

	E-Post SMTP Server (x64) Standard シングルサーバ版 続き
アカウント	SMTP受信制限設定【effect.dat】 ○ (指定アドレス・ドメインの受信許可／受信禁止)
	SMTP認証設定 ○ (認証あり・認証なし)
アカウント情報のインポート・エクスポート	○ (*14)
エイリアス	○ (*15)
エイリアス情報のインポート・エクスポート	○ (*14)
メーリングリスト機能	○ (連番、表題、Reply-To:ヘッダ、投稿パスワード、添付ファイル削除、投稿内容保管など)
メーリングリスト情報のインポート・エクスポート	○ (*14)
メーリングリストメンバーのインポート・エクスポート	○ (*14)
対応IPバージョン	IPv4／IPv6
ログ取得機能	接続マシン／SMTP受信／ SMTP送信／SMTPローカル送信／ SMTP配送失敗／SMTP配送詳細／ SMTP受信詳細／ ――
管理面のセキュリティ	○ (システム環境パスワード／ドメイン管理パスワード／ メールボックスフォルダのデータ暗号化／アカウント情報エクスポート時のパスワード暗号化)
Web管理機能	○ (*16) (3階層:システム管理者・ドメイン管理者・個別ユーザー)
コマンド操作機能(コンソール機能)	○ (*17) (システム環境／ドメイン管理／アカウント管理／エイリアス設定／メーリングリスト設定など)
迷惑メール対策	ORDB参照(DNSBL方式)機能、SURBL/URIBL方式による参照機能(メールフィルタ)
送信ドメイン認証対応	SMTP受領時での DMARC/DKIM/SPF/ARC 対応機能 new! (オプションのアドオンツール「サポート2」よりダウンロード) (*18)
簡易アーカイブ(メールバックアップ)	全メール複写機能 及び ジャーナルオプション機能(「サポート2」よりダウンロード)
ログ解析・集計 レポート機能	ログ解析・集計レポート機能 (付属ツールE-Post Loganalyzerによる)
メールボックス使用状況 レポート機能	メールボックス使用状況レポート機能 (付属ツールE-Post Loganalyzerによる) (*19)
ユーザーへのメールボックス 使用量警告メール機能	ユーザーへのメールボックス使用量警告メール機能 (付属ツールE-Post Loganalyzerによる) (*19)

- (※5) ネットワーク負荷のない理想的な環境でのメールサイズ2〜3KB程度による試験結果です。メールフィルタの設定を多数登録しているとき、設定量だけ負荷がかかり、配送能力は低下します。
- (※6) SSL/TLS通信を検証するだけなら自己認証局でも十分ですが、本格運用にあたっては正規の認証局(CA)による証明書発行と取得が必要です。なお2019年1月公開の20181224最新差分アップデート以降を適用した最新版では、SSLは廃止され、TLS1.0〜TLS1.3に対応します。
- (※7) STARTTLS(SMTP)と SMTP Over SSL との違いですが、SMTP Over SSL が465番ポートで接続時点から”暗号通信”されるのに比べ、STARTTLS は25番ポートのまま接続、最初は”プレーン通信”でネゴシーション後に途中から”暗号通信”を開始するという基本的な違いがあります。設定の要点は、STARTTLS の受信時には(※6) のSSL(TLS)の証明書・鍵情報をそのまま用いる一方、送信時には「ESMTPで送信」を有効設定にするだけで STARTTLS の送信が可能になります。
- (※8) 認証ファイルによりユーザーごとのSMTP認証有無設定が可能です。またSMTP認証付きで外部SMTPへの送信リレー設定を行う場合、組み合わせる外部のホスティング・レンタルサーバは原則、SMTP AUTH(SMTP認証)を実施していることを前提としています。
- (※9) 2021年4月以降の最新差分アップデートを適用することが必要です。さらにIISなどのWebサーバ動作環境が必要です。
- (※10) CGIツールの getattach.exe は次年度更新用CDに収録されるほか、「サポート2」サイトよりダウンロード可能です。
- (※11) SMTPでのユーザー情報が連携されます。SMTP認証パスワードについては連携はありません。
- (※12) 自動転送機能と自動応答機能とは排他でいずれかの設定が可能です。両方とも有効にする設定はできません。また自動応答機能での自動応答文はJIS(iso-2022-jp)に変換して登録する必要があります。Web管理ツールから登録する場合は強制的にJIS(iso-2022-jp)で登録されるので変換する必要はありません。
- (※13) 追加処理プログラムで指定できるのは標準コンソールベースで動作するプログラムに限られます。GUIベースのプログラムは実行できません。
- (※14) タブ区切り形式テキスト(TSV)により可能です。
- (※15) エイリアスは実アカウントとの関連づけが原則です。エイリアスどうしの関連づけは対応しません。なお、作成エイリアスは必要ライセンス数としてカウントされます。
- (※16) IISなどのWebサーバ動作環境が必要です。
- (※17) Web管理ツールが動作するよう設定されている必要があります。
- (※18) SMTP受領時でのDMARC対応ツールは2024年6月公開の送信(DMARC)アドオン EPSTDIMARC v1.06cです。EPSTDIMARCを設定することでDMARC/DKIM/SPF/ARCのすべてを含む対応が可能となります。その他従来からのツールとしては、DKIM対応ツールの送信ドメイン認証(DKIM)アドオン EPSTDIM v1.04a、SPF対応ツールの送信ドメイン認証(SPF)アドオン GETSPF v1.07です。EPSTDIMARC・EPSTDIMは次年度更新用CDに収録されるほか、すべて「サポート2」サイトよりダウンロード可能です。
- (※19) 2018年7月公開の最新差分アップデートならびにそれ以降のモジュールでのE-Post Loganalyzerに実装された機能です。なお、SMTP Serverには、POP3/IMAPプロトコルを実装していないため、警告メールを送信することはできても、実際にユーザーが警告メールを読み出す手段はありません。

動作環境		必要ライセンス数について
対応OS	Windows Server 2016 / 2019 / 2022 (*20)	E-Post Secure Handler (x64) の必要ライセンス数はユーザー数であり、E-Post SMTP Server (x64) シリーズの必要ライセンス数は「アカウント数＋エイリアス数＋メーリングリスト設定数」の合計数です。
組み込み可能なE-Post	64bit版 E-Post SMTP Server (x64) シリーズ、64bit版 E-Post Mail Server (x64) シリーズ (*21)	E-Post Secure Handler (x64) および E-Post SMTP Server (x64) シリーズのパッケージは、50user版/100user版/250user版という区切りになっています。たとえば150の必要ライセンスが想定される場合は、必要ライセンス数が充足するよう250user版をお求めください。
適正ユーザー数規模	50userから250userまでの規模	
内部メールサーバ	E-Post Mail Serverシリーズ その他、RFCに準拠した他社製メールサーバ	ライセンス認証について 「ライセンスキー」を入力して、ライセンス登録を行う際、80番ポートを使って弊社認証サーバとの間で通信が行われます。通信は、Windowsのインターネットオプション設定を参照します。閉じられたイントラネット環境で、Standard版をご利用になる場合でも、初回のライセンス登録時だけは、インターネット接続環境で認証していただく必要があります。ライセンス登録時でさえもインターネットに接続できない環境でご使用開始せざるを得ない場合は、作業員が赴き、手動でライセンス登録する、いわゆるアクティベーション作業を承ります。こちらは有償(首都圏以外は交通費別途)にて承っております。依頼される場合は、弊社営業担当までご相談ください。
対応ブラウザ (許可・拒否・回復等)	Microsoft Edge、Mozilla Firefox、Google Chromeなど主要ブラウザ (*22)	
対応メールクライアント (許可・拒否)	Windows Mail、Microsoft Outlook、Lotus Notes8.5、Mozilla Thunderbird、Becky!、ShurikenなどRFCで規定されているmailtoリンクがフルに使用可能な主要メールクライアントソフト (*23)	

- (※20) 64bit版 E-Post (x64) シリーズは64bitOS環境で64bitアプリケーションとして動作します。Windows Serverのエディションは利用制約の少ないStandardエディション以上をお薦めします。なお、Windows Server の日本語環境での運用が前提です。
- (※21) E-Post BossCheck Option (x64) とは併用できません。
- (※22) ブラウザで許可・拒否・回復などの操作を行うのがメインの操作となります。
- (※23) メールクライアントでも許可・拒否設定を行えますが、サブ操作としての位置づけです。mailtoリンクの動作が保証されないWebメールでは対応が困難なことがあります。

その他

E-Postシリーズはサーバ製品のため、Webメールクライアント機能は搭載していませんが、オープンソースの日本語対応WebメールソフトであるRoundcube Webmail や RainLoop についてインストールガイド・ユーザーズガイドを独自に作成、サイトに公開しております。



仕様表はこちらからもご覧いただけます

開発・販売元

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

<https://www.e-postinc.jp>

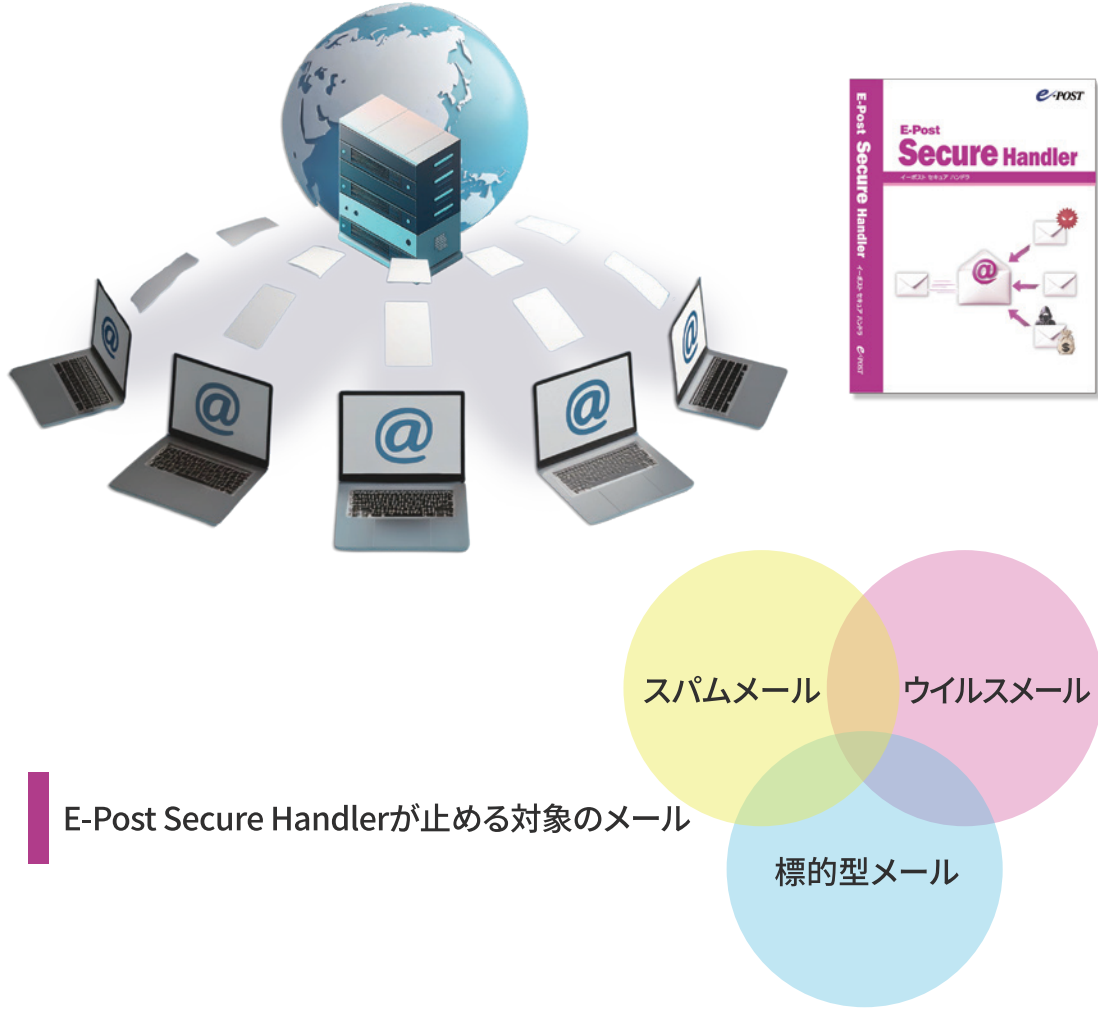
問合せは sales@e-postinc.jp



標的型メール攻撃も防御するメールゲートウェイソフトウェア

E-Post Secure Handler

イーポスト セキュア ハンドラ



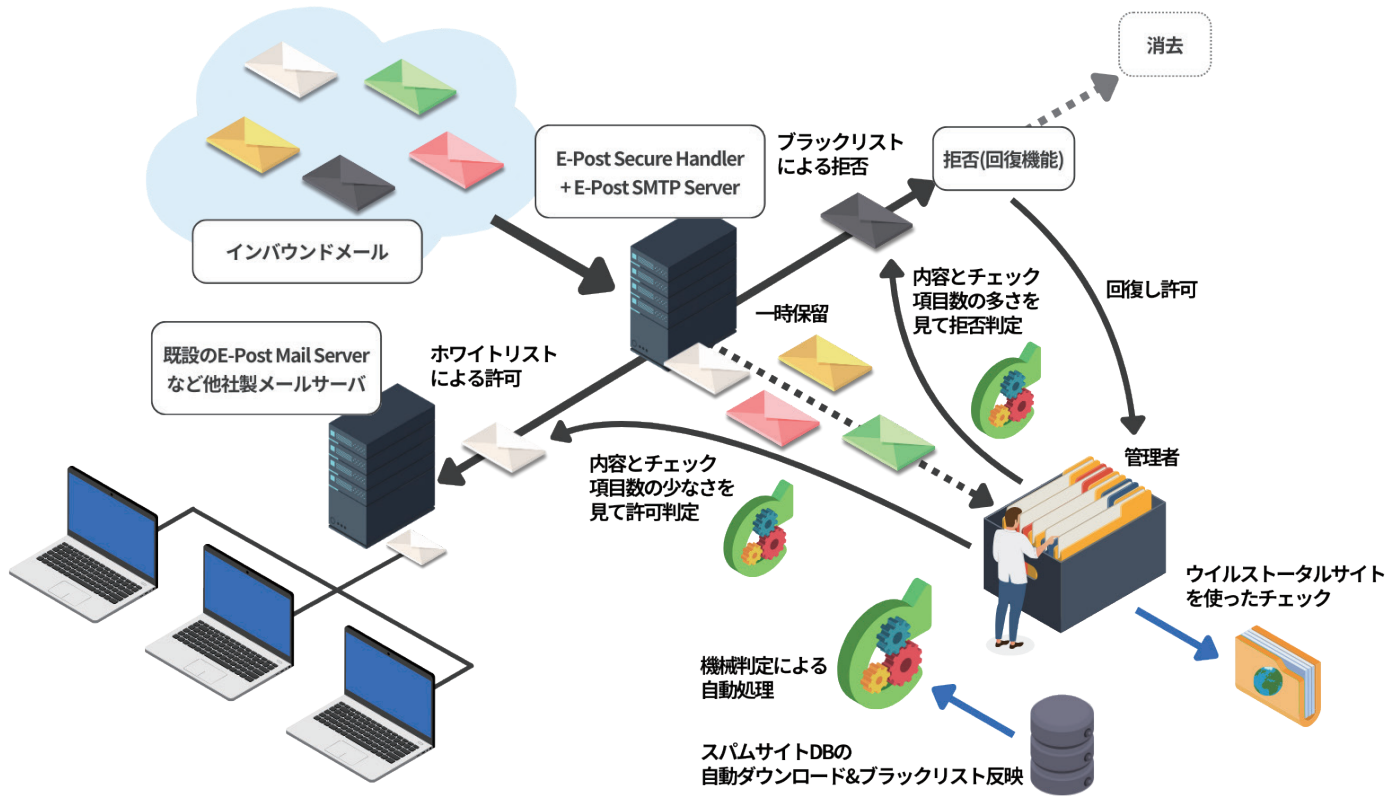
E-Post Secure Handlerが止める対象のメール

E-Post Secure Handlerは、外部から届けられるインバウンドメールについて、ブラックリストにより拒否、ホワイトリストにより許可する一方、それ以外の不審なメールや不明なメールをすべて一時保留します。一時保留メールは、許可か拒否のいずれかの自動判断がアプリにより処理されます。管理者は必要に応じて保留中メールをブラウザやメーラーで確認し、安全なメールとして受信を許可するか拒否するかの判断を行えます。

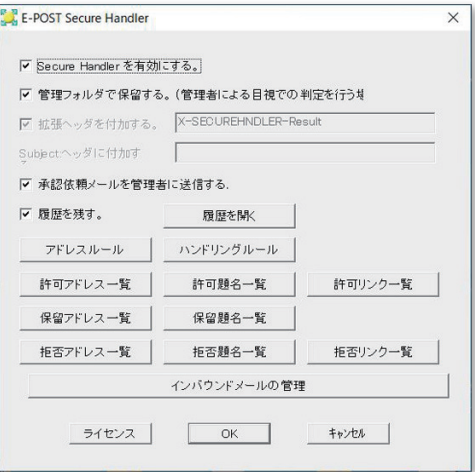
総合的視点からウイルスを含むマルウェアやスパムメールのみならず、標的型メール攻撃などに対しても最高の防御となりうるインバウンド承認・自動判断機能をもつメールゲートウェイです。

E-Post Secure Handler (x64)

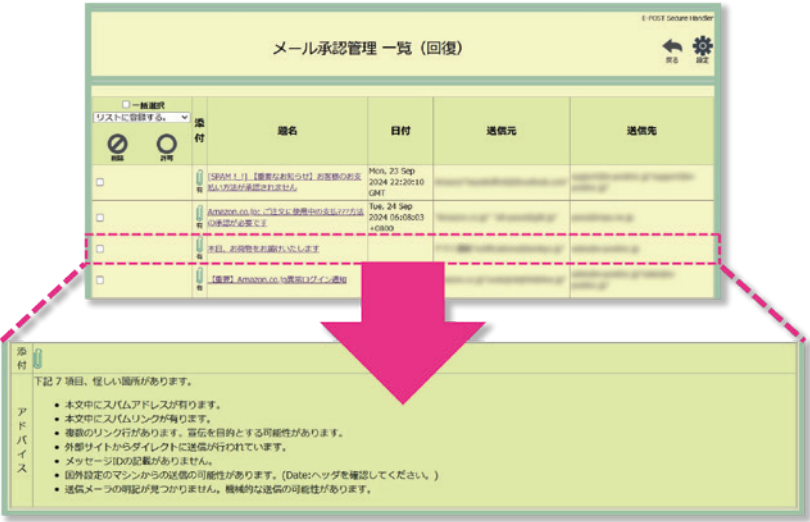
全体構成と機能概要



- 外部から届けられるインバウンドメールのうち、安全なメールのみ通すセキュアな純国産メールゲートウェイ
- ホワイトリストとブラックリスト以外のメールは一時保留され、管理者がブラウザやメーラーで受信拒否か受信許可かを判断可能
- 一時保留したメールは23個のチェック項目で判定、不審メールと判断されるポイントをわかりやすく表示
- 怪しい添付ファイルや未知のウイルスメールでもアンチウイルスベンダーの最新情報が集積しているウィルストータルサイトでチェック可能
- 許可されたメールはホワイトリストへ、拒否されたメールはブラックリストへそれぞれのデータテーブルに自動登録
- いったん拒否したが後で必要なメールだとわかった場合にもその場で回復が可能
- 管理者がいちいち判断して作業する手間を省くため、許可／拒否を自動的に機械判定させるコマンドを用意、継続的な自動処理が可能
- スパムサイトや危険サイトの最新データのダウンロード機能が装備、拒否リンカー一覧テーブルによりスパムサイトのリンク情報をチェック、拒否させることが可能
- SMTPゲートウェイE-Post SMTP Server(x64)を標準装備、SMTPエンジンからWeb管理ツールまですべてオリジナルの純国産
- 数多くの導入実績を誇る64bit対応のWindows版メールサーバソフトウェアE-Post Mail Server(x64)との組み合わせに最適



Secure Handler 管理画面



Secure Handler 承認管理画面

E-Post Secure Handler (x64) 仕様・機能一覧表

	E-Post Secure Handler (x64) (*0)
メール保留条件 (ハンドリングルール)	・エンベロープの受信先(ドメイン・アカウント) ・エンベロープの送信元(ドメイン・アカウント) ・メールヘッダの受信先(ドメイン・アカウント) ・題名でのキーワード ・リンク情報(本文掲載のURL) ※いずれも複数指定(ワイルドカード指定)可
判定方法	・保留メール通知からのメールによる許可・拒否判定操作 ・ブラウザから保留メール閲覧による許可・拒否判定操作 (*1) ・アプリによる許可・拒否自動判定 (*2) (*3)
強制拒否(ブラックリスト)	・送信元エンベロープの登録・削除・閲覧(システム・ブラウザ) ・題名の登録・削除・閲覧(システム・ブラウザ) ・リンク情報(本文掲載のURL)の登録・削除・閲覧(システム・ブラウザ) (*4) ※いずれも複数指定(ワイルドカード指定)可
強制許可候補確認	・アプリにより許可判定された送信元エンベロープ・題名を直接リスト登録せず目視による操作で最終判定
強制許可(ホワイトリスト)	・送信元エンベロープの登録・削除・閲覧(システム・ブラウザ) ・題名の登録・削除・閲覧(システム・ブラウザ) ・リンク情報(本文掲載のURL)の登録・削除・閲覧(システム・ブラウザ) ※いずれも複数指定(ワイルドカード指定)可
メンテナンス	・判定待ちリストの取得機能(承認者) ・履歴の取得・履歴の削除(管理者のみ) ・許可・拒否の結果履歴ログ(システム)
拒否メール判定回復機能	・判定ミス等で保留ないし拒否されたメールを許可メールとして回復(ブラウザ・管理者) ・各ユーザーログイン情報設定によりユーザー別に保留されたメール回復も可能(ブラウザ・各アカウント)

(*0) E-Post SMTP Server (x64) 付属ありの[フルモデルSMTPゲートウェイタイプ]と、E-Post SMTP Server (x64) 付属なしの[組み込み型オプションタイプ]に製品が分かれます。[組み込み型オプションタイプ]は、E-Post Mail Server Standard (x64)、E-Post Mail Server Enterprise II (x64)、E-Post SMTP Server Enterprise II (x64) と組み合わせて使用する場合にご選択ください。
(*1) ブラウザによる保留メール閲覧による許可・拒否判定を行うには、Windows ServerにIISを機能追加し、なおかつCGIが動作する設定にする必要があります。またブラウザによる閲覧時には、23個のチェック項目によって不審メールと判断されるアドバイス情報が表示されます。不審な添付ファイルがある場合、Virus Total (ウィルストータル) サイトでのウイルス・マルウェア検査を行うよう促します。
(*2) 定期的に自動判定を行う場合は、自動実行するコマンドを呼び出すバッチファイルを用意されていますので、そのバッチファイルをOSで用意されているタスクスケジューラへ登録することが必要です。アプリによる許可・拒否自動判定を行うコマンドは次年度更新継続が前提です。
(*3) 自動判定実行時には、弊社独自に用意したスパムリンクデータベースが運用マシン上にダウンロードされます。利用には100MB程度の空き領域が別途必要です。データベースダウンロードは次年度更新継続が前提です。
(*4) 自動判定実行時にダウンロードされたスパムリンクデータベースは、拒否リンカー一覧テーブル(リンク情報のブラックリスト)に自動的に反映され、スパムメールや危険なメールを拒否する判定目的に利用されます。

	E-Post SMTP Server (x64) Standard シングルサーバ版 〔 E-Post Secure Handler (x64) には標準で付属します SMTP Serverを付属しない組み込みオプションタイプもあります〕
配送性能 (運用環境により異なります)	～30万通/時間 (*5)
管理ドメイン数	最大512ドメイン
対応プロトコル	SMTP
暗号化通信 (xxxx over SSL[TLS])	SMTP over SSL(TLS) (*6)
暗号化通信 (STARTTLS)	STARTTLS (SMTP) (*7)
SMTP認証 (SMTP AUTH)	○ (*8) (PLAIN, LOGIN, CRAM-MD5)
SMTP認証 送信者の信頼度設定	○ (3段階: SMTP認証ID・SMTP認証ID=エンベロープ・SMTP認証ID=エンベロープ=ヘッダFROM)
接続 ロック アウト	SMTP認証接続ロックアウト機能 ○ (設定回数以上SMTP認証失敗した同一IPアドレスに対する指定時間の接続ロックアウト ／指定IPアドレスに対する永続的な接続ロックアウト／指定IPアドレスに対する接続許可)
	IPロックアウト機能 ○ (設定回数以上SMTPで連続接続してくる同一IPアドレスに対する指定時間の接続ロックアウト ／指定IPアドレスに対する永続的な接続ロックアウト／指定IPアドレスに対する接続許可)
SMTPゲートウェイ機能・フォワード機能 ゲートウェイテーブル【gateway.dat】	○ (フォワード先固定／対象ドメインごとの振り分け／対象メールアドレスごとの振り分け) (SMTP認証付きで外部SMTPへの送信リレー設定も可能)
中継の制限機能 (SMTP受信送信の制限)【effect.dat】	○ (IPアドレスや接続ドメイン名、メールアドレスでの許可・接続拒否、中継の許可・禁止など)
ORDB参照機能 (DNSBL方式サイト参照)【ordb.dat】	○
SMTP配送の詳細設定	○ (全体共通設定 永続的拒絶時のリトライ／一時拒絶時のリトライ／サーバ無応答時のリトライなど)
SMTP配送の利用時間設定【usetime.dat】	○ (全体共通設定)
SMTP配送・SMTP受信時の添付ファイル分離 およびファイル受信通知	○ (*9) (メールデータEMLファイルの取得とファイル受信通知[メールストレージ機能] ／CGIツール (*10) を使った添付ファイルの分離・取得とファイル受信通知[メールストレージ機能])
SMTP受信メールサイズ制限・同報数制限	○ (全体共通設定)
メールボックス保管サイズ制限	○ (全体共通設定)
メールフィルタ設定【mail.dat】	○ (全体共通設定 タイトル／本文／ヘッダ／SPAM判定用にURIBL [SURBL] サイト参照 ／拒否／タグ付け通過／指定アカウントへの転送など)
ActiveDirectoryユーザー管理との連携	△ (*11)
E-Post独自方式ユーザー管理	○
アカ ウン ト 別 設定	自動転送設定 ○ (*12) (自動転送時の送信元指定など)
	自動応答設定 ○ (*12)
	「メール制御」機能での追加処理プログラム ○ (*13)
	メールボックス保管サイズ制限 ○
	個別メールフィルタ設定【mail.dat】 ○
	利用時間設定 ○
送信先制限設定【sender.dat】	○ (指定アドレス・ドメインの送信許可／送信禁止)