

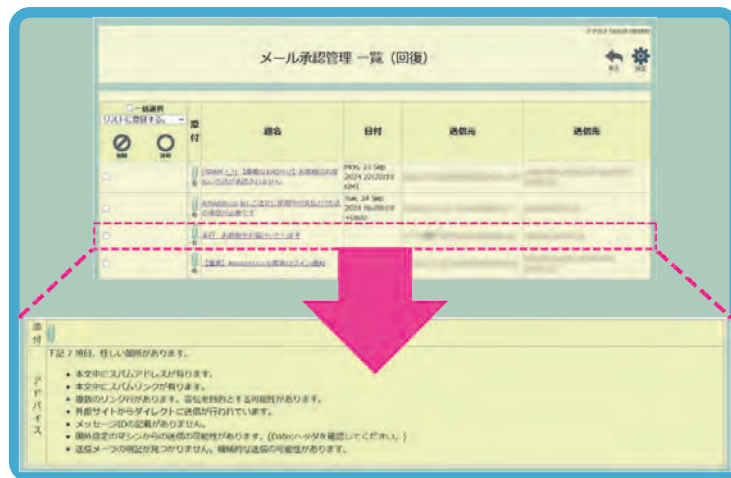
Web管理機能

Webからのシステム管理が可能。
1カ所でまとめて管理できる「コントロールセンター」

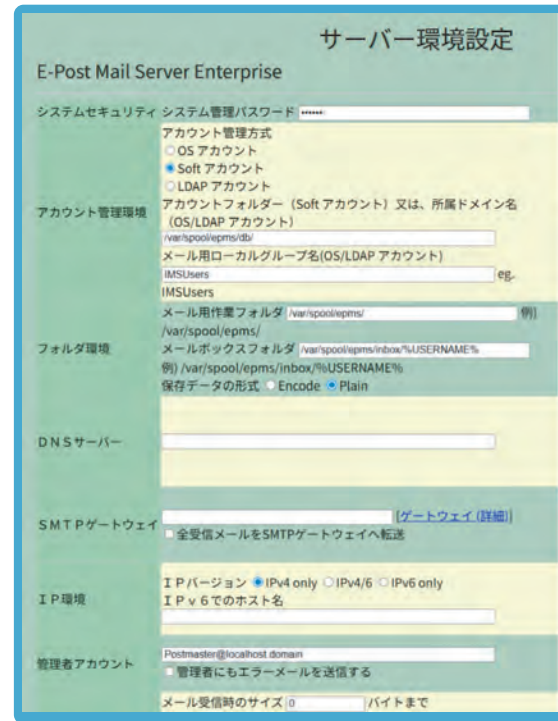


メール承認管理機能 ※Enterprise版のみ

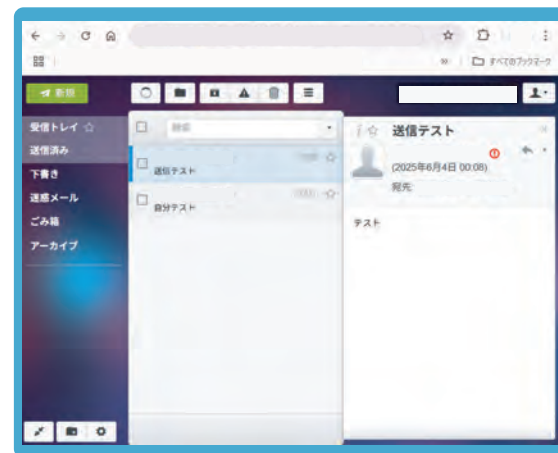
メールは23個のチェック項目で怪しさを判定、
不審なメールは一時保留され判定ポイントをわかりやすく表示。



サーバー設定画面



RainLoop設定後画面 (イメージ)



即日稼働のOS込みメールサーバアプライアンスモデル

E-Post Mail Server V

イーポストメールサーババイ

豊富な導入実績のある
E-Postシリーズを、アプライアンスに。
設置してすぐに使える、安心の専用機。



仕様表はこちらからご覧いただけます。

E-Post
Mail Server V



Windows版の説明資料ですが、
Secure Handler機能についてはこちらをご覧ください。

E-Post
Secure Handler



ご用命は…

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
サンプラワービル

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

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

問合せは sales@e-postinc.jp



メールサーバ専門ベンダーが送る
信頼性抜群のアプライアンス



CALライセンスやOS費用がかからず
初期導入コストを大幅削減



アプライアンスなので
設定・構築作業の導入期間を短縮

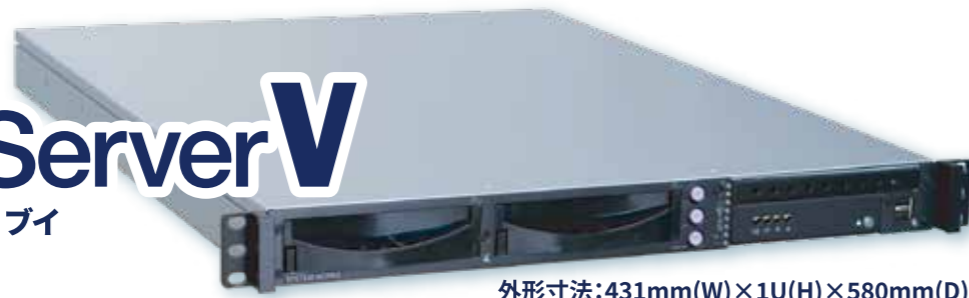


国内生産だからできる
膨大な日本語技術情報と安心のサポート体制

Windows版のメールサーバとして高い評価を得ている E-Post Mail Server のアプライアンス製品が復活!

E-Post Mail Server V

イーポスト メールサーバ



外形寸法:431mm(W)×1U(H)×580mm(D)

導入メリット

- 1 歴史あるWindows版「E-Post Mail Server」シリーズの安定稼働の実績を踏襲。
- 2 BSD版環境のため、コストのかかる別途OSやCALの費用を見積もり不要。
- 3 わずらわしい設定・構築作業がなく、わずかな設定作業ですぐ本稼働できます。
- 4 あらかじめユーザー数規模で最適な構成にしているため、キitting不要。
- 5 国内生産であるため、参考資料・FAQなど膨大な日本語情報が充実。
- 6 万が一のトラブルでも心配なし、万全の日本語サポート体制。

主な特長

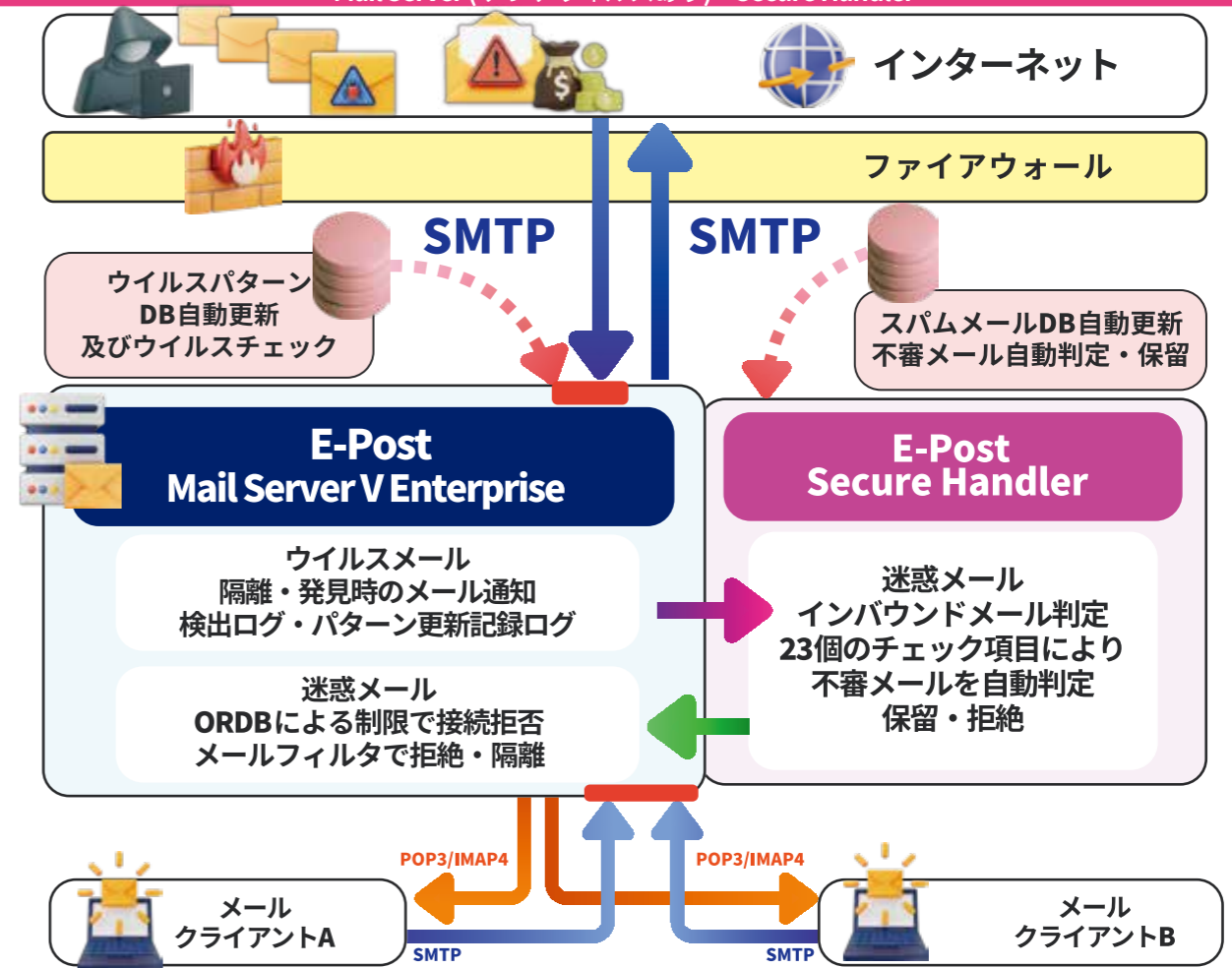
- 1 Webからの完全管理、SSHでのアクセスも可能。
- 2 メールサーバとして必要な条件を十分に満たすWindows版譲りの豊富な機能。
- 3 Standard版は、上長承認 (BossCheck) 機能を標準搭載。
- 4 総当たり攻撃やDDoS攻撃へのセキュリティ対策強化。
- 5 PPAP代替の添付ファイル分離配送・ファイル受信通知機能。
- 6 Enterprise版は、アンチウイルス機能を装備。
- 7 Enterprise版は、不審・標的型・スパムなどのメール排除に有効なSecure Handler搭載。
- 8 WebメールソフトRainLoopをバンドル済み。1台でメールサービス提供が可能。
- 9 Windows版バックアップ/復元ツールTB SafeBox付属。SSHで安全な世代管理が可能。

BSD版E-Post Mail Server Standard Enterprise Vシリーズ アプライアンス製品ラインアップ

製品分類・主要用途	Standard/ Enterprise	スパム・ウイルス・標的攻撃対策	HW/SW 区分	User ライセンス数	ハードウェアスペック	型番
Mail Server メールサーバ向き [SMTP/POP3/IMAP4]	Standard	<ul style="list-style-type: none"> 標準装備 (ORDB参照機能とメールフィルタによるSURBL参照機能)のみ 	VHW (アプライアンス)	250User	<ul style="list-style-type: none"> POWER MASTER Server Rシリーズ RAID1構成 HDD SATA 2TB×2 CPU Xeonシリーズ(4Core) メモリ16GB <small>※IMAP使用時1人当たりのメールBOX平均6GBを想定</small>	EP-BEPMVS-S-250-PMR
	Enterprise	<ul style="list-style-type: none"> Secure Handler付き (スパムDB判定・標的型攻撃対策・不審メール全般) アンチウイルス機能搭載 (ウイルスDB/パターンマッチング検査) 標準装備 (ORDB参照機能とメールフィルタによるSURBL参照機能) 				EP-BEPMVS-E-250-PMR

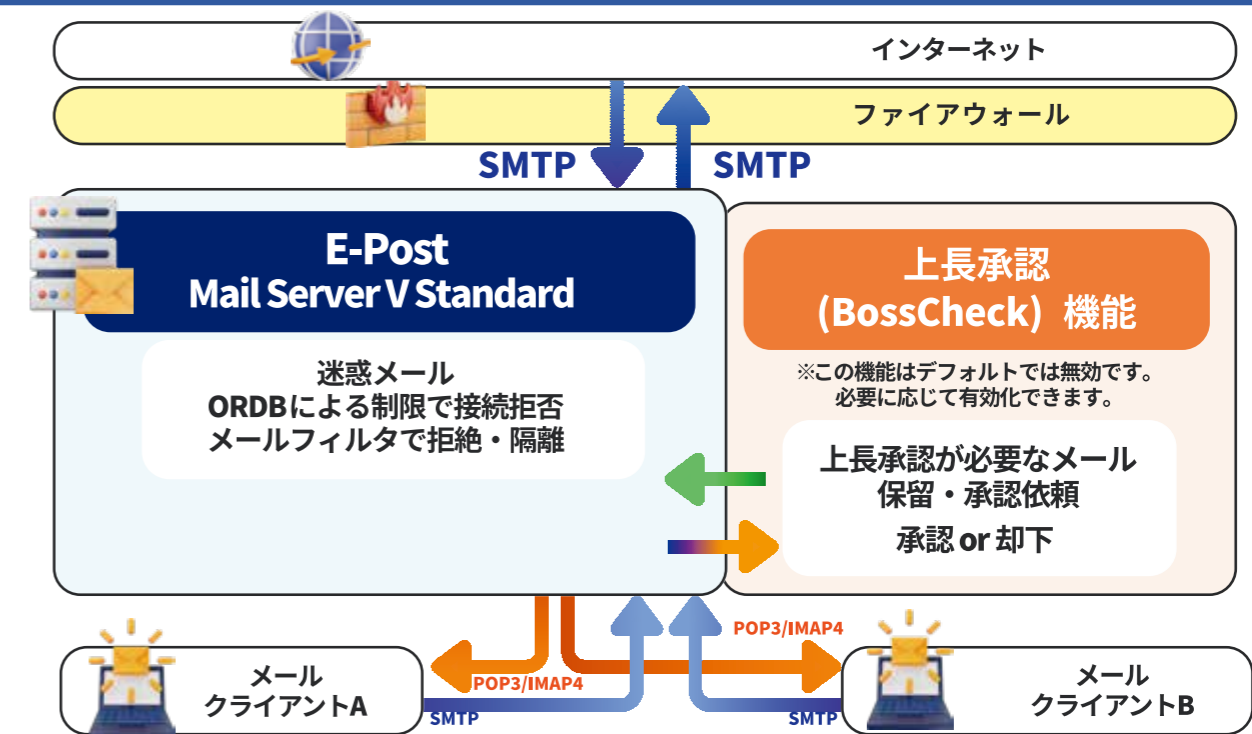
E-Post Mail Server V Enterprise 内部構成図

Mail Server (アンチウイルスあり) + Secure Handler



E-Post Mail Server V Standard 内部構成図

Mail Server + 上長承認(BossCheck) 機能



E-Post Mail Server V シリーズ 機能一覧表

製品名	E-Post Mail Server V Standard (+0)	E-Post Mail Server V Enterprise (+0)
配送性能 (運用環境により異なります)	～30万通/時間 (+1)	一般万通/時間 (+2)
管理ドメイン数		最大512ドメイン
対応プロトコル		SMTP/POP3/IMAP4 (+3)
暗号化通信 (SSL/TLS/STARTTLS)		SMTP over SSL, POP3 over SSL, IMAP4 over SSL (+4) STARTTLS (SMTP), STARTTLS (POP3), STARTTLS (IMAP4)
SMTP認証 (SMTP AUTH)		(+5) (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)
SMTPゲートウェイ機能: フォワード機能 ゲートウェイサーバ [gateway.dat]		(フォワード先設定 / 宛先ドメインごとの振り分け / 宛先メールアドレスごとの振り分け) (SMTP[基本: 先送]送付先で外部SMTPへの送信/拒絶も可)
中継の制限機能 [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 [ordb.dat] (DNSBL方式)		(全体共通設定)
SMTP配送の詳細設定		(全体共通設定 永続的拒絶時のトライ /一時拒絶時のトライ/サーバ無応答時のトライなど)
SMTP配送の利用時間設定 [usetime.dat]		(+6) (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		(+7) (メールサーバーEM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 (+8)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/URL [SURBL] サイト参照 /拒否/タグ付け通過/指定アクションへの転送など)
SURBL/URLBL方式による参照機能		(上記メールフィルタ機能に用意)
POP3認証方式		USER/PASS (平文) / APOP_AUTH (PLAIN/LOGIN/CRAM-MD5) (+9)
接続ロックアウト機能		(設定回数以上POP3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POP3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)
IMAP4認証方式		LOGIN (平文) / AUTHENTICATE (PLAIN/LOGIN/CRAM-MD5) (+10)
接続ロックアウト機能		(設定回数以上IMAP4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IMAP4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)
E-Post方式ユーザー管理		
ActiveDirectoryユーザー管理との連携 (LDAP)		(+11)
OSアカウントとの連携管理		(+12)
自動転送設定		(+13) (自動転送時の送信先指定など)
自動応答設定		(+13)
追加処理プログラム		(+14)
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)
SMTP受信制限設定 [effect.dat]		(+15) (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)
POP3認証設定		(有効/無効)
IMAP4認証設定		(有効/無効)
アカウント情報のインポート/エクスポート		(+16)

- (+0) BSD版 E-Post Vシリーズはすべて64ビット版です。E-Postとは別に、IMAP4対応Webメールシステムとして RainLoop Community Edition がバンドルされ、インストール及び基本設定済みです。
- (+1) 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を～3KB程度による試験結果です。なお、アンチウイルス機能を持つ Enterprise版での配信設定は、アンチウイルス機能を搭載しない Standard 版に比べて、約1/3～1/10程度低下します。メールフィルタの設定を多数登録しているときも、設定量だけ負荷がかり、配信能力は低下します。
- (+2) 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を～3KB程度による試験結果です。アンチウイルス機能はSMTP受信するメールに対してのみ働きます。マシン全体のウイルス検索 SpamAssassin (スパムアサシン) はできません。Anti-Virusエンジンのファストスキャンは、株式会社サイ・テックの製品のみが連携します。
- (+3) POP3プロトコル使用時は、1ユーザー10000ユーザークラスの大規模利用でも、サーバの能力さえあれば理論上の問題は少ない使用実績もあります。一方、IMAP4プロトコル使用時は最大でも1ユーザー500ユーザークラスまでとして、アラブライズ製品では250user版を使用しています。
- (+4) SSL通信を検証するだけでなく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)による証明書書の発行と取得が必要です。最新版では、SSLは廃止され、TLS1.0～TLS1.3に対応します。
- (+5) 認証ファイルによりユーザーごとのSMTP認証が無効設定が可能です。
- (+6) 利用するには全体共通設定の設定ファイル [usertime.dat] をコントロールから接続設定する作業が必要です。
- (+7) 同機能は付属オプションCGIツール getattach の導入・設定作業が必要です。ApacheのWebサーバ環境を利用します。
- (+8) CGIツールの getattach は新規ご購入時にはバナナインストール済みですが導入・設定作業は未設定です。
- (+9) APOP認証とSMTP認証で使われる認証ファイルは共用です。AUTHはSASL [Simple Authentication and Security Layer] と呼ばれる認証方式で、E-Postでは便宜上POP-AUTHと呼んでいます。利用するにはメールクライアント側の対応が必要です。
- (+10) IMAP4サービスの認証方式は PLAIN/LOGIN/CRAM-MD5 対応となります。
- (+11) Active Directory, 連携LDAPによる管理方式です。POP3認証設定時はIMAP4認証設定のユーザー名・パスワード部分が連携されます。SMTPはユーザー情報だけが連携されます。SMTP認証パスワードは連携しません。
- (+12) SMTPではユーザー情報のみが連携されます。SMTP認証パスワードは連携しません。
- (+13) 自動転送機能と自動応答機能とは排他して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。自らの自動応答機能でWeb管理画面から編集できる自動応答文については強制的にJIS (iso-2022-jp) に変換して登録されます。
- (+14) 追加処理プログラムで指定できるのは標準コンソールで動作するプログラムやスクリプトのみです。
- (+15) アカウント単位の設定ファイル [effect.dat] は [送信先制限 (sender.dat)] の入力項目を [送信先制限 (effect.dat)] とし、かつ effect.dat の編集が行えます。
- (+16) タブ区切り形式テキスト (TSV) に移行可能です。エクスポート時にレコーの行末はLFとなります。インポート時のレコードの行末はLFおよびCRLFが有効です。

製品名	E-Post Mail Server V Standard (+0)	E-Post Mail Server V Enterprise (+0)
エイリアス		(+17)
メーリングリスト機能		(連絡先、表題、Reply-To/CC/投稿パスワード、 添付ファイル削除、投稿内容保管など)
上長による承認/却下機能		(+18) (承認/却下による上長の承認/却下の実行)
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受信詳細 / SMTP送信 / SMTPローカル送信 / SMTP配送失敗 / SMTP配信詳細 / POP3受信 / IMAP4受信 / POP3受信詳細 / IMAP4受信詳細 (+19)
管理画面のセキュリティ		(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 (システム管理)		(+20) (システムダミー/パスワード/DKIM/DMARC/SPF/フォルダ/メール /システム停止・再起動・設定情報/バックアップ/リストア)
Web管理機能 (メールサーバー管理)		(+20) (3階層: システム管理者・ドメイン管理者・個別ユーザー)
Web管理機能 (Secure Handler承認管理)		(+20) (保留メール閲覧による許可 - 拒否判定操作 / 強制拒否 (ブラックリスト) / 強制許可 (ホワイトリスト))
コマンド操作機能 (コンソール機能)		(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)
mitler インターフェース機能		(+21)
アンチウイルス機能 (ファストスキャン Anti-Virusエンジン)		(+22) ウイルスメールの隔離 / ウイルス発着時のメール通知 / ウイルス検出ログ ウイルスバスター更新記録ログ)
E-Post Secure Handler機能による 総合的なセキュリティ対策 (詳細は別表を参照)		(+23) 怪しいメール検出 / 権限の強化メール拒否 / スパムメール検除
迷惑メール対策 (まとめ)		- ORDB参照 (DNSBL方式) 機能 - メールフィルタによるSURBL/URLBL方式 による多層検出 - ORDB参照 (DNSBL方式) 機能 - メールフィルタによるSURBL/URLBL方式 による多層検出
送信ドメイン認証対応		SMTP受信時での DMARC/DKIM/SPF対応機能 (オプションツール EPSTDKIM/EPSTDKIM/GETSPFを付属) (+24)
ログ解析・集計レポート機能		ログ解析・集計レポート機能 (ツール FreeBSDB版 E-Post Log analyzer を付属) (+25)
メールボックス使用状況レポート機能		ログ解析・集計レポート機能 (ツール FreeBSDB版 E-Post Log analyzer を付属) (+25)
ユーザーのメールボックス 使用警告メール機能		ログ解析・集計レポート機能 (ツール FreeBSDB版 E-Post Log analyzer を付属) (+25)
簡易メールアーカイブ		全メール一括検索機能 及び ジョーナル機能
TB SafeBox (メールデータバックアップ及びリストア)		メールデータのバックアップ及び復元ツール (オプションツール Windows版 E-Post TB SafeBox を付属) (+26)

- (+17) エイリアス設定と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、作成エイリアス必要ラテンズ数は数としてカウントされます。
- (+18) 上長側が承認・却下するメールソフトは、RFCで規定されている mailtoリンクが使用可能である必要があります。mailtoリンクが正常に働かずにWebメールソフトでは対応が困難な場合があります。Enterprise版には Secure Handler 機能変更のため、実質的に上長承認 (BossCheck) 機能はご利用できません。Secure Handler機能と上長承認 (BossCheck) 機能を同時に使用することはできません。
- (+19) 拒否ログの行末はLFで改行されます。Windowsマシンにダウンロードして開くときはLFを改行として認識できるエディタを開いてください。
- (+20) Web管理機能は、ApacheのWebサーバ環境を利用しています。E-Post Vシリーズではすべて設定済みです。
- (+21) E-Post Vシリーズに搭載されている mitler インターフェースは次のソフトウェア clamav-milter / spamass-milter / milter-greylist が動作確認されており、補足マニュアルに設定手順を掲載しています。
●clamav-milter (Clam AntiVirus (クランアンチウイルス、略称Clam AV)) / SMTPサーバと clamd のソケット通信を行うプログラム ●spamass-milter (SpamAssassin (スパムアサシン)) はバムフィルタリングのプログラム ●milter-greylist (milter-greylist) は、株式会社サイ・テックの製品のみが連携します。
- (+22) アンチウイルス機能はインターネット接続環境が前提です。アンチウイルス機能はSMTP受信するメールに対してのみ働きます。マシン全体のウイルス検索 SpamAssassin (スパムアサシン) はできません。Anti-Virusエンジンのファストスキャンは、株式会社サイ・テックの製品のみが連携します。
- (+23) Secure Handler 機能はインターネット接続環境が前提です。Secure Handler 機能は Enterprise 版に実装されています。わかりやすい機能は別表を参照してください。
- (+24) SMTP受信時でのDMARC対応ツールは2024年2月公開の送信ドメイン認証 (DMARC/DKIM/SPF) アドオン EPSTDKIM v1.08です。EPSTDKIMをインストールすることDMARC/DKIM/SPFのすべてをきむ対応が可能になります。その他従来からの付属ツールとして、DKIM対応の送信ドメイン認証 (DKIM) アドオン EPSTDKIM v1.08、DMARC/SPF対応の送信ドメイン認証 (SPF) アドオン GETSPF があります。OpenDKIMをインストールは、MLTE機能は有効にする必要がありません。EPSTDKIM/EPSTDKIM/GETSPFの各ツールは、新規ご購入時にはバナナインストール済みです。導入・設定作業はすべて未設定です。
- (+25) FreeBSDB版 E-Post Log analyzer はコンソールからコマンド操作でスクリーン動作するツールです。定期実行には cron tab コマンドを利用します。Log analyzerは新規ご購入時にはインストール済みです。
- (+26) Windows版 E-Post TB SafeBox は Windows OS からバックアップや復元ツールを使って安全な通信 (SSH) を行い、E-Post Vシリーズに接続、サーバのメールデータを監視し、Windows E-Post Vシリーズの両方に保存するバックアップ/リストアツールです。操作は基本的にはWindows上のGUIで完了します。

E-Post Secure Handler 機能一覧表 (+0)

機能	OS及びハードウェア仕様
メール保留条件 (ハンドリングルール)	エンベロープの暗号化 (ドメイン/アカウント) エンベロープの送信先 (ドメイン/アカウント) とメールアドレスの重複 (ドメイン/アカウント) 1層でのメール検出 (ドメイン/アカウント) ※1層も複数検出 (ワイルドカード指定) ※1層も複数検出 (ワイルドカード指定)
判定方法	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) APIによる許可/拒否自動判定 (+2, +3)
強制許可 (ホワイトリスト)	- 送信先エンベロープの登録・削除・閲覧 (システム/ブラウザ) - 宛名の登録・削除・閲覧 (システム/ブラウザ) - リンク情報 (本文/検出URL) の登録・削除・閲覧 (システム/ブラウザ) (+4) ※1層も複数検出 (ワイルドカード指定) ※1層も複数検出 (ワイルドカード指定)
強制許可可検知確認	APIによる許可/判定された送信先エンベロープ/宛名を接続し登録せず自らの管理で最終判定
強制許可 (ホワイトリスト)	- 送信先エンベロープの登録・削除・閲覧 (システム/ブラウザ) - 宛名の登録・削除・閲覧 (システム/ブラウザ) - リンク情報 (本文/検出URL) の登録・削除・閲覧 (システム/ブラウザ) ※1層も複数検出 (ワイルドカード指定) ※1層も複数検出 (ワイルドカード指定)
メンテナンス	- 判定時リスリの取捨選択 (承認者) - 履歴の取得・履歴の閲覧 (管理者のみ) 許可/拒否の結果確認ログ (システム)
拒否メール判定回復機能	判定ミス等で一旦拒否されたメールを許可メールとして回復 (ブラウザ)

(+0) E-Post Secure Handler 機能が実装されるのは、E-Post Mail Server Enterprise V シリーズのみです。