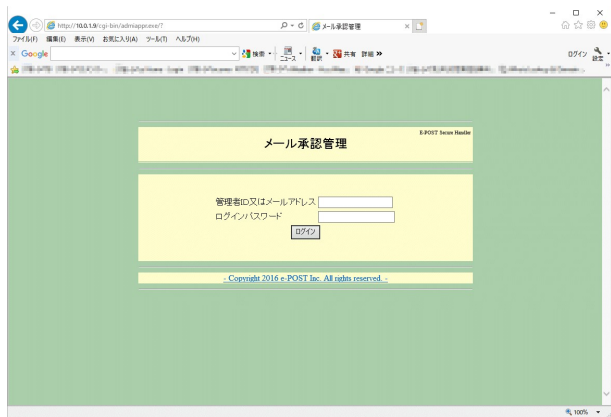


## ログイン

ブラウザから <http://localhost/approval/> を表示するとログイン画面が開きます。

デフォルトでは、管理者IDは、“admin”、ログインパスワードは、“secret”で設定されています。

管理者ID 及びログインパスワードの変更は、IIS で割当てた CGI フォルダに保存されている、admiappr.ini ファイルをメモ帳で開き、“id=admin”、“pw=secret”の行を任意の管理者ID 及びパスワードに変更してください。

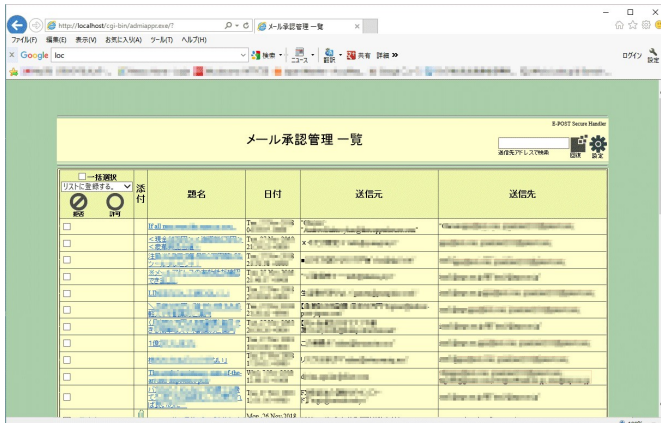


## 許可設定及び拒否設定

ブラウザからログインが成功すると、承認待ちのインバウンドメール一覧が表示されます。

メール行の左側のチェックボックスをチェックし、許可又は拒否(アイコン)ボタンを押すことで許可又は拒否が実行されます。

その際、情報をホワイトリストとして登録するか否かを選択するために、上部のリストボックスの表示で、“リストに登録する”又は、“リストに登録しない”が選択できます。





## メール閲覧

ブラウザからログインが成功すると、承認待ちのインバウンドメール一覧が表示されます。

メール内容を閲覧し確認したいときは、題名をクリックすると、閲覧画面が表示されます。

許可または拒否する際に、情報をホワイトリストとして登録するか否かを選択するために、上部のリストボックスの表示で、“リストに登録する”又は、“リストに登録しない”が選択できます。



[ヘッダ情報の]欄をクリックするとヘッダが表示できます。



添付ファイルが含まれている場合、デフォルトの設定ではダウンロード時に、拡張子を除去し MIME によるアプリの自動起動を抑制します。

添付ファイルのダウンロードを禁止したい場合や、拡張子を除去しないでダウンロード設定することも可能です。

設定については、cgi-bin 保存フォルダに含まれる、“admiappr.ini”ファイルの内容を参照してください。



アドバイス欄は、管理者が承認、拒否の判断材料として、表示しているメールについて”怪しさの判定結果”を機械が判定した結果を表示します。※cgi-bin フォルダにある admiappr.exe をコマンドプロンプトから実行させる事で機械判定による一括処理が可能です。

## メールの回復や完全な削除

承認待ちのインバウンドメール一覧の右上に表示されている回復アイコンをクリックすると表示されます。ここでは、メール一覧や閲覧ページで拒否設定を行ったメールが保管されているので、何らかの理由で拒否したメールを再許可したい場合や、完全に削除したい場合この画面にて操作を行います。

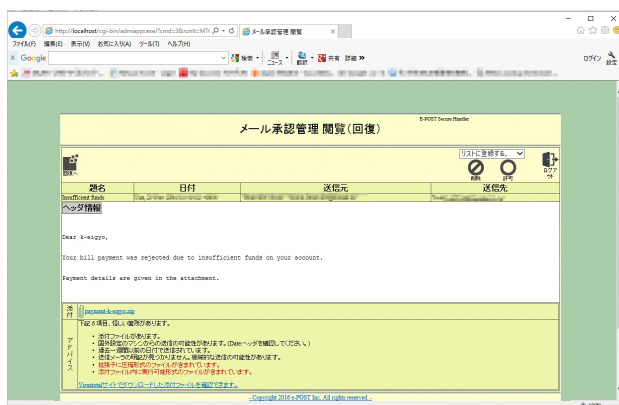
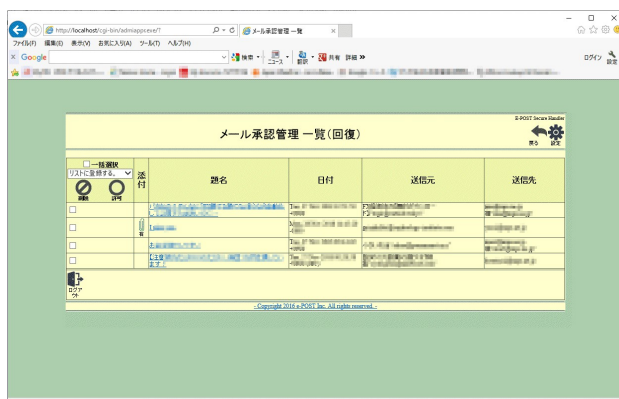
操作方法は、メール一覧の表示や拒否&許可設定と同様に行えます。

※メールからの制御による拒否では、メールは保管されません。WEBからの操作のみに有効です。

※回復より許可を実施した場合、メールシステムへ戻され、送信先へ配送されます。

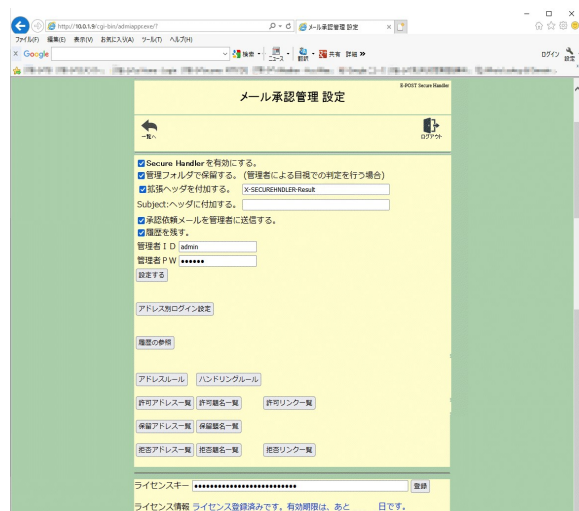
※回復より削除を実施した場合、本システムからのメールの回復はできなくなります。

“メール一覧”へ戻る場合は、“メール一覧(回復)”ページの右上の“戻る”アイコンをクリックします。



## 設定

承認待ちのインバウンドメール一覧の右上のアイコンをクリックすると設定が表示されます。



### Secure Handler を有効にする。

インバウンドメール承認を有効にする場合、チェックボックスをオンにします。

### 管理フォルダで保留する。(管理者による目視での判定を行う場合)

セキュアハンドラによる保留条件に合致したインバウンドメール承認を管理者が目視で行う場合、チェックします。

### 拡張ヘッダを付加する。

管理者が目視で行わず、セキュアハンドによる判定を任意の拡張ヘッダとして追加する場合、チェックし追加する拡張ヘッダ名を項目として指定します。

### Subjectヘッダに付加する。

管理者が目視で行わず、セキュアハンドによる判定を任意の文字列(例:SPAM や JUNK)として SUBJECT(題名)メールヘッダの先頭に記載する場合項目として指定します。

### 承認依頼メールを管理者に送信する。

ご使用のメーラにてインバウンドメールの受信の許可や拒否を行う際の承認依頼を生成したい場合、チェックボックスをオンにします。

オフでは、承認依頼のメールは生成されません。ブラウザでのみ管理する際に、依頼メールの生成を抑止します。

### 履歴を残す。

インバウンドメールの受信の許可や拒否を行った履歴(ログ)を残したい場合、チェックボックスをオンにします。

### 管理者ID

ログイン時の管理者IDを登録します。

### ログインパスワード

ログイン時のパスワードを登録します。

### ライセンスキー

製品のライセンスキーを登録します。

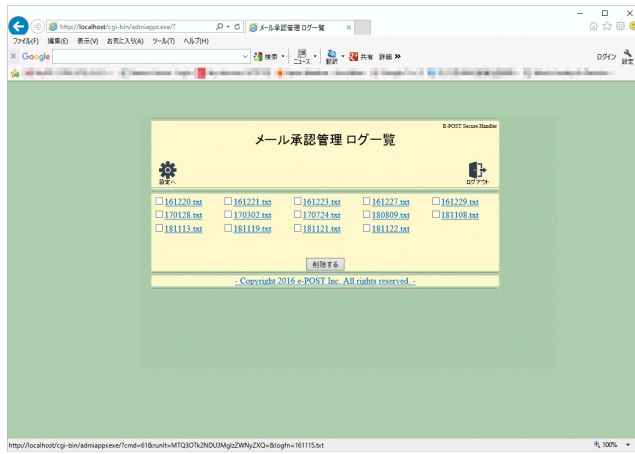
### アドレス別ログイン設定

を設定する項目です。書式は) <メールアドレス>,<パスワード> で行います



### 履歴の参照

履歴内容を参照する場合クリックすると履歴一覧が表示されます。



## アドレスルール

ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、reciver.dat という承認発生条件を設定するファイルを表示します。

3行目の管理者アドレスを適正なアドレスに設定します。他項目は特別な事情がない限り、変更しないでください。

1行目:送信元アドレスのホワイトリストファイルが指定されています。

2行目:送信元アドレスのブラックリストファイルが指定されています。

3行目:題名でのハンドリングルール(以下)ファイルと管理者アドレスが指定されています。

**管理者アドレスは、E-Post Secure Handler を組み込む Mail/SMTP サーバを通過するアドレス(内部ドメインのアドレス)を指定します。**

外部ドメインでのアドレス指定は出来ません。



## ハンドリングルール

ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、reciverkey.dat という承認発生条件(主に題名キーワード)を設定するファイルを表示します。

特別な事情がない限り、記述済みの最初から2行分(white=... および black=...)は変更しないでください。

1行目:題名のホワイトリストファイルが指定されています。

2行目:題名のブラックリストファイルが指定されています。

3行目以降:承認対象となる題名や送信先などの条件を列挙します。

ここで指定した条件に一致したメールが承認対象のメールとして保留されることになります。



### 【設定できる条件】

設定条件には、ワイルドカード“\*”での指定が可能です。

ワイルドカードが含まれない指定文字列は完全一致となるので注意が必要です。

[to0=非保留送信先]について

エンベロープの送信先(同報の場合、最初のアドレス)に、ここで定義した文字列が含まれていないとき、インバウンドメール承認を実施します。

[to1=保留送信先]について

エンベロープの送信先(同報の場合、最初のアドレス)に、ここで定義した文字列が含まれているとき、インバウンドメール承認を実施します。

[cc0=非保留送信先]について

エンベロープの送信先(同報の場合、2つ目以降のアドレス)に、ここで定義した文字列が含まれないとき、インバウンドメール承認を実施します。

[cc1=保留送信先]について

エンベロープの送信先(同報の場合、2つ目以降のアドレス)に、ここで定義した文字列が含まれているとき、インバウンドメール承認を実施します。

[envf0=非保留送信元]について

エンベロープの送信元に、ここで定義した文字列が含まれないとき、インバウンドメール承認を実施します。

[envf1=保留送信元]について

エンベロープの送信元に、ここで定義した文字列が含まれているとき、インバウンドメール承認を実施します。

[date0=非保留日付]について

Date:ヘッダにここで定義した文字列が含まれないとき、インバウンドメール承認を実施します。

[date1=保留日付]について

Date:ヘッダにここで定義した文字列が含まれるとき、インバウンドメール承認を実施します。

[from0=非保留送信元]について

From:ヘッダにここで定義した文字列が含まれないとき、インバウンドメール承認を実施します。

[from1=保留送信元]について

From:ヘッダにここで定義した文字列が含まれるとき、インバウンドメール承認を実施します。

[sub0=非保留題名]について

Subject:ヘッダにここで定義した文字列が含まれないとき、インバウンドメール承認を実施します。

※保管文字コードはデフォルトは SHIFT-JIS コードです。(admiappr.ini 内の code=設定が反映されます。)

[sub1=保留題名]について

Subject:ヘッダにここで定義した文字列が含まれるとき、インバウンドメール承認を実施します。

※保管文字コードはデフォルトは SHIFT-JIS コードです。(admiappr.ini 内の code=設定が反映されます。)

## 【設定例】

Date ヘッダの時差が"+0900"以外を保留し承認対象とする場合。(みなし、国外のクライアントから送信されているメールを保留承認)

date0=\*\*+0900\*

特定のメールアドレス宛が含まれるメール保留し承認対象とする場合。(特定内部アカウント宛のメールを保留承認)

to1=hogehoge@xxx.co.jp

cc1=hogehoge@xxx.co.jp

特定の表題が含まれるメール保留し承認対象とする場合。(詐欺メールの可能性のあるメールを保留承認)

sub1=\*請求\*

## 許可アドレス一覧

ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、reciverwhiteaddr.dat という承認許可された、エンベロープの送信元が保存されるファイルを表示します。

送信元のホワイトリストテーブルとして機能します。

設定条件には、ワイルドカード"\*"での指定が可能です。



ワイルドカードが含まれない指定文字列は完全一致となるので注意が必要です。



### 保留アドレス一覧

ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、receivergrayaddr.dat という WEB 管理で操作された承認許可回数を超えるまでの「許可アドレス一覧」へ登録が保留されている、エンベロープの送信元が保存されるファイルを表示します。

保留内容は、〈アドレス〉〈カウント数〉が含まれます。

許可回数は、admiappr.ini 中の「ホワイトリストへの登録までの許可設定回数(グレーリストでの保持回数)whitecount=〈許可が必要な回数〉」に設定された値になります。

### 拒否アドレス一覧

ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、receiverblackaddr.dat という承認拒否された、エンベロープの送信元が保存されるファイルを表示します。

送信元のブラックリストテーブルとして機能します。

設定条件には、ワイルドカード“\*”での指定が可能です。

ワイルドカードが含まれない指定文字列は完全一致となるので注意が必要です。



### 許可題名一覧

ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、receiverwhiteword.dat という承認許可された、メールの題名が保存されるファイルを表示します。

題名のホワイトリストテーブルとして機能します。

設定条件には、ワイルドカード“\*”での指定が可能です。

ワイルドカードが含まれない指定文字列は完全一致となるので注意が必要です。

※保管文字コードはデフォルトは SHIFT-JIS コードです。(admiappr.ini 内の code=設定が反映されます。)



### 保留題名一覧

ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、receivergrayword.dat という WEB 管理で操作された承認許可回数を超えるまでの「許可題名一覧」へ登録が保留されている、エンベロープの送信元が保存されるファイルを表示します。

保留内容は、〈題名〉〈カウント数〉が含まれます。

許可回数は、admiappr.ini 中の「ホワイトリストへの登録までの許可設定回数(グレーリストでの保持回数)whitecount=〈許可が必要な回数〉」に設定された値になります。

※保管文字コードはデフォルトは SHIFT-JIS コードです。(admiappr.ini 内の code=設定が反映されます。)

### 拒否題名一覧

ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、receiverblackword.dat という承認拒否された、メールの題名が保存されるファイルを表示します。

題名のブラックリストテーブルとして機能します。

設定条件には、ワイルドカード“\*”での指定が可能です。

ワイルドカードが含まれない指定文字列は完全一致となるので注意が必要です。

※保管文字コードはデフォルトは SHIFT-JIS コードです。(admiappr.ini 内の code=設定が反映されます。)



### 許可リンク一覧



ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、reciverwhitelink.dat という、メール本文中に記載されたスパムにしないリンクを保存するファイルを表示します。本文内のリンクのホワイトリストテーブルとして機能します。設定条件には、ワイルドカード“\*”での指定が可能です。ワイルドカードが含まれない指定文字列は完全一致となるので注意が必要です。



### 拒否リンク一覧

ボタンをクリックすると、E-Post Mail/SMTP Server インストールフォルダ内に設定される、reciverblacklink.dat という、メール本文中に記載されたスパムにしたいリンクを保存するファイルを表示します。本文内のリンクのブラックリストテーブルとして機能します。設定条件には、ワイルドカード“\*”での指定が可能です。ワイルドカードが含まれない指定文字列は完全一致となるので注意が必要です。



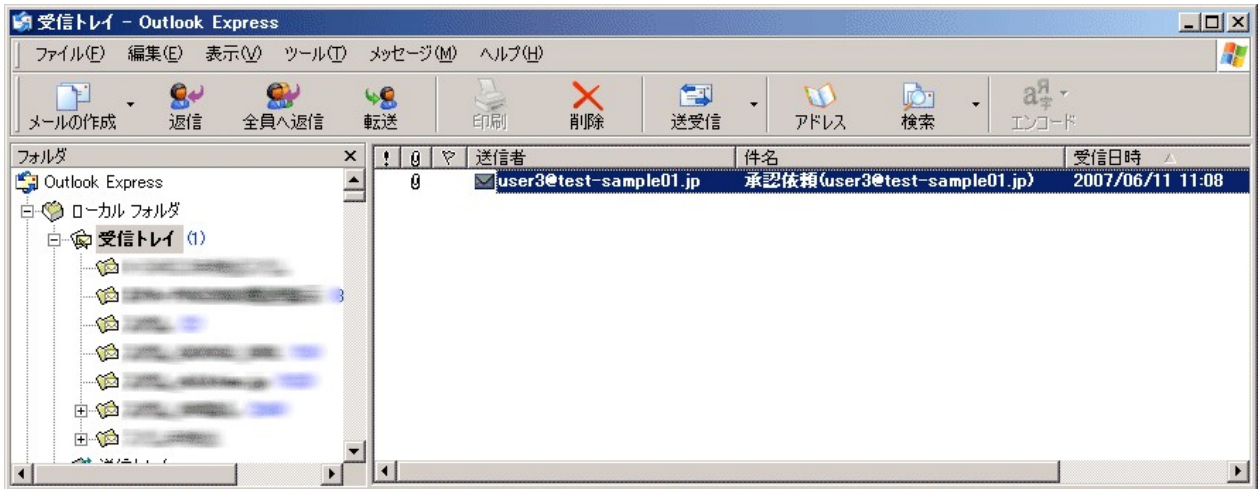
以上の設定が終わったら[OK]ボタンを押して設定を保存します。

「Secure Handler を有効にする。」や「承認依頼メールを管理者に送信する。」の変更を行った場合は、[E-Post Mail Control]を起動し、[サービス]タブの EPSTRS について停止→開始を行うと機能が反映されます。

## メールからの操作

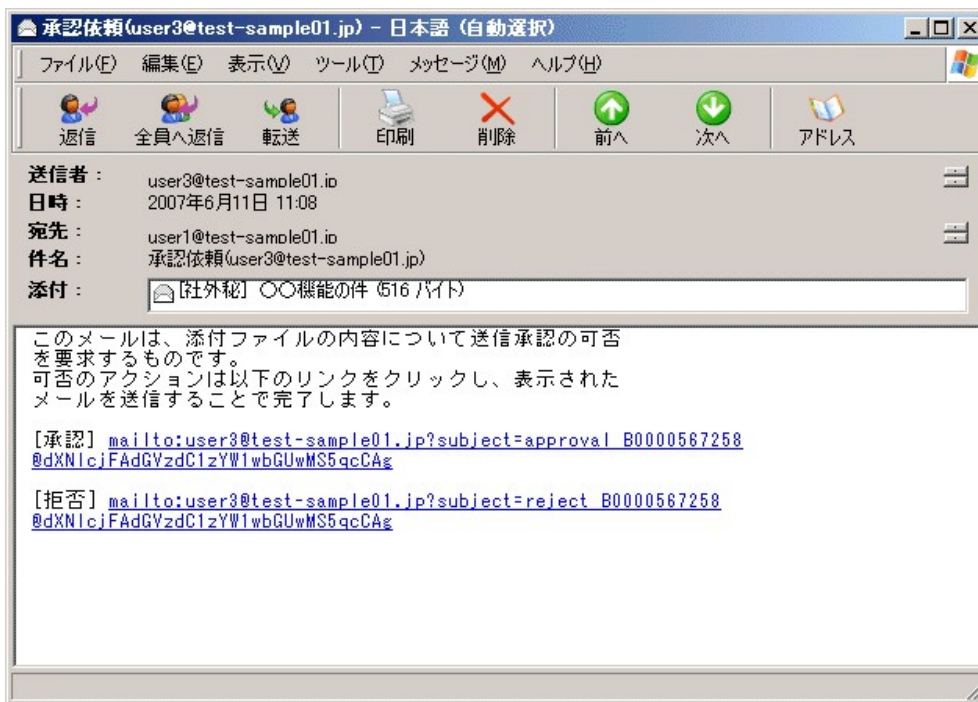
### 管理者のメールから承認、拒否する

外部サイトから内部ドメイン宛にメールが送られてくると条件に一致した場合、インバウンドメール承認管理者宛に「承認依頼メール」が送信されます。

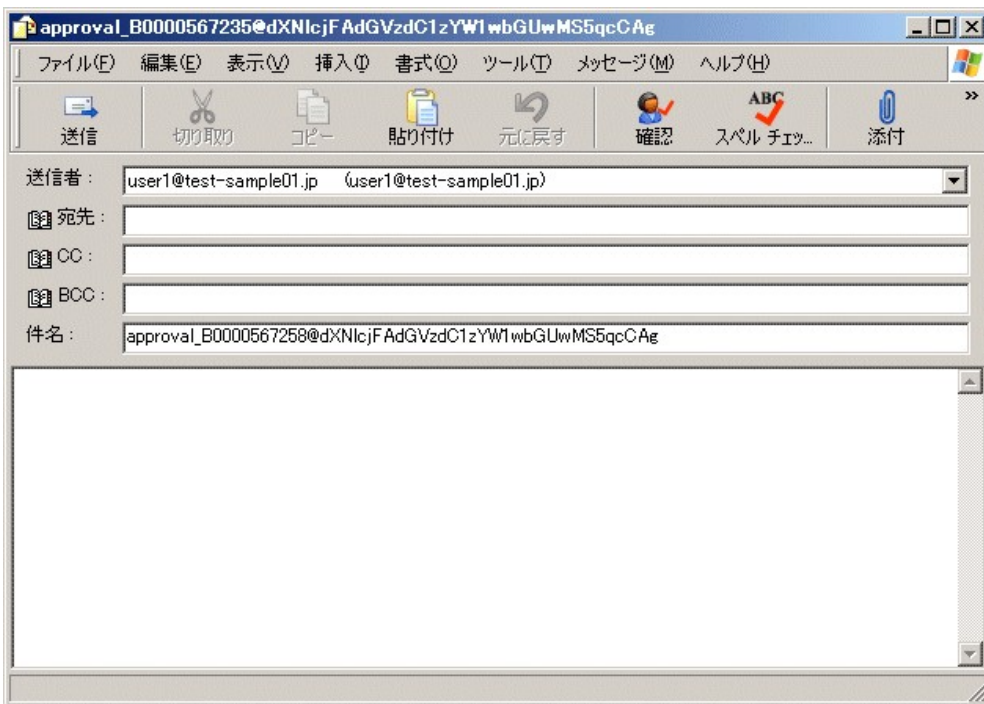


インバウンドメール承認管理者は、メールを参照し、承認・拒否を決め、「承認依頼メール」に記載されたリンクをクリックします。

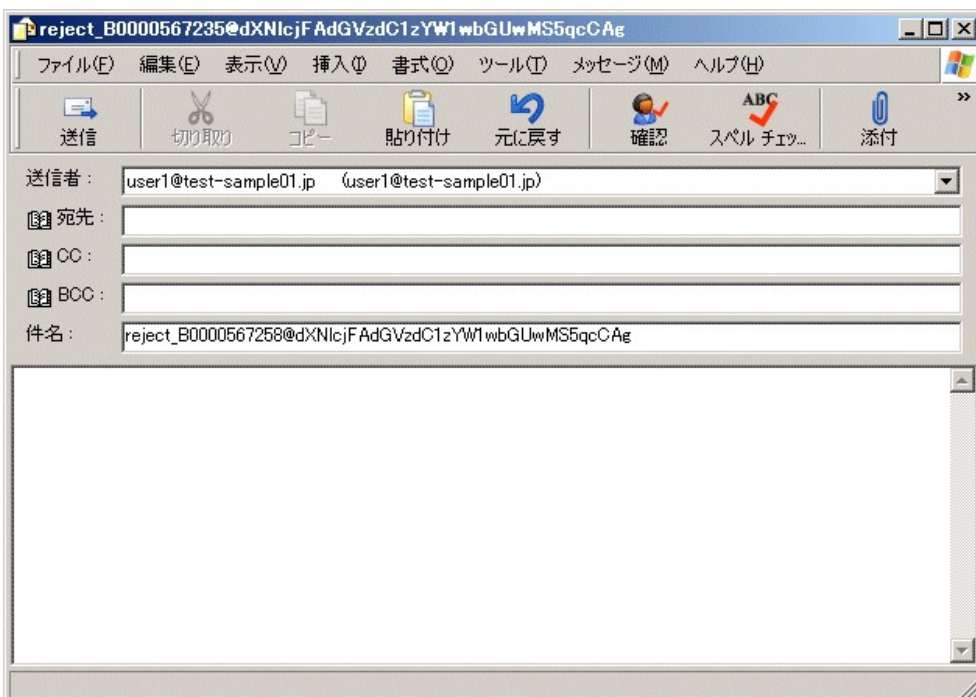
承認または、拒否メールが作成されますので、作成されたメールを送信します。



## [承認]のリンクを選択した場合(承認)



## [拒否]のリンクを選択した場合(拒否)



インバウンドメール承認管理者からの承認または、拒否メールを送信します。

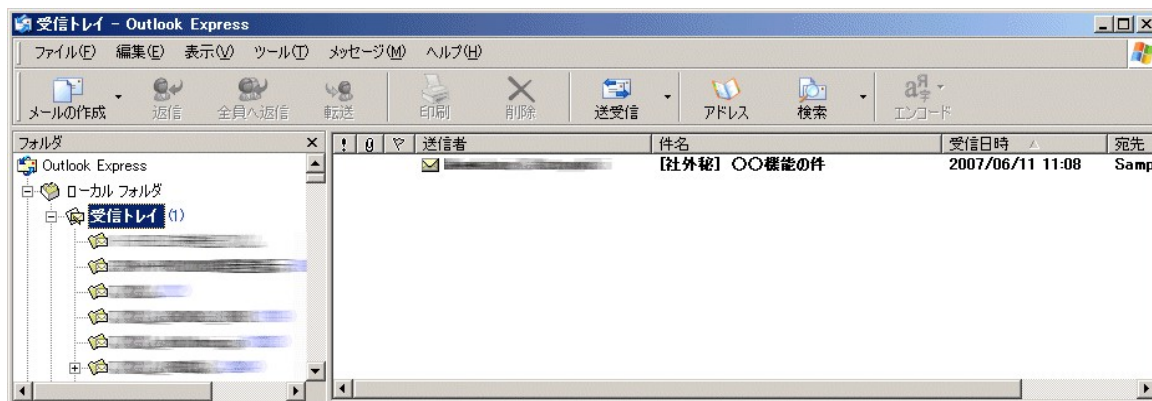
その際、送信先が送信元宛となっていますが、メールは内部制御メールとして処理され送信先には何も送信されないメールです。

制御により、承認された場合は、ホワイトリストに送信元アドレスと題名が登録され、且つ送信先に保留中のメールが送信され、拒否された場合は、ホワイトリストに送信元アドレスと題名が登録され、且つ保留中のメールは破棄されます。

### [承認された場合の動作]

ホワイトリストへの登録

保留中メールの送信



### [拒否された場合の動作]

ブラックリストへの登録

保留中メールの破棄

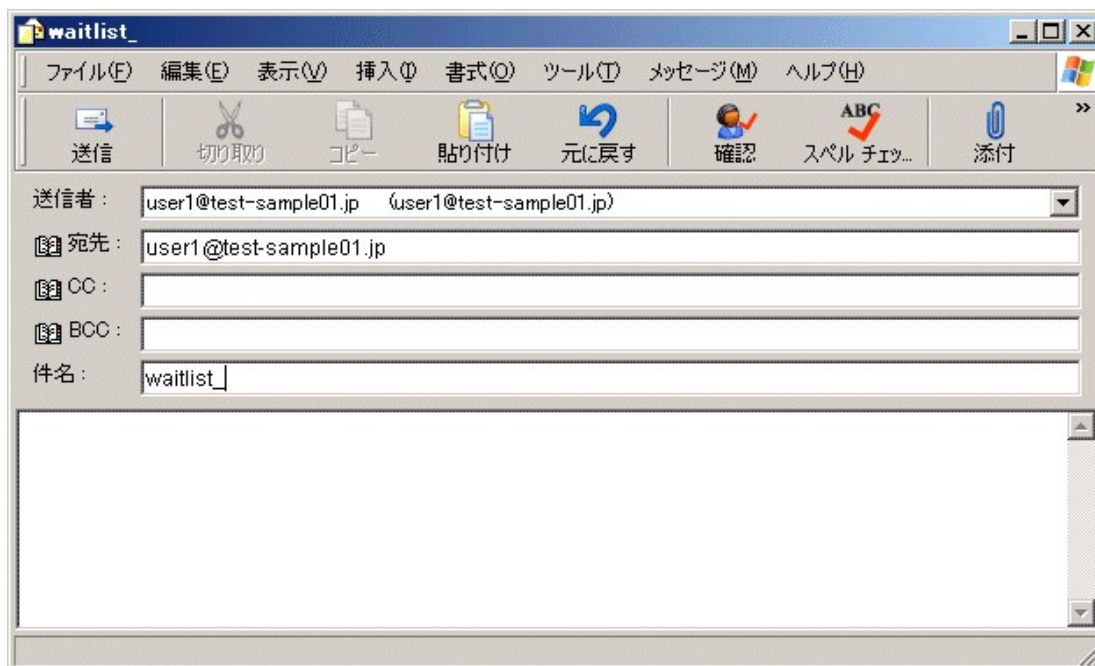


## 承認待ちメールの一覧を取得する場合

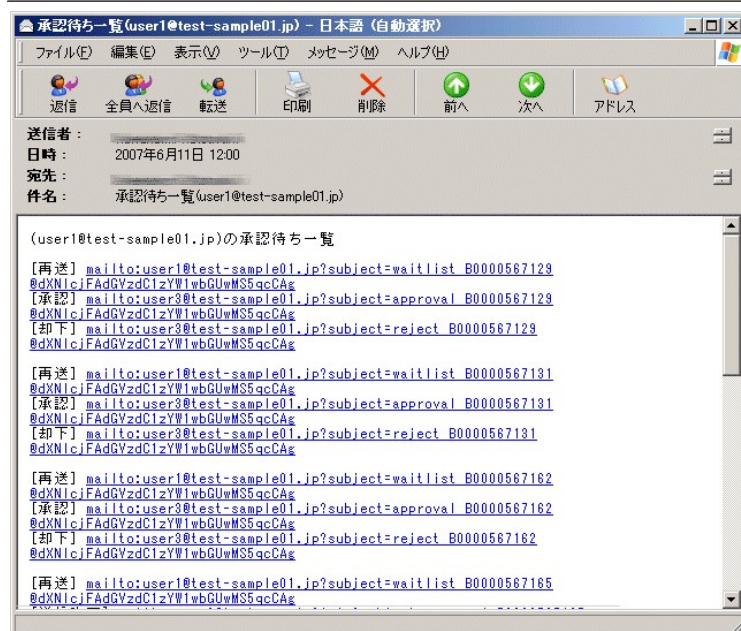
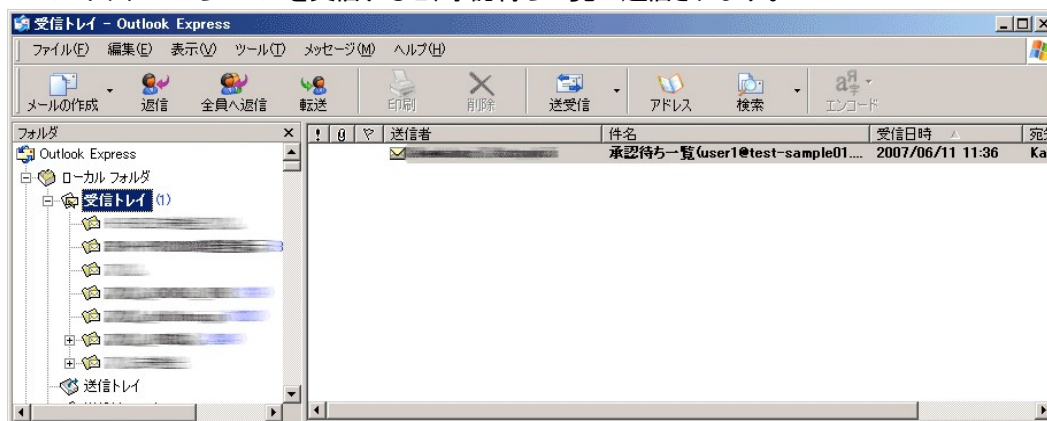
上長は、自身のメールアドレス宛に溜められている承認待ちメールの一覧を取得することができます。

新規メールを作成しメール送信します。

(送信先は、自分宛とし、本文は記載せず、表題は、“waitlist\_”とします。)



メールボックスからメールを受信すると、承認待ち一覧が送信されます。

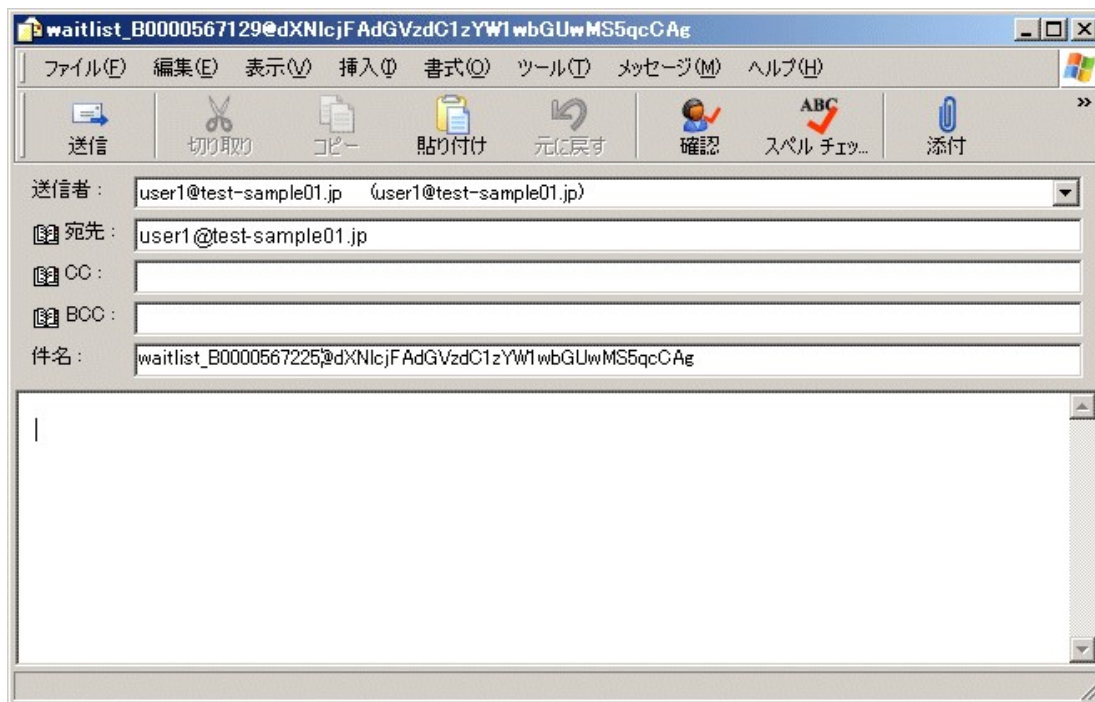


### 承認依頼メールを再取得する場合

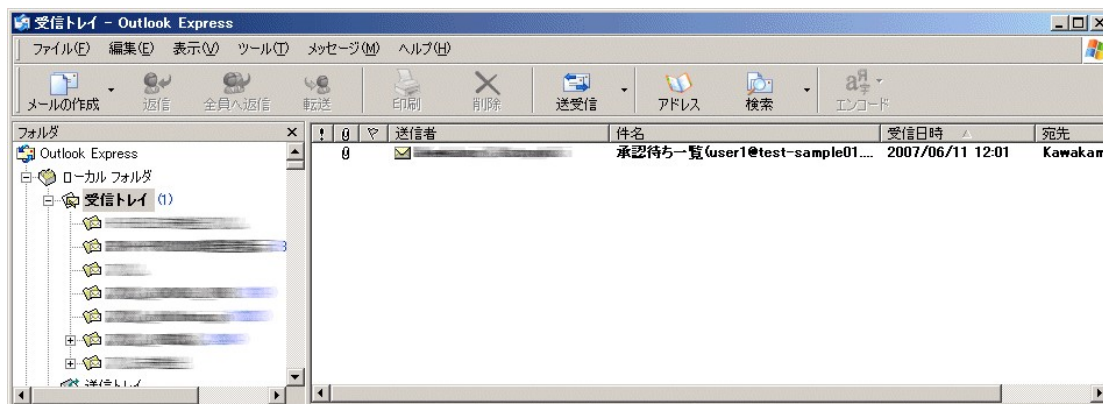
上長は、自身のメールアドレス宛に溜められている承認依頼メールの再取得を行うことができます。

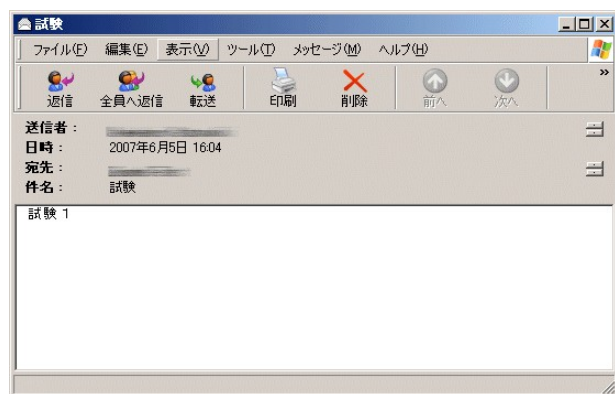
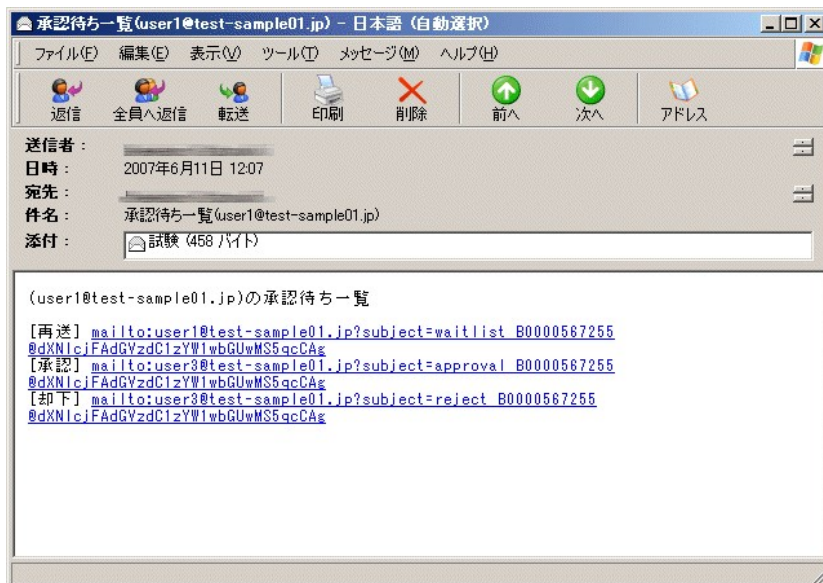
新規メールを作成しメール送信します。

(送信先は、自分宛とし、本文は記載せず、表題は、“waitlist\_<対象メール><承認者アドレス (BASE64 でエンコードされたもの)>”とします。)



メールボックスからメールを受信すると、承認依頼メールが再取得されます。





## 制御メールの書式

承認制御の方法は届いた承認依頼メールが作成した制御用リンクをクリックし、作成されたメールを送信することで処理を完了させます。

制御用リンクには、

`<承認依頼アドレス>と表題に<制御ワード>_<対象メールID@ユニーク番号>`

が含まれます。

### [制御ワード] について

制御ワードは、承認待ちフォルダに溜められたメールを操作するためのワードで以下の制御をそれぞれ行います。

表題に以下の制御ワードを記入し、承認依頼者宛にメールを送ることで、許可、拒否の動作が実施されます。

### 承認命令

`approval_<対象メールID@ユニーク番号>`

### 拒否命令

`reject_<対象メールID@ユニーク番号>`

表題に以下の制御ワードを記入し、担当上長が自分宛にメールを送ることで、担当承認待ち一覧や、承認依頼内容を再取得することができます。

### 管理者の承認待ち一覧の取得命令

`waitlist_`

### 管理者の承認依頼内容の取得命令

`waitlist_<対象メールID@ユニーク番号>`

担当上長が何らかの理由で、代理の承認者を割り当てたい場合、表題に以下の制御ワードを記入し、担当上長が自分宛にメールを送ることで、承認依頼メールを代理承認者に送信させることができます。

### 管理者の代理人設定命令

`setproxyuser_<代理承認者アドレス>`

代理の承認者を割り当てを解除したい場合、表題に以下の制御ワードを記入し、担当上長が自分宛にメールを送ることで、承認依頼メールを上長自身への送信へ戻すことができます。

### 管理者の代理人解除命令

`setproxyuser_`

代理の承認者の割り当て状態を確認したい場合、表題に以下の制御ワードを記入し、担当上長が自分宛にメールを送ることで、代理承認の設定の有無をメールで確認することができます。

### 管理者の代理人設定状態確認命令

`getproxyuser_`

## 履歴の取得

`approvalgetlog_<取得対象の年月日(YMMMDD)>`

履歴の取得は、“管理者アカウント”で定義されているメールアカウントからの要求のみ処理します。

履歴は、日単位でファイルとして保存されていますので、必要な年月日(YMMMDD)を指定します。



例1) 2007年06月20日の履歴を取得する場合

approvalgetlog\_070620

例2) 2007年06月の履歴を取得する場合

approvalgetlog\_0706

例3) 2007年の履歴を取得する場合

approvalgetlog\_07

例4) 保存されている全ての履歴を取得する場合

approvalgetlog\_

#### 履歴の削除

approvaldellog<取得対象の年月日(YMMDD)>
---------------------------------

履歴の削除は、“管理者アカウント”で定義されているメールアカウントからの要求のみ処理します。

履歴は、日単位でファイルとして保存されていますので、必要な年月日(YMMDD)を指定します。

例1) 2007年06月20日の履歴を削除する場合

approvaldeklog\_070620

例2) 2007年06月の履歴を削除する場合

approvaldellog\_0706

例3) 2007年の履歴を削除する場合

approvaldellog\_07

例4) 保存されている全ての履歴を削除する場合

approvaldellog\_

## 機械判定による一括処理

cgi-bin フォルダにある admiappr.exe をコマンドプロンプトから以下の書式で実行させる事が出来ます。  
バッチファイルやタスクスケジューラーで定期的に実行させると、管理者の操作負担が軽減されます。

### スパムサイト DB のダウンロードについて

機械判定を実行すると、当社が定期的に更新するスパムサイト DB が同時にダウンロードされ、[<実行時フォルダ>%DB] フォルダへ情報が展開されます。

※プロキシ経由の DB のダウンロードは、IE の設定内容に沿って行われます。

なお、DB データ領域は約 100MB の空き領域を確保してください。

最新のダウンロードの結果は、[<実行時フォルダ>%receiverblacklink.dat]内にタイムスタンプとして記載されます。(以下)

---

Thu Dec 29 10:23:48 2016

に更新が行われました。

---

### 書式)

**admiappr cmd=A pw=</パスワード> loopmin=<実行間隔(分)> autoaction=1 enter=<0 or 1> autopass=<機械判定による怪しい箇所数> viewfolder=<空欄または、reject>**

※pw(パスワード)は、Web からのログインパスワードと同一です。

※loopmin への指定値は繰返し実行を行う場合、その時間間隔を分単位で指定します。0又は引数が指定されない場合は、繰返さず終了します。

※autoaction への指定は、機械判定による承認、拒否の振分を実際に実行するか、しないかを指定します。(0:実行しない 1:実行する)

※enter への指定値は、ホワイト又はブラック用リストへの登録をするか、登録しないかを指定します。(0:登録しない、1:登録する)

※autopass への指定値を超えた場合が拒否対象となります。

※viewfolder への指定は、回復フォルダを選択する場合、“reject”と指定し、通常は空欄とします。

### 実行例1)

**怪しい箇所が2箇所以下は許可判定としホワイトリストへ登録、3箇所以上は拒否判定としブラックリストへ登録する場合**

```
cd C:%Program Files%EPOST%cgi-bin
```

```
. %admiappr.exe cmd=a pw=secret autoaction=1 enter=1 autopass=2
```

### 実行結果)

---

B2147497977@MDAwMDNAa3QyLnRlc3QglCAg.MSG を確認します。

下記 1 項目、怪しい箇所があります。

過去一週間以前の日付で送信されています。

評価 pass

---

:

---

B2147498002@MDAwMDNAa3QyLnRlc3QglCAg.MSG を確認します

下記 3 項目、怪しい箇所があります。

国外設定のマシンからの送信の可能性があります。(Date:ヘッダが 国外)

送信メーラの明記が見つかりません。機械的な送信の可能性があります。

エンベロープの送信元()と From:ヘッダが異なっています。(偽装されている可能性があります。)

評価 reject

---

### 実行例2)

メール回復フォルダのデータを一括で完全削除する場合

```
cd C:\Program Files\EPOST\cgi-bin
```

```
.\admiappr.exe cmd=f pw=secret autoaction=1 enter=0 autopass=0 viewfolder=reject
```

## 機械判定の内容

現在以下の23項目判定を行っています。

1. 本文の空判定
2. 添付有無判定
3. 圧縮形式添付の有無判定
4. スпамタグ付きの題名
5. ブラックリストに定義されているリンクを含む本文
6. 連続空白行検査
7. リンク数検査
8. ホップ数検査
9. 送信元記載検査
10. メッセージID 記載検査
11. 送信元が国外設定のマシン
12. 日付が未来
13. 日付が一週間前以前
14. 文字コードがシフト JIS
15. 機械的な送信
16. From:ヘッダ長判定
17. From:ヘッダ名称文字判定
18. エンベロープの送信元(%s)と From:ヘッダが不一致
19. 添付の拡張子が実行可能形式
20. 添付の圧縮ファイル内に実行可能形式のファイルの有無
21. 添付の圧縮ファイル内に圧縮形式のファイルの有無
22. 添付ファイル名が長い
23. 添付ファイル名に連続した空白文字

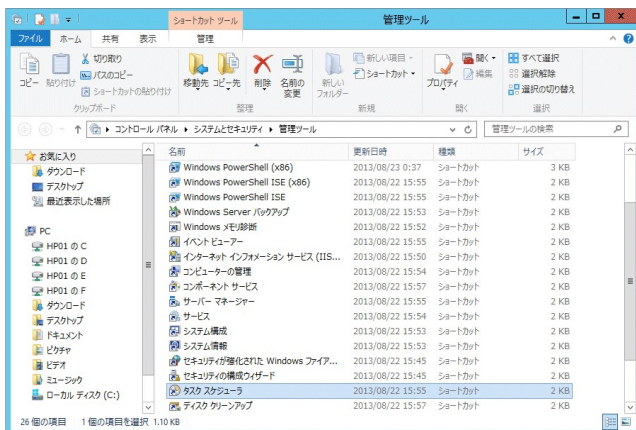
## 自動化(タスクスケジューラへの登録)

cgi-bin フォルダにある securehandler.bat をタスクスケジューラに登録することで、定期的に機械判定による一括処理を自動で行うことができます。

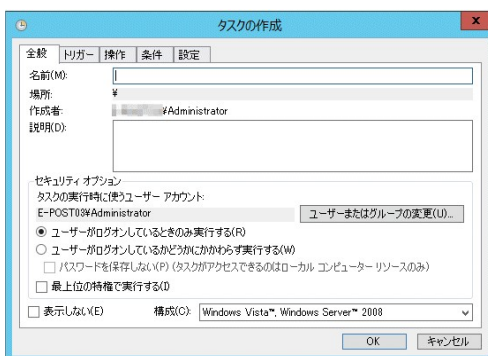
拒否判定されたメールは回復フォルダに保存されますので、判定間違いのメールがあれば、管理者が改めて承認直すことができます。

## Windows Server 2012R2 での設定例

“管理ツール”または“コンピュータの管理”から、“タスクスケジューラ”を起動します。



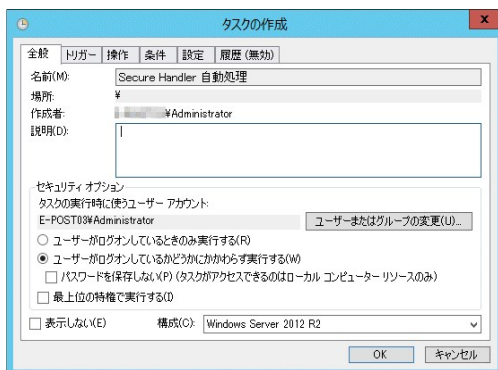
起動したタスクスケジューラの管理画面から、“タスクの作成”をクリックすると“タスクの作成”ダイアログが表示されます。



“名前(M)”に任意の名称を登録します。

“セキュリティ オプション”の“ユーザーがログオンしているかどうかにかかわらず実行する(W)”を選択します。

“構成(C)”で“Windows Server 2012 R2”を選択します。

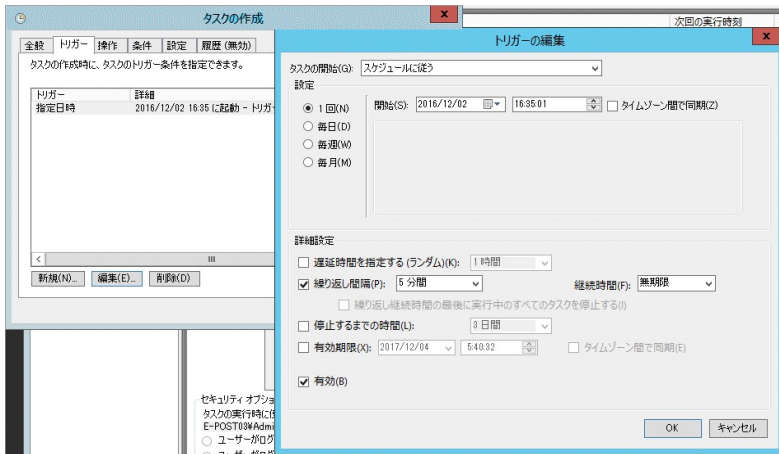


“トリガー”タブを選択します。

“新規(N)”をクリックし、“タスクの開始(G)”を“スケジュールに従う”にします。

“設定”を“1 回(N)”を選択し、“開始(S)”は開始させたい任意の日時とします。

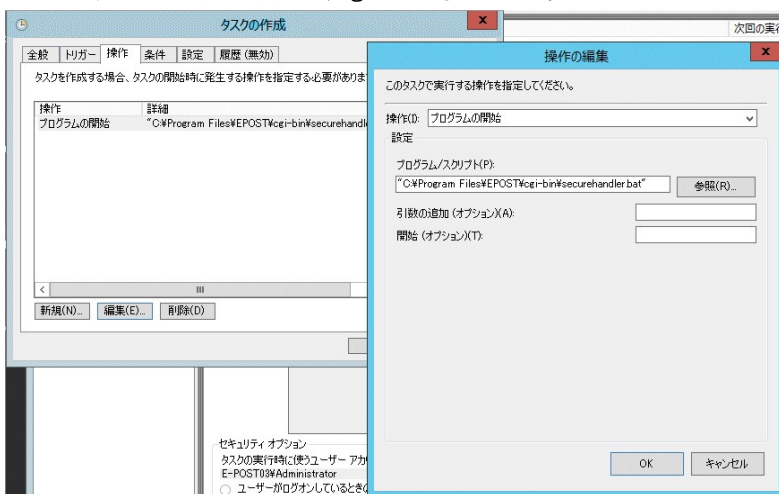
“詳細設定”で“繰り返し間隔(P)”をチェックし、任意の間隔を選択します。



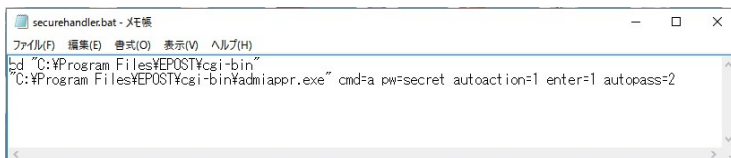
“操作”タブを選択します

“新規(N)”をクリックし、“操作(O)”で“プログラムの開始”を選択します。

“プログラム/スクリプト(P)”で、cgi-bin フォルダにある securehandler.bat を登録します

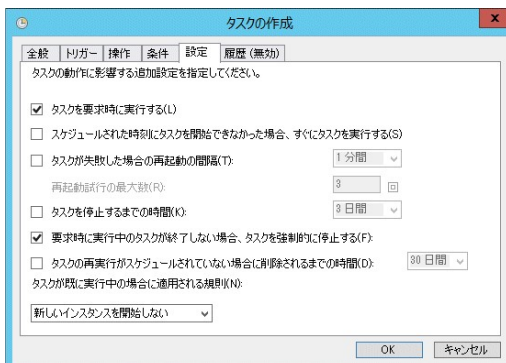


指定した、securehandler.bat の内容はデフォルトで以下となっています。  
パスワードや、判定値は設定環境に応じて編集してください。

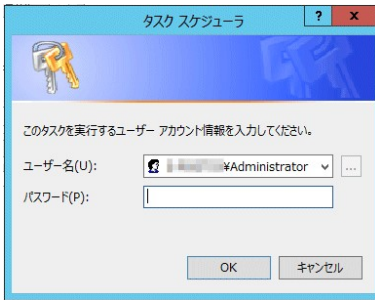


“設定”タブを選択します

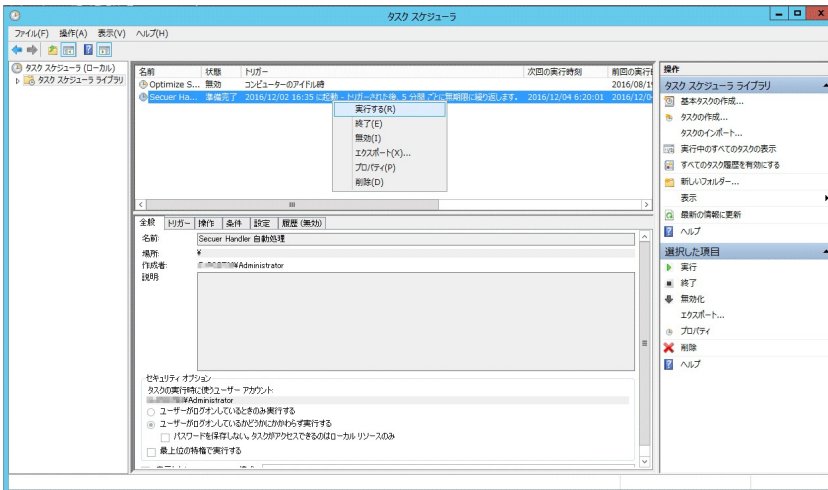
“タスク要求時に実行する(L)”をチェックします。



OK ボタンを押すと、実行するアカウントとパスワードを要求されますので、管理者権限を持つアカウントとパスワードを登録すると、設定が完了します。



登録されたタスクを実行するには、タスクスケジューラの管理画面から作成したタスクを右ボタンでクリックしたメニューの“実行する(R)”をクリックします。



正しく実行されているか否かは、実際に任意のメールを送信し、定期的に承認もしくは、拒否で回復フォルダへの移動処理が行われているか否かを確認します。

## admiappr.ini について

'admiappr.ini'ファイルは、WEB 管理用 CGI'admiappr.exe'へ実行時オプションを指定するファイルです。

```
admiappr.ini - メモ帳
ファイル(F) 編集(E) 書式(O) 表示(V) ヘルプ(H)
'管理者ID
id=admin

'パスワード
pw=secret

'承認管理URL
urlpath=/approval/

'HTMフォルダ
html=C:\Program Files\EPOST\admiappr%

'承認待ちメールフォルダ
approval=C:\mail\approval%

'メール作業フォルダ
work=C:\mail%

'ローカルドメイン一覧(カンマ区切り eg. domain1.jp, domain2.jp)
localdomain=local.domain

'ホワイトリストへの登録までの許可設定回数(グレイリストでの保持回数)
whitecount=1

'拒否アドレステーブル
blackaddr=C:\Program Files\EPOST\MS\receiverblackaddr.dat

'保留アドレステーブル
grayaddr=C:\Program Files\EPOST\MS\receivergrayaddr.dat

'許可アドレステーブル
whiteaddr=C:\Program Files\EPOST\MS\receiverwhiteaddr.dat

'拒否語名テーブル
blackword=C:\Program Files\EPOST\MS\receiverblackword.dat

'保留語名テーブル
grayword=C:\Program Files\EPOST\MS\receivergrayword.dat

'許可語名テーブル
whiteword=C:\Program Files\EPOST\MS\receiverwhiteword.dat

'拒否リンクテーブル
blacklink=C:\Program Files\EPOST\MS\receiverblacklink.dat

'許可リンクテーブル
whitelink=C:\Program Files\EPOST\MS\receiverwhitelink.dat

'リンクDB更新サイト
update site=fastscan.on.coocon.jp

'リンクDB更新間隔(時間)
update time=4

'文字コード
code=SHIFT-JIS

'ページあたりの表示行
rege=20

'無操作タイムアウト時間(秒)
time out=900

'ブラックホワイト各テーブルへの登録 0:しない 1:する
entry=1

'添付ファイルのダウンロード許可 0:許可 1:拡張子除去 2:禁止
attach=1

'テーブル表示コード 0:UTF8 1:JIS
rawtable=0

'テーブル最適化 0:しない 1:する
optimize=1

'自動処理のマルチスレッド数
maxthread=20
```

指定内容は以下の通りとなります。

**管理者ID** id=admin (デフォルト admin)  
管理者ログオンIDが指定されます。  
実際の運用時には、変更することも可能です。

**パスワード** pw=\*\*\*\*\* (デフォルト secret)  
ログオンパスワードが指定されます。  
実際の運用時には、任意のパスワードに変更してください。

**承認管理 URL** urlpath=/approval/  
リンク先フォルダ名を指定します。

**HTM フォルダ** html=C:\Program Files\EPOST\admiappr%

上記「承認管理 URL」で実際に利用される HTML ファイル群が保存されているフォルダ名です。

**承認待ちメールフォルダ** approval=c:¥mail¥approval¥

インバウンドメールの保留フォルダ先で、メールサーバ設定時の「作業フォルダ」¥approval¥が指定されます。メールサーバの設定により「作業フォルダ」を適切に変更してください。'approval'は変更してはいけません。

**メール作業フォルダ** work=c:¥mail¥

メールサーバ設定時の作業フォルダを設定します。

**ローカルドメイン一覧(カンマ区切り eg. domain1.jp, domain2.jp) localdomain=local.domain**

メールサーバ設定時の内部ドメイン名を、カンマ区切りで設定します。

**ホワイトリストへの登録までの許可設定回数(グレーリストでの保持回数) whitecount=<許可が必要な回数>**

WEB 管理で対象となるメールを許可を実施して対象の送信元エンベロープと題名が、ホワイトリストに登録されるまでにグレーリストとして保持する回数です。

このカウント値が0である場合は、即時ホワイトリストへ反映されます。

**拒否アドレステーブル** blackaddr=C:¥Program Files¥EPOST¥MS¥receiverblackaddr.dat

<メールサーバプログラムインストールフォルダ>¥receiverblackaddr.dat が指定されます。

メールサーバの設定により「メールサーバプログラムインストールフォルダ」を適切に変更してください。

'receiverblackaddr.dat'は変更してはいけません。

**保留アドレステーブル** grayaddr=C:¥Program Files¥EPOST¥MS¥receivergrayaddr.dat

<メールサーバプログラムインストールフォルダ>¥receivergrayaddr.dat が指定されます。

メールサーバの設定により「メールサーバプログラムインストールフォルダ」を適切に変更してください。

'¥receivergrayaddr.dat'は変更してはいけません。

**許可アドレステーブル** whiteaddr=C:¥Program Files¥EPOST¥MS¥receiverwhiteaddr.dat

<メールサーバプログラムインストールフォルダ>¥receiverwhiteaddr.dat が指定されます。

メールサーバの設定により「メールサーバプログラムインストールフォルダ」を適切に変更してください。

'receiverwhiteaddr.dat'は変更してはいけません。

**拒否題名テーブル** blackword=C:¥Program Files¥EPOST¥MS¥receiverblackword.dat

<メールサーバプログラムインストールフォルダ>¥receiverblackword.dat が指定されます。

メールサーバの設定により「メールサーバプログラムインストールフォルダ」を適切に変更してください。

'receiverblackword.dat'は変更してはいけません。

**保留題名テーブル** grayword=C:¥Program Files¥EPOST¥MS¥receivergrayword.dat

<メールサーバプログラムインストールフォルダ>¥receivergrayword.dat が指定されます。

メールサーバの設定により「メールサーバプログラムインストールフォルダ」を適切に変更してください。

'receivergrayword.dat'は変更してはいけません。

**許可題名テーブル** whiteword=C:¥Program Files¥EPOST¥MS¥receiverwhiteword.dat

<メールサーバプログラムインストールフォルダ>¥receiverwhiteword.dat が指定されます。

メールサーバの設定により「メールサーバプログラムインストールフォルダ」を適切に変更してください。

'receiverwhiteword.dat'は変更してはいけません。

**拒否リンクテーブル** blacklink=C:¥Program Files¥EPOST¥MS¥receiverblacklink.dat

<メールサーバプログラムインストールフォルダ>¥receiverblacklink.dat が指定されます。

メールサーバの設定により「メールサーバプログラムインストールフォルダ」を適切に変更してください。

'receiverblacklink.dat'は変更してはいけません。



**許可リンクテーブル** whiteword=C:\Program Files\EPOST\MS\reciverwhitelink.dat

<メールサーバプログラムインストールフォルダ>\reciverwhitelink.dat が指定されます。

メールサーバの設定により<メールサーバプログラムインストールフォルダ>を適切に変更してください。

'reciverwhitelink.dat'は変更してはいけません。

**リンク DB 更新サイト** updatesite=fastscan.on.coocan.jp

判定の自動化を実施する際、弊社が提供するスパムサイトや危険なサイトの最新データベースをダウンロードするサイトを指定しています。

※接続は、IE の接続設定に依存します。

**リンク DB 更新間隔(時間)** updatetime=4

上記リンク DB 更新サイトからダウンロードし直す間隔を時間単位で指定します。(デフォルトでは4時間で指定してあります。)

※データベースの更新は、使用期間を過ぎるとライセンスキーを登録するまで実行が行えなくなり、次年度毎に更新を行う必要があります。

**文字コード** code=SHIFT-JIS

上記、reciverblackword.dat,reciverwhiteword.dat に保管される際の文字コードです。

変更はできません。

**ページあたりの表示行** rengo=20

WEB 管理でメール一覧への1ページあたりに表示できるメール数を指定します。

**無操作タイムアウト時間(秒)** timeout=900

WEB 管理をログオンしたままの無操作状態が一定期間あった場合に、再びログオンを必要とさせる時間を設定します。

**ブラックホワイト各テーブルへの登録** 0:しない 1:する entry=1

WEB 管理からや自動処理実行時に操作結果を登録するかしないかの起動時の初期値を設定します。

**添付ファイルのダウンロード許可** 0:許可 1:拡張子除去 2:禁止 attach=1

WEB 管理からメール内の添付ファイルをダウンロードする際に、拡張子を除去することにより、添付ファイルを無害化(WINDOWS 上で実行できない)するか否かの設定です。

**テーブル表示コード** 0:UTF8 1:JIS rawtable=1

WEB 管理からキーワードテーブルの編集時に、UTF8 に変換し表示するか、テーブルの生データのまま表示するかの設定をします。

**テーブル最適化** 0:しない 1:する optimize=1

自動処理実行時に作成したテーブル内に登録したデータの重複除去や、ワイルドカード指定化による最適化を実施するか否かの設定をします。

**自動処理のマルチスレッド数** maxthread=20

自動処理実行時に同時処理するメール数を指定します。

**To:ヘッダに記載可能な上限アドレス数** max\_to=0 未定義の場合:0=制限なし

'To' ヘッダに記載されている送信先アドレス数が指定した数を超えさせたくない場合に設定します。

**Cc:ヘッダに記載可能な上限アドレス数** max\_cc=0 未定義の場合:0=制限なし

'Cc' ヘッダに記載されている送信先アドレス数が指定した数を超えさせたくない場合に設定します。

会社名および 担当部署名	
お名前	フリガナ：
ご住所	フリガナ：
	都 道 市・区・郡 府 県
	区・町・村
TEL / FAX	Tel. (      )      —      Fax. (      )      —
E-MAIL アドレス	
製品名及び ライセンスキーNo.	
使用OS	何れかに○をつけてください。 1. Windows server 2016   2. Windows server 2019   3. Windows server 2022 4.その他
メインメモリサイズ	
お問合せの内容（できるだけ詳しく記載をお願いいたします。）	

発売元 **株式会社 イー・ポスト**

〒169-0075

東京都新宿区高田馬場1-33-14 サンフラワービル

TEL. 03-5272-5386 FAX 03-6856-9729