地方公共団体向け ASP サービスから学ぶ「拡張性」と「保守性」の意識

富士通エフ･アイ･ピー株式会社

■ 執筆者Ｐｒｏｆｉｌｅ ■

2014 年　富士通エフ･アイ･ピー（株）入社
第二システム事業部　公共システム部所属
LGWAN-ASP プロジェクト担当

荒井　栞

■ 論文要旨 ■

筆者は、アウトソーシング・クラウドに特化した、インフラ基盤の構築・運用に携わっている。現状の環境から新しい IaaS 基盤への拡大を受け、利用者・提供者への意識からこれまで「こなす作業」であったものが「考える作業」に変化していった。その中でもっとも重要なテーマが「拡張性」と「保守性」の考慮である。

本稿では、IaaS 基盤の構築を通して、現状環境の理解と課題の認識、課題に対するアプローチの仕方、さらにその中での変化していった筆者の意識について述べる。

■ 論文目次 ■

１．はじめに ……《 3》
１．１　当社の概要
１．２　LGWAN-ASPサービスの特徴

２．「こなす作業」から「考える作業」へ……《 4》
２．１　「利用者・提供者」への意識と「社会に対する影響」の意識
２．２　課題

３．課題解決のためのアプローチ ……《 5》
３．１　現状の環境の理解と拡張性の考慮
３．２　施策の検討
３．２．１　施策１ ― 「拡張性」と「保守性」の考慮
３．２．２　施策２ ― 「セキュリティ（ポリシー）」の考慮

４．成果と今後の目標……《 8》
４．１　課題の解決
４．１．１　成果１―ミドルウェアの設定への活用
４．１．２　成果２―レビューの観点の変化
４．２　今後の目標

５．おわりに ……《 9》

■ 図表一覧 ■

図１　LGWAN-ASPサービス構成概要……《 3》
表１　LGWAN-ASP サービス利用形態……《 4》
表２　問題解決アプローチとその効果……《 8》

１．はじめに

１．１　当社の概要

当社は全国に 16 箇所あるデータセンターを基盤に「アウトソーシング」、「クラウド」、「ソリューション」の３つのサービスを提供している。中でも「アウトソーシング」では、システムの企画からインフラ構築、運用、保守までのライフサイクル全般を支援しており、安心・安全で高品質なサービスを実現できるワンストップソリューションの提供が強みとなっている。また、企業の中で ICT システムの重要性が増し、「クラウド」サービスの導入が注目される中、大規模なデータセンターを活用した Infrastructure as a Service（以下、IaaS という）の提供にも力を入れている。

私は配属されてからの 1 年間、データセンターに特化したアウトソーシング・クラウドサービスのひとつである「LGWAN-ASP プロジェクト」で、サービスの立ち上げからシステムの設計構築・運用に携わってきた。LGAWN-ASP の概要は次項にて述べる。

１．２　LGWAN-ASP サービスの特徴

総合行政ネットワーク（Local Government WAN：以降 LGWAN という）とは、全国の地方公共団体を結ぶ行政専用のネットワークである。この LGWAN を介して、地方公共団体向けにアプリケーション・サービスを提供するプロバイダを「LGWAN-ASP（Application Service Provider）」という。平成 25 年から LGWAN は「政府共通ネットワーク」として整備され、地方公共団体では業務システムの ASP 利用が本格化している。

当社が提供する LGWAN-ASP サービスは、横浜データセンターに ASP 提供可能な LGWAN 接続基盤を構築し、LGWAN 全国域への接続環境を 24 時間 365 日提供している。また、LGWAN 接続基盤上には ASP 事業者が地方公共団体向けにサービスを展開できるように IaaS 環境を構築し、クラウドサービスとして仮想マシンの提供も行っている。LGWAN-ASP サービス構成概要図を**図１**に、利用形態を**表１**に示す。

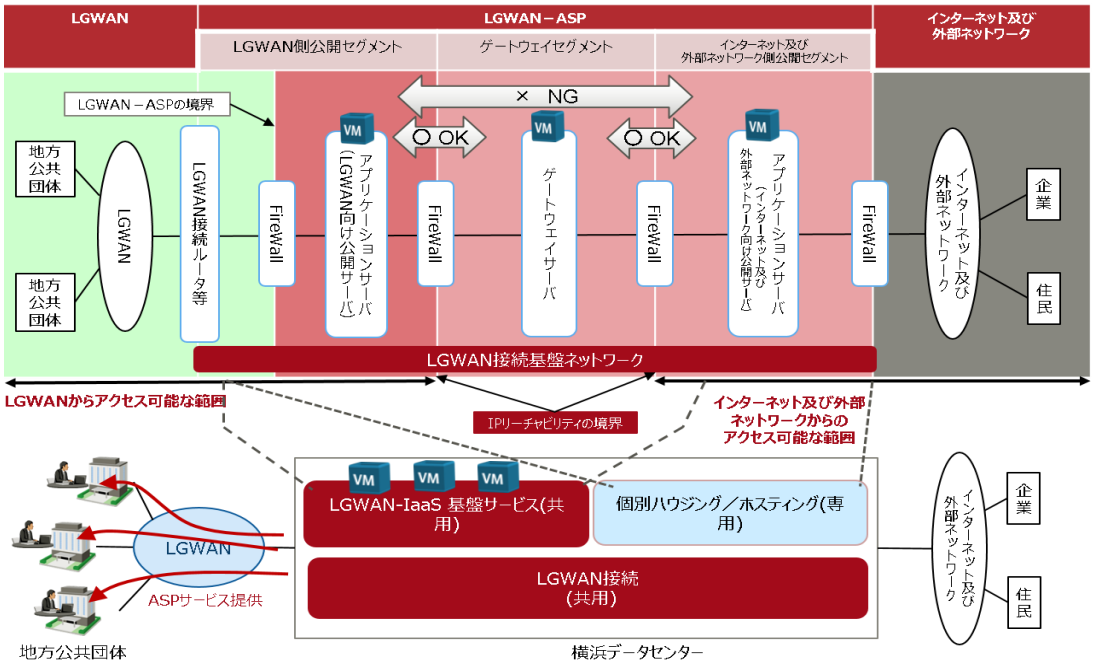

図 1 LGWAN-ASP サービス構成概要

表１　LGWAN-ASP サービス利用形態

利用形態･方法1	利用形態･方法2
LGWAN接続基盤 + LGWAN-IaaS基盤 （VM）利用	LGWAN接続基盤 + 自社システム持ち込み （ハウジング/ホスティング）
ASPサービスに必要なAPを各セグメント上で当社が提供するVM上に構築	利用者が横浜DCに持ち込んだシステムからLGWAN接続のネットワーク基盤のみ利用してLGWANに接続

LGWAN-ASP サービスの提供には、以下の点を考慮しなければならなかった。

まず一点目は、LGWAN 独自の規則の考慮である。LGWAN は地方公共団体情報システム機構（以下、J-LIS という）が運用を担っており、独自の様々な規則が存在する。例えば、接続環境は「LGWAN 公開セグメント」、「ゲートウェイセグメント」、「外部接続セグメント（インターネット接続セグメント）」と３セグメントを論理的に分割する（図１参照）。LGWAN に接続する外部ネットワークシステムは、LGWAN に対して、自ネットワークを中継した IP リーチャビリティが発生しないように接続を構成する必要があり、LGWAN の閉域性やセキュリティを担保できる環境としなければならない。

二点目に、本サービスの利用者は地方公共団体であり、サービスを提供する ASP 事業者にとっても、重要な社会インフラの位置づけとなる。当社が提供する環境は利用者/提供者の双方にとってトラブルが発生すれば社会に対する影響が非常に大きいことを常に意識しなければならない。

２．「こなす作業」から「考える作業」へ

２．１　「利用者・提供者」への意識と「社会に対する影響」の意識

LGWAN 接続基盤の構築では、主に私は要件に合わせて「必要な作業をこなす」ことに積極的であればよかった。接続基盤は実際にお客様のアプリケーションが稼動していない状態で、「LGWAN に接続する」というゴールが決まっていたからである。しかし、次期構築である IaaS 基盤ではそうはいかなかった。IaaS の特徴である、顧客の増加を見越した構築が求められ、更には顧客ごとに弊社へのサービス提供形態の要求が変化する。それぞれの顧客に合わせたサービス要件を考え、設計・構築作業や運用計画を練り、安心・安全で高品質なサービスを実現する必要があった。

２．２．課題

IaaS 環境の構築では、基盤となる物理サーバの構築や顧客である ASP 事業者（以下、テナントという）に提供する仮想サーバの構築、既存のネットワークの拡張・接続を行ってきた。これまで構築してきた経験にのっとり、弊社内部で管理している運用サーバやネットワーク構成・設定は現状で稼動しているものを継承することを基本として考えていた私は、早くも壁に突き当たる。仕事を進めるにあたり、私には経験以上のものが求められた。

私に必要なスキルや課題は以下のものであった。

（１）ネットワークやミドルウェアの「拡張性」と「保守性」を考慮した構成定義

LGWAN 接続基盤の環境は拡張性・保守性の考慮に不足があったため、LGWAN 接続基盤内の構成方針の見直しを指示され、任された。

（２）「顧客要件」に合わせた作業やスケジュール調整

定められたスケジュールの中で顧客との頻繁な意識合わせや、時には J-LIS と顧客の仲介として調整が求められた。

（３）LGWAN 環境の理解

上記二点の課題を克服するためには、LGWAN の要件や構成を理解しなければならなかった。

本項では私が任され、最も良い経験となった項番（１）の課題に対して、「現状のネットワーク環境の問題を解決していく過程」を述べていく。

３．課題解決のためのアプローチ

３．１　現状の環境の理解と拡張性の考慮

急務となっていたのは LGWAN 接続基盤と IaaS 基盤の接続のための、LGWAN 接続基盤側のネットワーク設定の整備だった。整備のためにはまず現状の環境を理解しなければならない。私は既存のファイヤーウォールの環境設計書を読み込むことからはじめた。

設計書の読み込みで分かったことは、これまでと同様の設定方法をとっていれば、これからテナントが増加するごとに細かな変更作業をしなければならず、作業リスクや工数の増大化が発生してしまうということだった。

３．２　施策の検討

ここで私は、この問題を考えるにあたり、「拡張性」や「保守性」と表現される内容とは一体何かという疑問と、それを理解する手段を模索する事となった。そこでまずは、現状の問題点を洗い出し、それに対する施策を検討した。

３．２．１　施策１ ― 「拡張性」と「保守性」の考慮

ファイヤーウォールのフィルター設定における問題点は、以下の通りであった。

【問題点】

◆ Class-map のほとんどがアドレスの直書きである

・設定の追加や変更の際に Class-map の書換えが必要なため、作業量が多くなる

◆ 同一の通信で複数ポートを持つ通信において、ポートごとに class-map が存在している

例）同じ HTTP 通信で複数ポートを持っているもの（80/tcp、3173/tcp、8443/tcp）

・ポートが多いほどに Class-map が大量に発生し、管理が煩雑になる

※Class-map の定義

通信の疎通許可の定義をする。構成要素は接続元 IP アドレス（source-address）、宛先 IP アドレス（destination-address）、宛先ポート（destination-port）である。例え

ば、NTP 同期の通信は以下のように記述する。

例）IP アドレス 172.31.1.1 のクライアントサーバから 172.31.2.1 の NTP サーバへ時刻同期を行う場合

```
class-map match-all ntp
    match source-address ipv4 172.31.1.1
    match destination-address ipv4 172.31.2.1
    match destination-port 123/udp
```

前提として、フィルター値には一つのアドレスを直に記述しても、アドレス群（172.31.1.1-172.31.1.10 など）として複数のアドレスを記述してもよい。また、アドレスをまとめて「host-group」として定義することで拡張性を持たせることができる。この設定を「フィルター設定」という。

以上の洗い出しから、解決策を悩みながら考えるうちに、「拡張性」や「保守性」とは一般的に表すことができず、自分自身が自ら考えていくことではないかと気づいた。そして自分なりに「拡張性」と「保守性」を考慮し、以下の施策を検討した。

【施策１】

① 同一ネットワークに複数機器が存在するか、増設可能性のある場合はアドレス群とし、ネットワーク単位でフィルター設定する

② 管理サーバ・端末グループ、テナントサーバグループなど、決まった通信を行う機器を host-group 化する

③ 同一の通信で複数ポートを持つ通信は、まとめてポート群とする

以下は①、②の例である。

172.31.1.0/24 のネットワークの運用管理サーバやメンテナンス PC など、サーバを管理する機器をグループ化する。

「kanri」という名前の host-group を作成する。

```
host-group kanri
    host ipv4 172.31.1.1
    host ipv4 172.31.1.198
    host ipv4 172.31.1.150-172.31.1.159
    ……
```

新しい機器が増えたらここに追記する

これにより、class-map の source-address や destination-address には上記のような host-group を設定すれば、新たなアドレスは host-group に追加するだけよくなり、Class-map の書換作業が発生しなくなる。「拡張性」と「保守性」の問題を解決できたように思える。

ところが、上記施策ではセキュリティ面を考慮できていないことに気づいた。例えば、テナントサーバ→弊社管理サーバへの通信について考察してみる。テナントサーバから、「172.31.1.1」宛ての通信を許可する場合に、上記のような「kanri」への通信を許可するとする。すると、通信要件にない「172.31.1.198」宛ての通信も許可されているため、本来は許可したくない不要なアクセスが発生してしまう可能性がある。つまり、「管理のし易さ」の観点が先行しすぎてしまっていたのである。自分がこれで良いと考えていた施策にもまだ落とし穴があり、さらに模索し続ける必要性を痛切に感じる結果となった。

３．２．２　施策２ ― 「セキュリティ（ポリシー）」の考慮

そこで下記のポリシー設定について検討し、次の施策を実施した。

【ポリシー】

◆　セキュリティ面を考慮し、弊社運用環境―テナント業務環境間の通信ではネットワーク単位のアドレス群によるフィルター設定は行わない

【施策２】

④　弊社運用環境―顧客業務環境間の通信では、通信要件で定めたアドレス・ポートのみ通信を許可する

以下は、施策１、施策２検討前と検討後の class-map の例である。

《施策検討前》

テナントサーバ（172.31.11.1、172.31.12.2、172.31.13.3）から、弊社運用環境の管理サーバ（172.31.1.30）に対する HTTP 通信をフィルター設定した。

```
class-map match-all Unyou-http-1
    match source-address ipv4 172.31.11.1,172.31.12.2,172.31.13.3
    match destination-address ipv4 172.31.1.30
    match destination-port 8080/tcp

class-map match-all Unyou-http-2
    match source-address ipv4 172.31.11.1,172.31.12.2,172.31.13.3
    match destination-address ipv4 172.31.1.30
    match destination-port 2535/tcp
```

《施策検討後》
テナントサーバへ「tenantSV」という host-group の適用と、ポート群の適用をした。

```
class-map match-all Unyou-http
    match source-address host-group tenantSV
    match destination-address ipv4 172.31.1.30
    match destination-port 8080/tcp, 2535/tcp
```

表２　問題解決アプローチとその効果

カテゴリ	実施前	実施後	効果
拡張性と保守性 フィルター設定	同一通信・複数ポートの Class-map の存在	グループ化による集約	新規機器追加時の容易性の確保
セキュリティ ポリシー設定	不要な通信が発生	不要な通信を排除	セキュリティの確保

これにより、「拡張性」と「保守性」を考慮した構成定義を実現することができ、結果、トラブルを低減させる事によって、システムの社会に対する影響をどのように考慮するべきかも学んだ。

また今回の対応を通じて、「拡張性」と「保守性」とは、言葉の上での意味は理解したつもりであったが、その本質に気づけていなかったのだと感じた。それが実際には、それぞれのシステムで異なるのだということを少しは理解できたと考えている。

４．成果と今後の目標

４．１　課題の解決

「拡張性」と「保守性」の考慮により、既存のファイヤーウォールの構成を改めることができた。これを基盤とし、IaaS 基盤ファイヤーウォールの設計･構築にも取り組み、LGWAN 運用基盤全体のネットワーク環境を整備することができた。

また、この成果は以下２つの成果ももたらした。

４．１．１　成果１―ミドルウェアの設定への活用

このような「拡張性」と「保守性」の考慮の仕方はファイヤーウォールのみでなく、ウ

イルスバスターやSystemwalker Centric Managerなど、既存のミドルウェアの拡張時にも活用することができた。これらは加えて顧客の要求に合わせた設計が必要のため、ベースとなる考えの確立は非常に有効であり、構築時に作業効率の向上と単純なオペレーションミスの防止に効果が見られた。

４．１．２　成果２―レビューの観点の変化

これまで設計書や運用手順書のレビューの観点は機器との整合性やオペレーションの分かりやすさを中心としてきたが、加えて「拡張性」と「保守性」の考慮もできるようになった。当プロジェクトは要件定義・構築において他部署との連携をしている。設計書や運用手順書の作成を他部署に依頼し、細かなレビューを行ってきた。VMware ESXi の設計書を例に上げる。IaaS 基盤は顧客の増加に伴いセグメントが増加する。現在の構成では仮想スイッチのセグメント管理が複雑になってしまうため、カテゴリやグループ化と言うキーワードによりテナントごとに設計書を更新できるよう、書き方の工夫を依頼した。

また、今後の顧客拡大に向けてドキュメントのどの部分をメンテナンスすればよいのかも明確になり、ドキュメント管理を有効にすることもできた。

４．２　今後の目標

これまでは設計や構築といった内部作業や調整を主に担当してきた。その中で、今までは目の前の「作業」をこなすことで精一杯であったものが、「利用者・提供者」と「社会に対する影響」への意識を持つことにより、能動的な作業やアプローチ方法を身につけることによって以前よりも視野を広げることができたと思う。私が次に実践しなければならないことは、サービス仕様に合わせた顧客ごとのサービス要件を「作っていくこと」であると感じている。今後は顧客の増加に伴う IaaS 基盤環境の拡大とともに、SE として非常に重要な「顧客視点」や「社会への影響」の観点も磨くことでお客様へよりよいサービスの提案や提供をしていきたい。

５．おわりに

配属されてからの１年、LGWAN-ASP プロジェクトという新サービスの立ち上げから運用まで経験したことは、SE の卵として非常に貴重で大きな経験となった。当サービスはまだまだ駆け出しであり、これからのサービス拡大に大きな期待がかかっている。今後より多くのサービスに適用可能な基盤の提供ができるよう、目標に向かって確実にステップアップしていきたい。

本稿の執筆により、配属されてからの１年間をじっくり振り返ることができた。自分の成果と課題が浮き彫りになり、改めて自分を見つめなおす良い機会だったと思う。