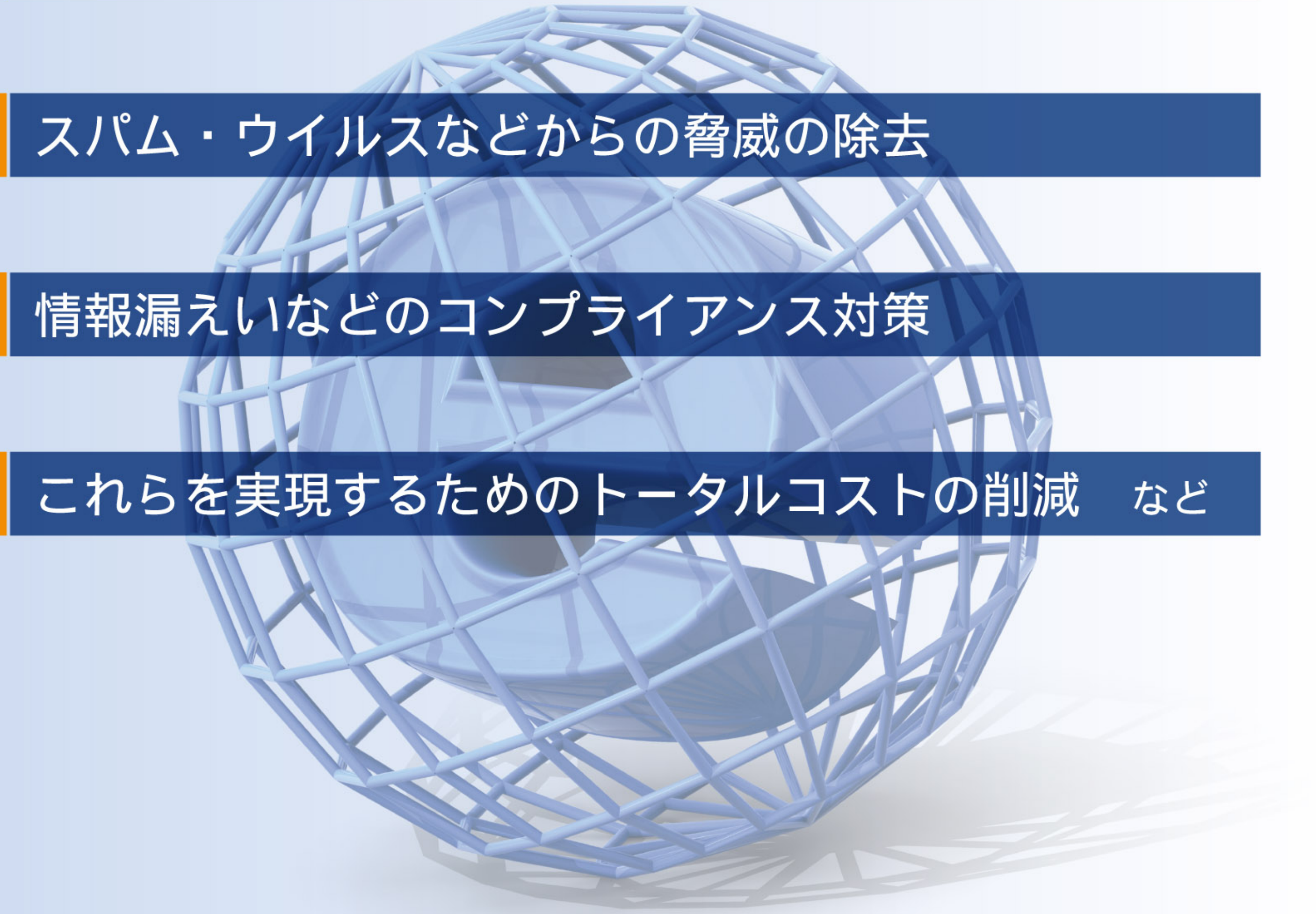
メールシステムに望まれることは何でしょうか？

現在のビジネス環境では、メールシステムはなくてはならないものになっています。しかしながら、メールシステムを取り巻く環境は、大きく変化してきています。



- システムダウンしない連続稼動
- スパム・ウイルスなどからの脅威の除去
- 情報漏えいなどのコンプライアンス対策
- これらを実現するためのトータルコストの削減　など

E-Post Mail Serverシリーズは、これらのニーズにお答えするメールサーバソフトウェアです。メールサーバソフトウェアのE-Post Mail Server (x64)、SMTPゲートウェイサーバソフトウェアのE-Post SMTP Server (x64)、上長承認メールシステムのE-Post BossCheck Server (x64)、標的型メール攻撃防御セキュアメールゲートウェイのE-Post Secure Handler (x64)の４つの製品群を用意しています。

E-Post Mail Server (x64)・E-Post SMTP Server (x64) 機能一覧表

製品名	E-Post Mail Server (x64)				E-Post SMTP Server (x64) (*0)			
	Standard		Enterprise II		Standard		Enterprise II	
	シングルサーバ	クラスタモデル(*0)	シングルサーバ	クラスタモデル(*0)	シングルサーバ	クラスタモデル(*0)	シングルサーバ	クラスタモデル(*0)
HAクラスタ機能（E-Post方式）(*1)	ー	○	ー	○	ー	○	ー	○
負荷分散機能（E-Post方式）(*2)	ー	○	ー	○	ー	○	ー	○
HAクラスタ対応（MSFC方式）(*3)	ー	○	ー	○	ー	○	ー	○
配送性能（運用環境により異なります）	〜30万通/時間 (*4)	ー (*5)	〜数万通/時間 (*6)	ー (*5)	〜30万通/時間 (*4)	ー (*5)	〜数万通/時間 (*6)	ー (*5)
管理ドメイン数	最大512ドメイン							
対応プロトコル	SMTP／POP3／IMAP4 (*7)				SMTP			
暗号化通信（SSL/TLS/STARTTLS）	SMTP over SSL、POP3 over SSL、IMAP4 over SSL (*8) STARTTLS (SMTP)、STARTTLS (POP3)、STARTTLS (IMAP4)				SMTP over SSL (*8) STARTTLS (SMTP)			
SMTP認証（SMTP AUTH）	○ (*9) （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）							
SMTP認証接続ロックアウト機能 new!	○ （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）							
SMTPゲートウェイテーブル【gateway.dat】・フォワード機能	○ （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 new!）							
中継の制限機能【effect.dat】（SMTP受信送信の制限）	○ （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方式サイト参照）	○							
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）							
POP3認証方式	○ USER/PASS（平文）, APOP, AUTH（PLAIN/LOGIN/CRAM-MD5）(*15) new!				ー			
POP3認証接続ロックアウト機能 new!	○ （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）				ー			
IMAP4認証方式	○ LOGIN（平文）, AUTHENTICATE（LOGIN/CRAM-MD5）				ー			
IMAP4認証接続ロックアウト機能 new!	○ （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）				ー			
ActiveDirectoryユーザー管理との連携	○ (*10)				△ (*11)			
E-Post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）							
アカウント別設定：自動応答設定	○ (*12,*13)							
アカウント別設定：「メール制御」機能での追加処理プログラム	○ (*14)							
アカウント別設定：メールボックス保管サイズ制限	○							
アカウント別設定：個別メールフィルタ設定【mail.dat】	○							
アカウント別設定：利用時間設定	○							
アカウント別設定：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）							
アカウント別設定：SMTP受信制限設定【effect.dat】new!	○ （指定アドレス・ドメインの受信許可／受信禁止）							
アカウント別設定：SMTP認証設定	○ （認証あり・認証なし）							
アカウント別設定：POP3無効化設定	○ （POP3有効／無効化の設定）				ー			
アカウント別設定：IMAP4無効化設定	○ （IMAP4有効／無効化の設定）				ー			
アカウント情報のインポート・エクスポート	○ (*16)							
エイリアス	○ (*17)							
エイリアス情報のインポート・エクスポート	○							
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	○							
メーリングリストメンバーのインポート・エクスポート	○							
対応IPバージョン	IPv4／IPv6 (*18)							
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／POP3受信／IMAP4受信／POP3受信詳細／IMAP4受信詳細／ーー		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／POP3受信／IMAP4受信／POP3受信詳細／IMAP4受信詳細／ウイルス検出／ウイルスパターン更新		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／ーー／ーー／ーー		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／ーー／ーー／ウイルス検出／ウイルスパターン更新	
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	○ (*19) （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）new!	○ (*20) （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）							
アンチウイルス機能	ー		○ (*21) ファストスキャン Anti-Virus エンジン		ー		○ (*21) ファストスキャン Anti-Virus エンジン	
対応IPバージョン	ー		○		ー		○	
ウイルス発見時のメール通知	ー		○		ー		○	
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）							
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 new!	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）(*22)							
ユーザーへのメールボックス使用量警告メール機能 new!	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）(*22)							

(*0) クラスタモデル版、シングルサーバ版のパッケージ内容は同一であり、クラスタモデル版ライセンスは、シングルサーバ版ライセンス×2と同等です。ですからシングルサーバ版2台分でもクラスタリング構成は可能です。
(*1) E-Post方式クラスタ機能は、IPレベルの監視を行います。サービスレベルの監視は行いません。HAクラスタ構成時の共有ディスクとして、Windows Serverの共有ドライブや、Windows系NASなど、UNC名でアクセスが可能なネットワーク共有ドライブが利用可能です。なお、E-Post方式クラスタ機能は、ファイルI/O性能が限られるネットワーク共有ドライブを利用するため、大規模な環境には向きません。500user以上の大規模環境では、シングルでのご利用か、MSFCクラスタ環境でのご利用を推奨いたします。
(*2) 負荷分散構成は可能ですが、ネットワーク共有ドライブによる共有ディスク方式を利用した場合、Ethernetの転送速度がボトルネックとなるため、負荷分散としての効果は十分に発揮できません。
(*3) MSFC方式フェールオーバークラスタに対応するには、MSFCが利用できる Windows Server 2008 Enterprise 以上か Windows Server 2012 / 2012 R2 / 2016 が必要です。ソフトウェアによる共有ストレージを利用する場合、Windows Storage Server 2008では Microsoft iSCSI Software Target の追加インストールが必要ですが Windows Storage Server 2012 / 2012 R2 / 2016 には標準でiSCSIターゲットサーバが付属します。また、ファイバーチャネルやiSCSIなど専用の共有ストレージを利用する場合は、関連ベンダーにお問い合わせください。
(*4) 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。なお、アンチウイルス機能を持つ Enterprise II 版での配送能力は、アンチウイルス機能を搭載しない Standard 版のそれに比べて、約1/3〜1/10程度に下がります。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かり、配送能力はその分低下します。
(*5) 共有ディスクのアクセス速度・転送速度が遅い場合、それらがパフォーマンス低下の要因となります。E-Post方式クラスタ機能は、ファイルI/O性能が限られるネットワーク共有ドライブを利用するため、user数の多い大規模な環境には向きません。大規模環境では高速なストレージを使用できるMSFC方式クラスタでの導入を推奨します。特にIMAP4プロトコルを利用して大量のメールデータにアクセスするときには影響が大きいことがわかっています。クラスタ構成時にユーザーアカウントをAD連携させた場合、加えてパフォーマンスは下がります。パフォーマンスを低下させないためには、E-Post独自アカウント方式で設定することを推奨します。
(*6) 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。
(*7) POP3プロトコル使用時は、1サーバ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的に問題は少なく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サーバ500〜1000ユーザークラスを目途にすることを推奨します。
(*8) SSL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）による証明書の発行と取得が必要です。
(*9) 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。
(*10) POP3認証時またはIMAP4認証時のユーザー名・パスワード部分が連携されます。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。
(*11) 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。
(*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。
(*13) 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変換する必要はなくそのまま登録できます。
(*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。
(*15) 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。これは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実装機能であり、利用するにはメールクライアント側の対応が必要です。
(*16) タブ区切り形式テキスト（TSV）により可能です。
(*17) 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。
(*18) E-Postクラスタ構成時に利用されるIP監視ツールであるIPWCS（IPWatcher）サービスは、IPv4環境でのみ使用可能です。IPWatcher は、IPv6には対応していません。
(*19) 利用するには、IISなどのWebサーバ動作環境が必要です。
(*20) 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。
(*21) アンチウイルスエンジンのファストスキャンは、株式会社ケイ・テックの製品ならびに商標です。株式会社ケイ・テックは2012年12月、米国のITセキュリティ調査企業OPSWAT認定パートナーとして認定・登録されています。
(*22) 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。
※ new! マークは2016年〜2018年に強化された新機能です。新規ご購入時には実装済みです。

動作推奨環境

対応OS	Windows Server 2008 / 2008 R2 / 2012 / 2012 R2 / 2016 (*23)
CPU	推奨：Xeonコア相当のCPU 2GHz以上
HDD	Enterprise II 版はプログラム領域として90MB以上、Standard版はプログラム領域として13MB以上、加えてユーザーメールボックスおよびメール作業領域として必要十分な空き容量
メモリ	推奨：2GB以上

(*23) (x64)版E-Post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。

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：03-5286-2610
https://www.e-postinc.jp
問合せは sales@e-postinc.jp

e-POST

Windowsメールサーバソフトウェアシリーズ

E-Post MailServer

メールサーバ／SMTPゲートウェイサーバ／上長承認メールシステム
標的型メール攻撃防御セキュアメールゲートウェイ

安定した稼動実績
独自のクラスタ構成により連続稼動を実現します。

安全を重視したセキュリティ対策
スパムフィルタ、ウイルスチェック、標的型メール攻撃対策機能を搭載し、メールの安全を図ります。

安心の充実サポート
純国産ソフトですので、日本語でのサポートやWEBによる豊富なドキュメントを活用できます。また国内のメール環境に即座に対応します。

GUIによる簡単操作
ウイザードによる簡単インストール＆設定。サーバソフトとは思えない簡単設計です。

しかも安価な価格設定
年間トータルコストの削減に大きく寄与します。