大規模メールシステムの設計

3.1 はじめに

2006年10月に提供を開始した「IIJセキュアMXサービス(以下SMX)」のシステムを、2017年4月に全面リニューアルしました。SMXは「メールゲートウェイ」と分類される機能を中心としたサービスです。お客様のメールシステムがメールを受け取る前に、一旦IIJのメールサーバでメールを受け取り、ウイルスフィルタ・迷惑メールフィルタ・送信ドメイン認証フィルタ・バックスキャッターフィルタ・サンドボックスフィルタなど、様々な技術で脅威メールを防ぎ、安全なメールのみをお客様のメールシステムにお届けします。

サービス提供開始から10年以上が経過し、その間にメールの通数やサイズなどの流量にはじまり、サーバのスペックからメールシステムの要件に至るまで、メールサービスを取り巻く環境は大きく変わりました。SMXのシステムもそのような変化に合わせて拡張に拡張を重ねてきたため、サービス開始当初とは大きく異なるシステム構成となっていました。しかし、アーキテクチャの根本はサービス開始当初から引き継いでいるものも多く、長い間システムに限界を感じていました。

そこで今回のリニューアルでは、システムをアーキテクチャから全面的に見直しました。本稿では、SMXの新しいメールシステムの特に配送系の設計について、見直しの経緯と共に紹介します。

3.2 リニューアルに向けた課題と目標

リニューアルにあたり、まず、古い配送系の課題を踏まえていくつかの目標を定めました。

3.2.1 アーキテクチャの見直し

1点目は、無理に拡張を重ねた古いアーキテクチャの見直しです。古典的な大規模メールシステムでは、図-1のように単機能のメールサーバ(Message Transfer Agent、以下MTA)を直列に並べて配送系を構成するアーキテクチャが一般的であり、リニューアル前のSMXの配送系もこれに類するアーキテクチャを採用していました。

このような、多段MTA構成のアーキテクチャの最大のメリットは拡張性の高さです。既存の配送系に対して、追加したい機能を持つMTAを連結することで、手軽に配送系を拡張できます。また、MTA間はメール配送の標準プロトコルであるSMTPで接続するため、異なるベンダーの製品を組み合わせる際もインタフェースの互換性を心配する必要がなく、製品の組み合わせが原因となるトラブルは起きにくい傾向にあります。

ただし、この拡張方法には副作用もあるため、過剰な適用は禁物です。最も懸念すべき副作用は、MTAの段数の増加に伴うストレージI/Oの増加と運用コストの増加です。多段MTA構成の配送系では、メールがMTAを通過するたびに受け取ったデー

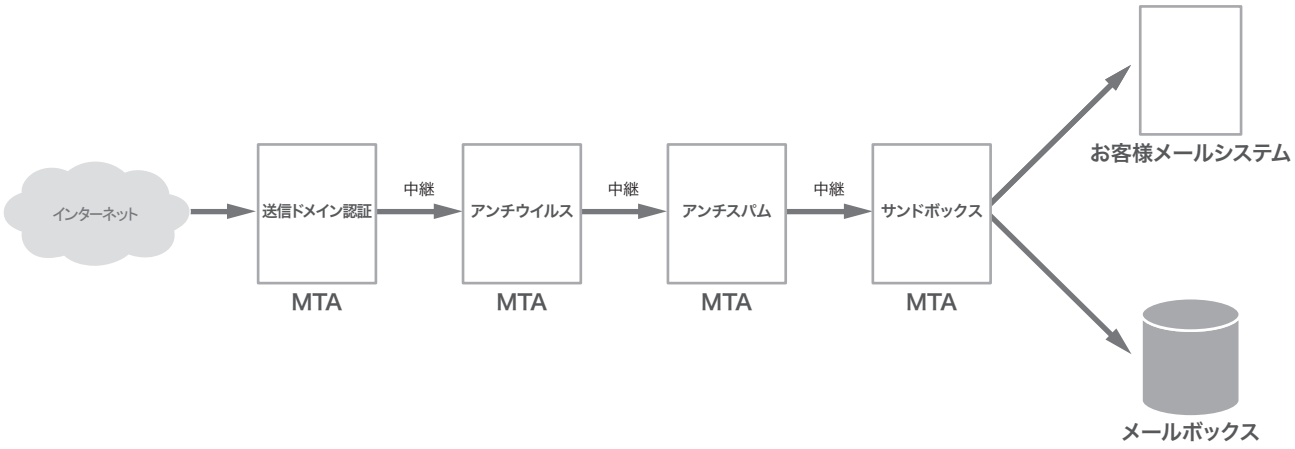


図-1 古典的なメールシステムのアーキテクチャ

タをストレージに書き出すため、メールサイズの何倍ものストレージI/Oが発生します。ほぼ同じ内容のメールが何度も書き出されるため、配送系全体として見ると無駄なストレージI/Oの多いアーキテクチャでもあります。NASやSANなどのネットワークストレージを用いる構成の場合、これらのI/Oだけでストレージネットワークを逼迫させてしまい、配送系全体のボトルネックになっていきます。従来のSMXの配送系でもストレージがボトルネックであった上に、CPUやメモリは遊んでしまい、高速化・大容量化が進むハードウェアの恩恵を十分に生かしきれていない状況でした。

更に、異なるMTAを直列に並べることは、運用方法の異なる様々なMTAが配送系に混在することを意味します。ログの見方・操作方法・障害対応手順・配送系増強の際の構築手順など、必要な知識が増えるだけでなく、それぞれのMTAが配送経路の分岐や通知メールの送信などを行うため、配送系内におけるメールの流れも複雑になり、配送系全体を把握することが困難になっていきます。

SMXでは、規模の拡大と共に配送系の拡張を繰り返したため、複雑で高コストな配送系になっており、これ以上の拡張は難しい状態でした。

3.2.2 フィルタ機能の向上

2点目の目標は、ウイルスフィルタ(アンチウイルス)及び迷惑メールフィルタ(アンチスパム)機能の精度向上です。メールセキュリティサービスにとって、アンチウイルス及びアンチスパムは双璧とも言うべき重要な機能です。

アンチウイルス、アンチスパム共に、数多くのセキュリティベンダーがサービスや製品を提供しているのですが、セキュリティ業界は変化が激しく、次々に新しい攻撃手法が生まれては、それに対抗する新しい技術の開発が日々行われています。そのため、ベンダーAの製品の検知精度が高い日もあれば、ベンダーBのサービスの検知精度が高い日もあり、ベンダーCが素晴らしい検知精度の新製品をリリースし、状況が一変することもあります。反対に、特定のベンダーのエンジンを一途に使い続けていると、そのエンジンが採用している技術が陳腐化し、検知精度が下がってしまうリスクがあるということでもあります。このような状況の中で、ウイルスメールや迷惑メールに対し、高い検知精度を維持するための仕組みの必要性を感じていました。

3.2.3 過度なベンダー依存の回避

3点目の目標は、特定ベンダーへの過度な依存の回避です。SMXは幅広い機能を提供するために、ベンダーの製品やサービスをシステムに数多く組み込んでいます。ベンダーの提供する製品やサービスは魅力的なものも多いですが、いわゆる「ベンダーロックイン」と呼ばれる状態にならないよう、依存度をコントロールする必要を感じていました。

特に海外のベンダーに多いのですが、ある日突然、競合他社に会社を丸ごと買収されて、提供中の製品やサービスが終了することも決して珍しくありません。組み込んでいる製品が急に使えなくなると、組み込んでいる側のインパクトは決して小さくはありません。インパクトをゼロにはできなくとも、最小限に抑えるための対策が必要でした。

3.3 単段MTA構成によるハードウエアリソースの有効利用

以上のような目標に沿って配送系をリニューアルするにあたり、まず、コモディティサーバの高性能化によって余裕のできていたCPUやメモリを活用して、システム全体のボトルネックであり、コスト要因にもなっているストレージI/Oの削減を目指すこととしました。

辿り着いたアーキテクチャは、従来とは正反対のものになりました。つまり、MTAは一段のみで無駄な中継はせず、単一の

高機能なMTAの中ですべての処理を完結させます(図-2)。このアーキテクチャでは、メールをストレージに書き出す処理は1回のみになるため、同じ内容を何度も繰り返し書き出していた従来の配送系に比べ、ストレージI/Oを大幅に削減することが可能です。

また、従来の配送系では、ストレージI/Oがボトルネックになり大半のサーバのCPUリソースが遊んでいる一方、一部のサーバでのみ、CPUに負担のかかるウイルススキャンなどによってCPUの稼働率が高くなっていました。均一な構成のMTAを並列に配置することで、これまで遊んでいたCPUリソースを負担のかかる処理に回せるようになり、配送系全体におけるCPUリソースの利用効率の向上も見込めます(図-3)。

SMXではアンチウイルス、アンチスパム共に複数のエンジンを採用しているため、単段MTA構成のアーキテクチャを実現するためには、1つのサーバ内でいくつものエンジンをメモリにロードする必要があります。一般に、アンチウイルスエンジンやアンチスパムエンジンは大量のデータをメモリに保持するため、大量のメモリを消費する傾向にあります。そのエンジンをいくつもロードするため、合計するとひと昔前のサーバでは収容できない量のメモリが必要になるのですが、前述のコモディティサーバの高性能化により、このような構成を取ることが可能になりました。

3.4 アンチウイルス／アンチスパムエンジンを交換可能に

次に、アンチウイルスエンジン及びアンチスパムエンジンは「いつでも入れ替えられる」ようにシステム全体を設計しました。

IIJでは、アンチウイルスエンジンやアンチスパムエンジンを自社開発しておらず、セキュリティベンダーの提供するエンジンを配送系に組み込んでこれらの機能を提供しています。そのため、検知精度に問題があっても自社で直接対応することはできません。しかし、逆の視点で捉え、陳腐化した技術を切り離し、旬な技術をタイムリーに組み込めることを強みとして活かせるよう、特定のアンチウイルスエンジンやアンチスパムエンジンに密に結合しない設計を目指しました。

まず、セキュリティベンダー各社のアンチウイルス及びアンチスパムエンジンの評価を行いました。IIJの管理するハニーポットで受信したウイルスメールや迷惑メールに対して、ウイルススキャン及び迷惑メールスキャンを行い、数ヵ月間かけて検知性能の統計を取り、比較を行いました。ウイルスメールや迷惑メールには流行のようなものがあり、短期間の検証では、評価期間中にたまたま行われていたスパムキャンペーン*1に対する検知性能の影響が大きく影響し、長期的な視点で見た場合の検知性能を適切に評価できない恐れがあります。そのため、検証期間は長めに設定しました。検証に際して、様々なセキュリ

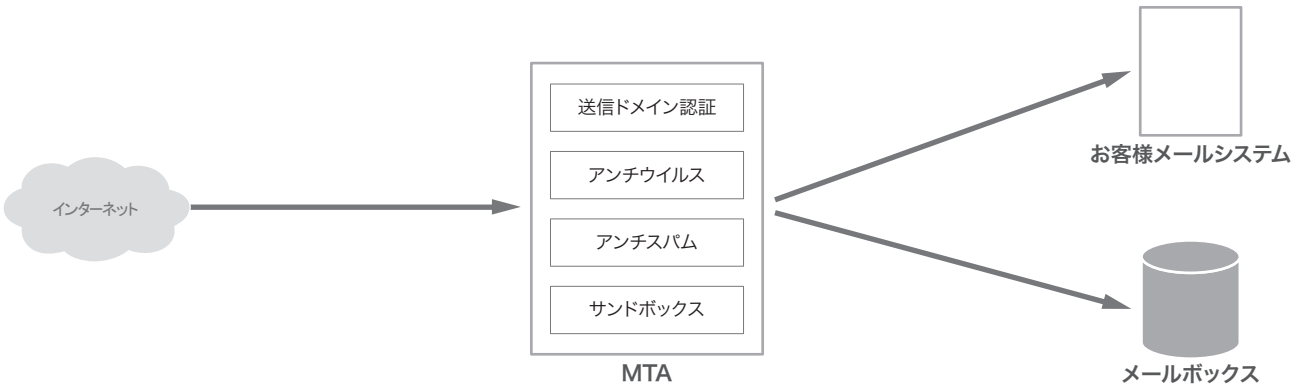


図-2 リニューアル後のメールシステムのアーキテクチャ

＊1　同一あるいは似通った迷惑メールの大量送信行為。

ティベンダーから製品説明を受けたのですが、特にアンチスパムエンジンについては製品によってアプローチに特色があり、検証結果もそのアプローチの差を反映した大変興味深いものでした。手間のかかる検証でしたが、おかげで各エンジンの検知精度や傾向を把握することができました。

また、更なる検知精度向上のため、アンチウイルスエンジン及びアンチスパムエンジンはそれぞれ複数組み込み、それぞれの処理結果を取りまとめたものを最終結果として扱うこととしました。

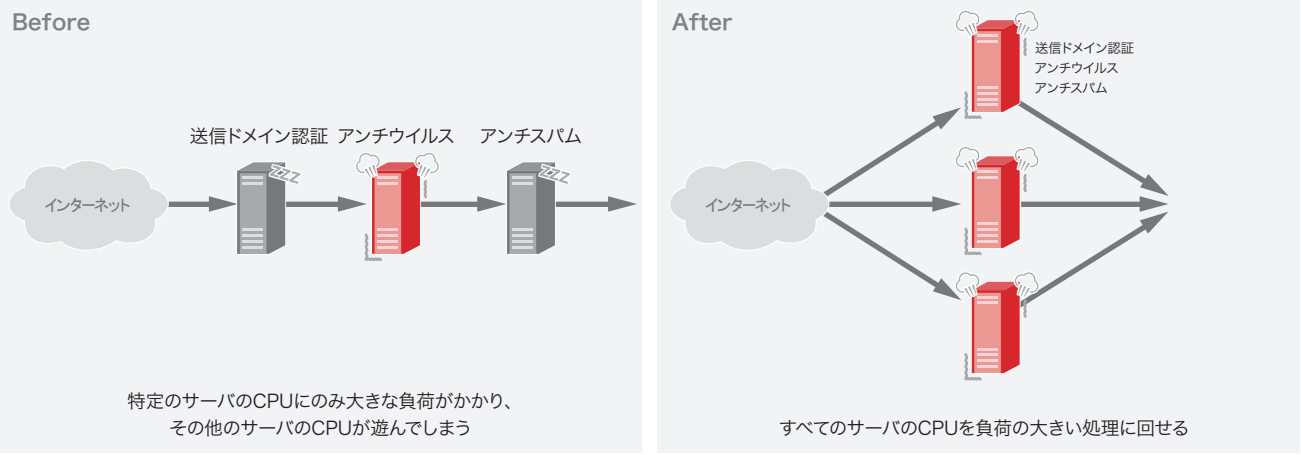
検証の結果から、そして普段運用する中の肌感覚からも言えると思うのですが、ウイルスメールや迷惑メールが撒かれ始めてからエンジンが検知するようになるまでの時間は、いずれかのエンジンが飛び抜けて優秀というものではありません。あるキャンペーンではエンジンAの検知が早く、別のキャンペーンではエンジンBの検知が早い、といった具合です。複数のエンジンを並べることにより、キャンペーンの初期段階のすり抜けを減らすことができるようになります。特にアンチスパムエンジンについては、あるエンジンの弱点を他のエンジンで補えるように、異なるアプローチのエンジンを組み合わせています。

複数のエンジンを組み合わせたのは、主に検知精度の向上を狙ったものでしたが、副次的な効果もありました。1つはスキャンエラーの削減です。ウイルスメールや迷惑メールでは、メールのヘッダや添付ファイルが破損していたり、意図的な細工が施されているために、スキャンを正常に完了できないケースも珍しくありません。複数のエンジンでスキャンすることにより、全くスキャンできないメールの数を大幅に抑えられるようになりました。また、ごくまれに特定のメールや添付ファイルをスキャンすると、アンチウイルスエンジンやアンチスパムエンジンがクラッシュしてしまうケースもあるのですが、そういった場合の緊急対応として、メールの疎通を優先し、問題の起きているエンジンを切り離すという選択肢を持つことができます。更に、セキュリティベンダーが会社ごと買収されて製品が使えなくなるような場合にも、インパクトを最小限に抑えることができます。

3.5 MTAの自社開発を決断

配送系のリニューアルにあたっての最大の問題は、この設計をどう実装するかでした。結果的に、MTAを自社開発することにしたのですが、他にも、Postfixやsendmailに代表されるオープンソースのMTAを組み合わせる方法や、MTAベンダー製のMTAを採用する方法がありました。

Postfixやsendmailでは、milterという高度な機能を実現するためのインタフェースが提供されており、手軽かつ安全にメールの制御や書き換えを実装可能です。その反面、milterによる



多段MTAアーキテクチャ　　単段MTAアーキテクチャ

図-3 ハードウェアリソースの有効活用

拡張では、アーキテクチャ上、特にI/Oのオーバーヘッドが大きくなってしまいます。また、機能面でもSMXのような複雑なシステムを実現するには機能不足であると言わざるを得ません。Postfixやsendmail本体を直接改造するアイデアもあるのですが、本家のアップデートに追従し続けるコストは想像よりずっと大きなものです。

ベンダー製MTAを採用する選択肢はとても現実的でした。いくつかのMTAベンダーがISPや大規模メール送信事業者向けのMTA製品を開発しています。これらの製品でも、これまでに説明したような、一段ですべての処理を行うことをコンセプトにしたものが主流になっています。また、様々なセキュリティベンダーのアンチウイルスエンジンやアンチスパムエンジンを差し替えて組み込めるようになっていたり、大規模な配送系で必要とされる細かい要求を満たす、柔軟で極限まで細かなカスタマイズが可能になっているなど、ベンダー製MTAはオープンソースのMTAとは比べ物にならないほど多機能で強力です。我々にとっても目指していた配送系を実現するのに最も「手っ取り早い」選択肢でした。実際、多くのISPや大規模メール送信事業者ではベンダー製MTAを採用しており、SMXの従来の配送系でも部分的にではありますが、ベンダー製MTAを組み込んでいました。

ベンダー製MTAを導入することの唯一の、そして最大の懸念は、SMXのすべてがそのMTAと一蓮托生になる点です。単段MTA構成のアーキテクチャでは、MTAは配送系そのものです。また、配送系以外も、サービス仕様から運用手順に至るまで、システム全体がMTAに深く依存することになります。つまり、「MTAでできることがSMXでできること」になり、その逆も然りです。

IIJでは、お客様の声だけでなく、メール業界やセキュリティ業界の最新動向も詳しくウォッチしながら、積極的なSMXの機能拡張を続けています。そのため、ときには他の事業者では必要としないような機能が配送系に要求される場合もあります。このようなケースで、MTAが備えていない機能をベンダーに追加してもらうのは一般的に困難です。MTAベンダーも数多くの顧客を抱えていますので、多くの顧客に必要とされる機能や、彼らにとって重要な顧客が必要とする機能の開発が優先されるのは必然であり、独自性の強い機能やニッチな機能の追加の優先度は低くならざるを得ません。ベンダー製MTAは、要求する仕様が明確かつ将来の仕様変更が少ないケースには向いていると思いますが、SMXの積極的な拡張方針を支え切れるかどうかは未知数でした。

また、ベンダー製MTAにも会社買収のリスクがあります。MTAにはシステム全体が大きく依存しますので、買収が実際に起きた場合の影響はアンチウイルスエンジンやアンチスパムエンジンに比べると甚大です。実際、ここ数年間で、MTAベンダーや製品の買収が数件ありました。MTAを開発しているベンダーは絶対数がそれほど多くないため、割合にするとかなり高く、見過ごせないリスクです。

最後の自社開発という選択ですが、こちらも決して容易い選択肢ではありません。ISPレベルの膨大な流量を支えるMTAには、極めて高い安定性、堅牢性及びパフォーマンスが求められます。それに加えて、SMXの多様な機能と柔軟性を実現しなくてはなりません。更に、将来に渡る機能拡張を支える技術力も求められます。

そのようなMTAをもしゼロから開発するのであれば、自社開発という決断はとてもできなかったかもしれません。しかし、IIJではメールシステムのコンポーネントの多くを自社開発してきた経験とノウハウがありました。そして頼りになる開発チームが揃っていたため、リスクは高そうだが、得るものも多い自社開発を決断することができました。

3.6 リニューアルの成果

3.6.1 開発目標の達成

MTAをはじめとしたシステム全体のリニューアルプロジェクトは最初のリリースを迎えるまでに丸1年以上を要し、筆者が経験した中でも最も大規模な開発プロジェクトとなりました。

長い開発期間と度重なるテストの末に完成したシステムでは、あらかじめ定めた目標は軒並み達成できました。柔軟かつ多機能なMTAによって、単段MTA構成アーキテクチャの配送系を実現することができました。従来の配送系で課題となっていたストレージI/Oは設計のとおり大幅に削減され、配送系全体のパフォーマンスも向上しました。ウイルスフィルタや迷惑メールフィルタは、大幅に見直したことで検知精度が一段と向上しました。また、それぞれのエンジンの検知率を継続的にウォッチすることで、検知率に変化があった場合にすぐにアクションを取れるようにしました。

このようにMTAを自社開発したことで、MTAベンダーが買収されるリスクから解放され、エンジンの入れ替えを可能にすることでセキュリティベンダーが買収された際の影響も最小限にとどめられるようにしました。今回のリニューアルで最も重要だったのは、すごく当たり前のようですが、IIJがベンダーの買収劇にふりまわされることなく、自身でサービスを主体的に動かすことができる基盤にできたことだと考えています。

3.6.2 副次的なメリット

当初から定めていた目標以外にも、いくつかの副次的なメリットがありました。

まず、不具合対応のスピードが改善されました。ベンダー製MTAの場合、不具合が発生するとその発生条件を洗い出してベンダーに報告し、修正を依頼するのですが、再現条件が不明だったり、再現条件にお客様の情報が含まれているためベンダーに渡すことができなかったりするため、不具合を確認してもらうまでに時間を要したり、そもそも不具合の確認ができなかったりすることもしばしばです。一方で、自社開発の場合は、運用チームと開発チームが緊密に連携できるため、特に不具合の原因の特定が圧倒的に早く、暫定対応・恒久対応ともに素早く適切に進めることができます。

また、直接比較することはできないのですが、結果的に自社開発の方が、チームが高いモチベーションを保った状態で開発を進められたのではないかと感じています。MTAまたはその他にベンダーの製品を組み込んだシステムを開発する場合、開発チームではベンダーの製品とのインタフェースの開発を行うのですが、製品の不明瞭な仕様と格闘する不毛な作業が多く、個人的にあまり楽しくない作業であることがしばしばです。一方、自社開発では作業量が圧倒的に多く、それが開発チームの負担になることが大きな懸念でした。しかし、忙しくこそあったものの、決してチームが疲弊していくという雰囲気ではなかったように感じています。やはり、自分たちの手で大規模なシステムを作り上げ、それが徐々に動く面白さがあるのではないかと思っています。

新システムは2017年4月にリリースし、丸1年かけて旧システムから移行しました。リリース後も様々な意見や要望をいただき、機能の追加や不具合の修正を行いましたが、矢継ぎ早の改修を実現できたのも、システムを自社開発したからこそ達成できたものと思っています。

補足をすると、ベンダーの製品を全面的に活用したシステムを否定するつもりは全くありません。どちらにもメリットとデメリットがあるため、状況に応じて適切なバランスを選択することが必要だと考えています。SMXでも海外を含む数多くのベンダー製品をシステムに組み込んでおり、日ごろからベンダー各社と緊密に連携を図りながらサービスを提供していることを最後に付け加えておきます。

今回は、SMXの配送系の設計について紹介しました。SMXは新しく手に入れたアーキテクチャを活かして、これからも進化を続ける所存です。

執筆者:
鈴木 高彦（すずき たかひこ）
IIJ ネットワーク本部 アプリケーションサービス部 サービス開発課 シニアエンジニア。
2004年IIJ入社。以降、一貫してメールサービスの開発に従事。
オープンソース送信ドメイン認証フィルタプログラム yenma の開発者。