セキュアな機能分散型メールシステムの構築と移行

○押久保智子
高エネルギー加速器研究機構　共通基盤研究施設　計算科学センター

概要

高エネルギー加速器研究機構メール環境の中核をなす電子メールシステム(KEKmail と称す)は、共通情報システムレンタルの一部として導入し、運用している。2008 年度末の共通情報システムのリプレースに伴い、KEKmail も更新した。

研究活動や日常業務に不可欠な情報基盤となっているメール環境は、24 時間 365 日無停止で、日々増大しているウイルスやスパム、攻撃などに対してセキュリティの高い運用を要求されている。そのような状況のもと、セキュアなシステムを構築し、メーリングリスト宛メールを除くメールの配信を停止することなくシステム移行を行なっている。本研究会では、KEKmail の機能紹介と移行方法について述べる。

1　システムを構築するにあたっての要件

システムを更新するにあたっては、現運用システムの功罪を洗い出し、全体的なシステム構成は現行システムの設計思想を引き継ぐこととなったが、一部には機能追加や改良、検討の余地があり、それらを満たす方向で新システムの構築を行った。現行システムからの引継ぎ要件としては、

(a) KEKmail は、独立したサブドメインに、運用の異なる研究系システム(PostKEK と称す)と管理局系システム(MailKEK と称す)の管理運用を行う。
(b) KEKmail の運用は機構の基幹サービスとなっているため、無停止運用ができる信頼性の高いシステムとする。
(c) メール環境の社会的状況の変化にも対応できるよう、拡張性がある構成にする。
(d) 外部からの攻撃からシステムを護るため、KEKmail 独自のファイアウォールを有する。
(e) Anti-virus は、受信メールと送信メールにおいて、各々に応じた処置が設定できる。
(f) Anti-Spam のフィルタリングは、受信メールに対してのみにて行い、信頼性のあるフィルタを行う。
(g) 機構外から KEKmail 上でメールの送受信ができる手段を、引き続き維持する。

などである。

機能追加、改良、検討要件としては、スプール領域の増量、管理用アドレスへの電子証明書の導入、メーリングリストの設定変更申請の Web 化、および、より利便性の良い Webmail ソフトの模索であった。

システム実装のパラメータとしては、登録ユーザ数は 2,000 人とするが、状況変化により 3,000 人まで対応可能な性能を有し、管理アドレスは 10,000 とした。メール処理能力としては、最大メールサイズ 20MB/mail のものをピーク時には時間当たり 3 万通の処理を遅延無く配送できること。IMAP は時間当たり 20,000 セッション要求と 300 ユーザの同時アクセスとを遅延無く処理できること等々としている。

2　システム構築

共通情報システムの入札に際し、メールシステムの仕様は製品仕様ではなく、機能要求仕様として入札を

行っている。入札の結果 IBM が落札したため、IBM 製品の System p5 550 や System x3650 でシステムを構築した。

設計に際しては、Reliability（信頼性）、Availability（可用性）、Serviceability（保守性、サービス性）に Integrity（保全性）と Security（安全性）を加えた RASIS を念頭において、設計している。

2.1　機能分散型システム構成

ハードウェア構成としては、機構 LAN とのネットワーク接続を含めて全体を二重の冗長構成とした。また、システムのサービスを機能別に分散し、各機能グループ内に同等構成のサーバを複数台配置するという機能分散型構成とし、高可用性で負荷分散を兼ね備えたものとしている。機能別サーバとしては、メール受信サーバ、スパム/ウィルスチェックサーバ、メール配信サーバ、ファイルサーバ、Webmail サーバ、認証サーバ、メーリングリストサーバ、情報発信用 Web サーバ、ユーザ個人の情報を提供する Web サーバ、LDAP サーバ、管理用サーバ、ログサーバ、ファイアウォールスイッチ、バックアップ装置などを配置している。但し、メール受信サーバに関しては、前々回メールシステム運用の教訓から、IMAP 同時接続による排他制御問題に対処するため、マルチプロセッササーバによる運用系と待機系とする冗長構成とし、障害発生時には、IBM の AIX 上で稼動するクラスタリングソフト HACMP(High Availability Cluster Multi processing)にて待機系に切り替える構成とした。今後、Webmail の利用が増加することが予測されるため、Webmail サーバには負荷分散装置を導入している。KEKmail のシステム構成概念図を図 1 に示す。

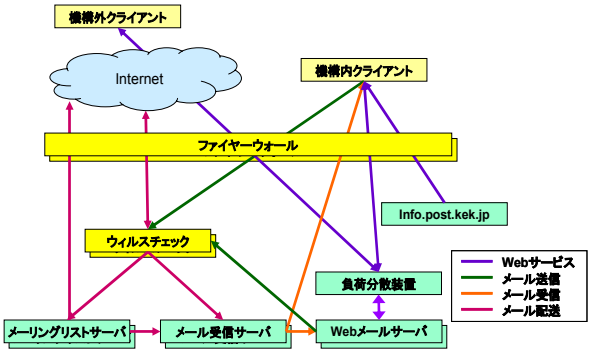

図 1　システム構成概念図

ソフトウェアとして、OS はメール受信サーバとメーリングリストサーバは IBM AIX、スパム/ウイルスサーバはセキュリティアプライアンス製品の IronPort AsyncOS、その他のサーバは Red Hat EL としている。MTA としては Postfix を、メーリングリストソフトは fml を利用している。今更新にあたり 1 章でも述べたが、Webmail ソフトが検討課題となっていた。導入にあたり、数社の製品とプロバイダー数社の Webmail を試用してみたが、どの製品にも一長一短があり、コストとメーカー対応面からトランスウェア社製の Acrive!Mail6 を採用し、メーカーに対しては、導入までに改良あるいは機能追加要望を行っている。

システム設置環境としては、機構計画停電時も運用できるよう、計画停電時に電力供給ができる環境である、ネットワーク系電源配下に機器を設置している。

2.2　ユーザ利用環境と管理者環境

ユーザ利用環境としては、前システムからの利用環境を引き継ぎ、IMAP をベースとした Web ブラウザでの利用環境を提供している。サーバと情報のやり取りを行う GUI である「ユーザ情報ページ」を設け、リソースの利用状況、パスワードの変更、メール転送設定、個人用スパムリストの設定、スパム判定メールの受信の可否、ログを確認したいという強い要望から、スパムログやウイルスログと連携した配送ログ可視化情報、メーリングリストの新規申請と設定変更申請および申請情報の閲覧機能、アドレス帳、利用更新手続き時の情報入力などを提供している。

管理者環境としては、各種サーバが複数台ずつ分散して稼動しているため、それぞれのマシンの稼動状態やサービスプロトコルの稼動監視、各種ログなどを集中管理しないとシステム管理は大変煩雑で負担の大きなものとなるため、各サーバのログを 1 台のホストに集約し、管理するツールを構築して管理している。管理ツールとしては主に、次のものを実装した。ユーザ登録情報、資源監視としてクォータ情報、メール配信ログ確認情報、サーバの状況表示、ウイルスログ一覧、スパムログ一覧、ファイアウォールログ一覧、および各サーバのアクセス数や処理数、負荷値などである。各種データを表やグラフの可視化情報として web ベースの GUI 環境で操作することで、管理者の日常業務は大変簡便なものとなった。また、メーリングリストに関しても、申請データをーデータベース化し、Web による管理ツールも実装している。

2.3　セキュリティ対策

分散したメールシステムの各サーバを外部からの攻撃より防御するため、独自のファイアウォールとして NetScreen を導入している。これにより、メールシステムに特化したセキュリティポリシーの運用が可能となると同時に、分散された複数のサーバに脆弱性が発見された場合でも、対策を安心してとることができるようになっている。

ウイルス対策としては、数社の対策ソフトを利用した経験から、サーバのソフトとしてはウイルス定義パターンファイルの提供が迅速であることを選択の第一とした。その結果、Sophos 社の Anti-Virus ソフトを導入した。Sophos のパターンファイルは 5 分間隔で提供されており、KEKmail も 5 分毎にパターンの更新を実施している。パターンファイルのアップデートは、多い日には 10 回近い更新がある。

研究や業務の効率を妨害する厄介なスパムの対策としては、複数のスパム対策機能を実装して強化している。KEKmail 外からの受信メールに対しては、第一段階として、セキュリティアプライアンス製品である IronPort C350 を導入し、複数の方法によりスパム対策を行っている。IronPort は、SenderBase と称する送信元 IP 評価データベース(DB)に基づくフィルタリング機能を有している。DB は各種ブラックリストへの登録の有無や企業情報などの 110 を超えるパラメータを常時監視し、統計対象メール 50 億通以上/日に則り作られており、閾値-4 での誤検知は 1/100 万通といわれている。KEKmail でも前システム導入当初に閾値-4 で運用を開始している。閾値を上げれば検知率も上がるが、誤検知が多いと導入した意味もなくなる。半年近くの運用を踏まえて閾値を見直し、現在まで-3.7 で運用を行っている。この DB は、CERT などの大量メール送信元は、リターンメールも多くなるため閾値が悪くなるりブロックされる傾向があるため、このようなサイトはホワイトリストへのリストアップも必要となる。これにより、凡そ 60%以上のスパムメールが KEKmail に取り込まれる前にフィルタされている。また、この製品には Anti-Spam もバンドルされており、ホワイトリスト、スパムリスト、コンテンツチェック、コンテンツの追加や From 等ヘッダーのチェック設定もでき、これらの機能もフルに活用している。第二段階としては、ユーザ固有のドメイン指定によるスパムリストを 10 件までではあるが、設定できる機能を作り込んでいる。

KEKmail 内からの送信メールについては登録ユーザのモラルを信じ、エンベロープ From のチェックのみで、本文のチェックは実施していない。

また、IronPort には LDAP と連携したチェック機能も携えている。 これを利用して、MX サーバへの SMTP 接続要求時に受信アドレスのチェックを行い、KEKmail に存在しないアドレス宛てメールは接続を拒否している。分散型システムにとってこの機能は、From 詐称の投げ込みメール対策としては、不可欠なものとなる。なぜならば、unknown user のエラーメールを当該ドメイン名で多量に詐称された From へ返信すると、From ドメイン先から当該ドメインがスパムサイトと判断されてしまうからである。

サーバ証明書の導入は当然のことながら、新システムから一部の管理用メールアドレスへ電子証明書を導

入し、管理者アドレスを詐称するメールに対処している。

3　システム移行

メールシステムの移行に関しては以下の 2 点を満たすよう、移行方法の検討を行った。

(a) メール受信サーバ名など、メールクライアントソフトで設定に利用しているホスト名を新システムに引き継ぐ。

(b) 出来得る限り運用を停止しない。やむを得ずサービスを停止する必要がある場合は、研究や業務に支障をきたさない時間帯に、最小限の停止に留める。

その結果、個人宛メールの配信を停止させないために、新旧システムを約ひと月間並行運用し、ユーザスプールについてはその間にユーザ自身でデータ移行をして頂く、という方法をとった。KEKmail の利用法として多々ある、当システムでウイルスやスパムのセキュリティチェックをした後各グループのメールサーバに転送するという利用法にとっては、無停止でのシステム移行となる。

システム設定となるユーザ情報やユーザ自身が操作できないメーリングリストのスプールに関しては、システム管理者の作業となるため、一部サービスを停止して実施せざるを得ない。システム切り替えの一週間前に 2.2 節で記した「ユーザ情報ページ」のサービスを凍結し、旧システムのパスワードや転送先設定などのユーザ設定情報を新システムへ移行を開始した。メール配送の切り替えとなる DNS のＭＸ設定変更は、メール流量の少なくなる金曜日の夜に実施している。メーリングリストサーバの移行作業は、メール配送が新システムに完全に移行されたのを確認した後、約 1 日間サービスを停止してスプールなどの移行を行った。

Webmail に関しても、システム切り替え直前までサービスを行っていたため、システム切り替え時から 2 時間半程サービスを停止して、Webmail のユーザ設定情報の移行を実施した。

新旧のメール受信サーバ名や SMTP サーバ名等は、MX サーバ切り替え時に、旧システムで使用していた代表ホスト名を新システムに引継ぎ、旧システムへの接続は、旧メール受信サーバ本来のホスト名を利用することとした。これにより、システムを移行してもメールクライアント側の設定変更は生じない。

ユーザ自身によるスプールの移行については、文房具的に利用され、利用者層が幅広いメールシステムに於いては問題もあるのではとの多くの意見があった。それについても、代表的なメールクライアントでの移行の操作方法を初心者でも分かるような手順書を用意する、実際にスプールを移行するための講習の場を数回設ける、それでも実現できない場合は申し出てもらい管理者側と協議して対処する、ということで了承を得られている。

4　まとめ

2008 年 9 月から 2009 年 1 月上旬にかけて構築したメールシステムの概要と移行について述べた。一年余り運用を行っているが、ソフトウェアやハードウェアのメンテナンス、バージョンアップ、障害による機器の入れ替え等を実施しているが、運用への影響は全く生じていない。また、セキュリティに対するインシデントも発生していない。無停止で運用できるセキュアなシステムを構築できたと自負している。

しかし、KEKmail は単なるメール配信システムというより、当機構の特殊性からツールの多い多岐にわたるシステムとなっている。このため、落札から運用開始までの限られた時間内でのツールの開発が問題となる。次の更新時の課題としては、より身軽なシステムとしてユーザのニーズに答えられるか、或いは、ユーザのニーズを変革することができるかにかかっていると考える。