O-009

F/W越しのMSファイルサーバでのファイル共有

Anecdotal report of file sharing with Microsoft Windows over F/W

○梅田浩貴†，植田泰士†，久留真治†，祖父江 真一†
Hiroki UMEDA†, Yasushi UEDA†, Shinji HISADOME†, Shin-ichi SOBUE†

1. 概要

宇宙航空研究開発機構（JAXA）は，平成15年10月旧宇宙3機関が統合し誕生したが，その経緯から，JAXAの機構内LANの中には，現在F/Wが存在しており，機構内部の通信にF/Wを越える通信が発生する．一方，Microsoft系サーバの通信では多数のポートが利用されることから、F/Wを越えて機構全体への共通的に提供すべきサービスの提供を行うことに困難が生じている．本報告では、現ネットワーク環境下でのファイルサーバの利用のための課題ならびにファイルサーバのWindowsドメインの機構全体への展開などの今後の課題について報告する．

2. JAXAのネットワーク

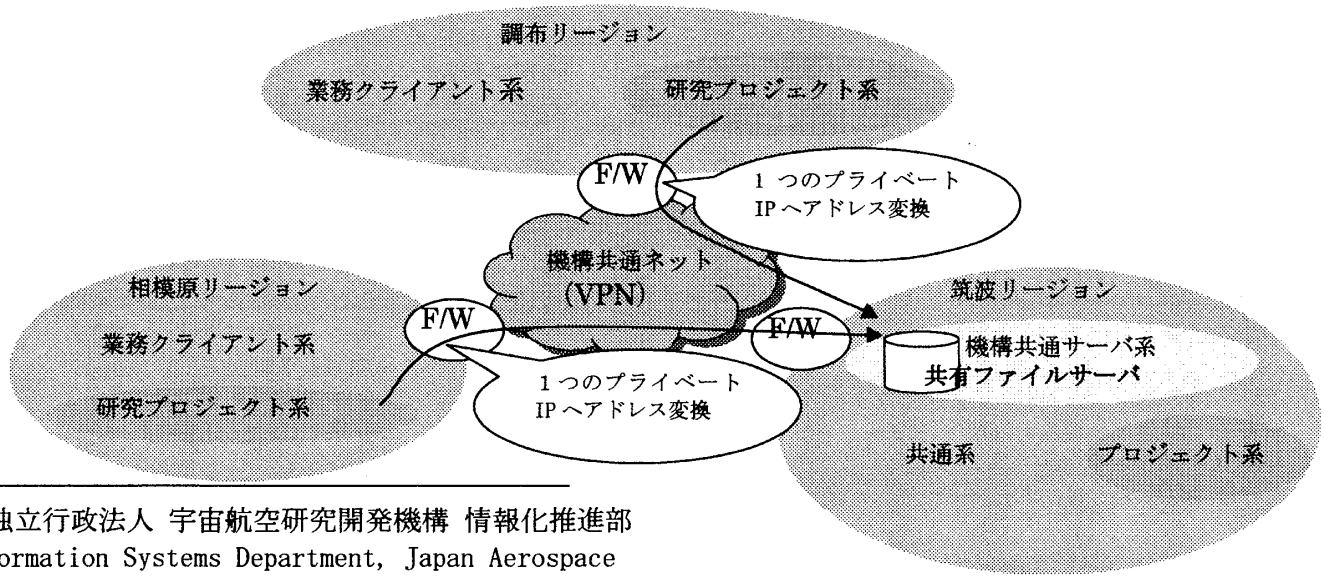
JAXAにおけるネットワークの構成概要を図1に示す。JAXAでは大きく分けて筑波、相模原、調布の3つのリージョンが存在する。各リージョンには業務クライアント系、研究プロジェクト系と呼ばれるサブネットが存在し、それぞれにＩＰアドレスが異なる体系で付与されている。このため、各リージョンの違いを吸収するとともに、業務クライアント系と機構共通のサーバ系を接続するために、各リージョンは機構共通ネットと呼ばれるVPNで結ばれ、各リージョンにはファイアウォール（F/W）が設置されている。研究プロジェクト系のF/Wでは、アドレス変換（NAPT）が実施され外部から内部のネットワークが直接参照できないようになっている。

また、旧機関におけるネットワーク構築の生い立ちの違いから、リージョンのネットワークはそれぞれ異なる性質を少なからず持っている。このため、異なるネットワークポリシーやセキュリティポリシーが存在し、結果として、ネットワーク統合においては、単純にネットワークを相互接続し完了という事ではなかった。他にも、日常業務を停止することなく運用体制を維持しながら、ネットワークを論理的に物理的に統一していくという困難な作業となった。このため、統合にむけたＩＰアドレスの見直しなどの作業は現在も続行中となっている。

3. 共有ファイルサーバ（共有FS）

JAXAでは、日常業務遂行のための全機構的な情報交換・共有・蓄積の手段を提供し、より一層の業務効率化を進めること、およびシステムの運用効率化・体制の強化によって、通常業務におけるデータ信頼性やセキュリティ水準を機構全体で一定水準まで向上させることを目的として、機構内に散在する部門ファイルサーバを集約・統合した共有FS及び同サーバの利用に際して必要となる認証サーバの整備し、共有FSをドメインコントローラとするWindowsドメインを構築した。
しかし、共有FS整備計画は旧NASDAにて策定されたため、当初利用想定範囲は筑波リージョンに限られたものであった。

図１．JAXAのネットワーク構成



† 独立行政法人 宇宙航空研究開発機構 情報化推進部
Information Systems Department, Japan Aerospace Exploration Agency

そのため、調布リージョン・相模原リージョンからの利用について規約等が十分な運用体制が整っていなかったが、管理部門やロケット・衛星部門が機構の３つのリージョンにまたがって業務を実施する必要が発生し、このため、ＦＷ、ＶＰＮ越し調布リージョン・相模原リージョンからの利用を暫定的に開始するための作業が必要となった。

4. 問題点

筑波リージョンにある共有 FS を相模原と調布の各リージョンより使用する際に、次の４つの主な問題点があった。

①Windows ファイル共有及びその際のユーザ認証に必要となる通信（UDP 等）を許可する必要がある。これによって F/W に多数の開放ポートを設定しなければならず、セキュリティの低下を招くという問題である。

②調布もしくは相模原リージョンでは、NAPT による１つのプライベート IP アドレスに変換のため、端末個別の IP アドレスが共有 FS から見えない。そのため、共有ファイルサーバに何か問題が起こった際に、どこからアクセスされたか特定されにくく、原因究明が困難になるという問題である。

③筑波リージョンではプライベート IP アドレスを割り当てている。それに対し、相模原・調布リージョンの研究プロジェクト系の多くは、グローバル IP アドレスを割り当てているというアドレス体系が異なるという問題である。

④筑波リージョンでは標準端末は全て同一のウイルス対策ソフトが入っており、サーバから強制的にパターンが更新されている。相模原・調布リージョンの端末におけるウイルス対策はそれとは異なり、各部門毎に一様でないという問題である。

以上の問題のすべてを根本的に解決するためには、ネットワークの再構築などの大規模な作業が必要となってしまうため、ネットワークの変更を小さくし導入し易い、且つセキュリティを維持できる解決方法を検討した。

5. 解決案

解決案として以下の３つが検討された。

案１：相模原リージョン・調布リージョンからの利用する端末に特定の IP アドレスを割当て、F/W でのアドレス変換では NAPT ではなく一対一の変換が可能な NAT とし、機構共通ネット上で使用されているプライベートアドレスを割当てる設定を行い、共有 FS にアクセスする。

案２：相模原リージョン・調布リージョンから共有 FS を利用したい端末が接続するネットワークを、V-LAN によってネットワークを切り離し。業務クライアント系としてプライベートアドレスを割当てる。

案３：共有 FS で利用する端末に IP-VPN のクライアントソフトウェアをインストールし、機構共通ネットを経由せずに筑波リージョンへ直接接続し、共有 FS へアクセスする。

案１は、現状の運用ポリシーに適合しており技術的な確実性は高いが、F/W に対して端末数分の設定をする必要があり端末数が増加すると管理が煩雑となってしまう欠点がある。案２は、端末のネットワーク移設となるため端末数の増加には柔軟に対応できるが、研究・プロジェクト系の資源を利用している端末がアクセスできなくなってしまうという欠点がある。案３は、共有ファイルサーバにとってバックドア的存在であり、VPN クライアントソフトウェアのサポート体制の構築をしなければならないと言った欠点がある。

本対応は暫定処置ということもあり、少数の端末が共有ファイルサーバにアクセス可能であればよいので、案１を採用することにした。

他にもファイアウォールのポート開放とウイルス対策ソフトの一様でないことによるセキュリティ懸念については、ポートの開放を最小限にする、共有ファイルサーバへアクセスする端末の対策ソフトは同様のソフトとしパターンファイルが最新にする、Windows のセキュリティパッチソフトを速やかに適用する、サーバの稼動状況を常に監視するといった一般的な対策を施した。

6. 今後の課題と展開

案１はあくまでも暫定的な措置であり、今後利用ニーズの増加により、相模原・調布リージョンの F/W に係る処理負荷や、処理性能上限、端末追加の度にネットワークの設定変更が伴うため管理・運用の手間、共有ファイルサーバの Windows ドメインへの非参加状態による影響等の基本的な課題を解決する必要がある。

上記とあわせて、JAXA では Windows ドメインの統一を目指している。各リージョンに共有ファイルサーバを設置し、筑波リージョンにある共有 FS をルートドメインとし、相模原と調布リージョンの共有 FS をサブドメインとする Windows ドメインを構築する。この設置により、WAN 回線を流れるトラフィックは通常時ドメインコントローラ間の複製トラフィックのみとなり、現状より F/W のポートを開放しなくてもよいためセキュリティ水準は向上する。さらに、Windows ドメインを構築することにより ActiveDirectory に機能を最大限に活用できるため、管理権限の委譲に伴い運用負荷の軽減、グループポリシー適用によるセキュリティや利便性の向上が期待できる。

各リージョンに共有 FS を展開し統一ドメインを構築するためには、以下の検討が必要となり、今後の調整課題となっている。

・ドメインコントローラ間の複製トラフィックの測定
・ドメイン統一による既存サービスの動作確認
・登録・管理情報が全機構的に一致しているか
・各リージョンでの運用体制の構築

7. 参考文献

[1] 植田泰士 JAXA における全社共有ファイルサーバ構築と今後の展望について FIT2004