利用形態に応じたネットワークストレージ環境の構築事例

石井, 大輔
九州大学応用力学研究所

https://doi.org/10.15017/4794818

出版情報：九州大学応用力学研究所技術室 技術室報告. 4, pp.48-51, 2022-07. Research Institute for Applied Mechanics, Kyushu University
バージョン：
権利関係：

九州大学応用力学研究所 技術室
技術室報告 Vol. 4, 48-51

利用形態に応じたネットワークストレージ環境の構築事例

石井　大輔

要　旨

ネットワーク越しの利用を前提に、ファイル（デジタルデータ）の保管・共有をするためのローカルストレージとして、様々な OS・H/W で構成されるネットワーク接続型ストレージ（NAS）がある。今回は、外部公開運用を想定した NAS の構築事例について紹介する。具体的には、FW を配置して多層防御する前提での NAS 構築ではなく、インターネット（外部ネットワーク）下での運用を想定したセキュアな高機能 NAS の設計・構築に取り組んだ。

キーワード

NAS　セキュリティ　外部公開　SFTP　GUI / CLI

1．はじめに

未曽有の COVID-19 に端を発したテレワークという新たな勤務形態は、働き方改革の一環として、業態によっては今や定着しつつあり、ワークライフバランスを実現するための一助となっている。この背景には、時間や場所を有効に活用して業務を遂行するために今や必要不可欠となっている、情報通信技術（ICT）の躍進と普及が根底にある。

現下において、あたかもオフィス（今までの勤務先）に居る時と同様の職場環境・会議環境などが、自宅や移動先で気軽に実現できるようになった一方、同時に必要不可欠とされているのは「セキュリティ」の担保である。情報セキュリティ・ネットワークセキュリティなど、昨今様々な用語が存在し、それらは少しずつ意味合いが異なるものの、ICT を活用する上でセキュリティの担保・堅持が非常に重要であることは疑う余地がない。

ICT やテレワークの普及・浸透によって利便性や機能性などが向上したことは、作業効率化や情報共有などの面から利点が大きい。その一方で、外部（社外等）から職場の重要データや個人情報等の機微なデータへ容易に接続できるようになったことは、セキュリティリスクが増大する契機となった。故に、利便性とセキュリティの均衡を考慮したシステム構築・運用が望まれるわけであるが、その線引きと実現は容易なことではない。

ここ数年における COVID-19 の影響によって、遠隔〇〇・シェア〇〇などの実現に関する相談・要請は格段に増え、大学の教育・研究を遂行する上で、半ば強制的に対応せざるを得ないものも少なくなかった（時間がない中での様々な環境整備には苦心した）。ただそういう状況においても、技術的には簡単に実現（導入）可能であるが、安全面を考慮すると軽々にはサービスの利用・提供を許可できない、と判断せざるを得ないことは当然あった。そこは技術面を担当する門番として、しっかりとした技術的裏付けに基づく判断を下す必要があるためで、世の中のシステム管理者・ネットワーク管理者は、同じような時期に同じような境遇を経験していたのではないだろうか。

何でもかんでも要求を突っ返してしまっては、我々の存在意義が薄れてしまう。そのため、技術職員に求められることは、出来る限りの事前調査・詳細検討を綿密にし、おおよその見当を付けて実現可否の初期判断をした上で、利便性とセキュリティを両立した技術的課題の実現に向けて挑戦することではないかと考えている。

現在まで多種多様な技術案件に取り組み、数々の課題解決や積極提案をしてきたが、その中でも今回は、様々な OS・H/W で構成されるネットワーク接続型ストレージ「NAS」に対する、利用形態に応じたストレージ環境の構築事例、特に外部公開運用を想定した試行例について紹介する。

２．ストレージについて

計算資源の高性能化や AI 技術の飛躍的な向上なども大きな要因の一つではあるが、例えば、ビッグデータを利活用した研究課題の解決や研究イノベーションの創出・実現のために、様々なデジタルデータの保管先として「ストレージ」と呼ばれる記憶装置は欠かせない。PC でいえば HDD がその一つだが、上記が関係するようなシステムで利用されるストレージの総容量は近年 P(ペタ)バイト級(10^{15} B)のものが一般的になっている。

また、このようなストレージの設置場所・構成環境も様々で、「オンプレミス（ローカル)」「クラウド」という独自環境で構成される形態が主流である（現在では両者の良いとこ取りをしたハイブリッド構成も存在)。この環境選択は、総費用（導入・運用・管理・保守に係る費用）対効果、利便性、取り扱うデータの価値（質・規模など)、セキュリティリスク、BCP 対策[1]など、ストレージ運用で重視する点に基づいて決定することになる。

では、大学内において複数の利用者で共用する目的として、ある程度の容量（例えば、TB 級：10^{12} B）を必要とするストレージの導入・運用を考えた場合、ローカルとクラウドのストレージ、どちらを選択するかと言われたら、初手として大抵は前者を選択するのではないだろうか。事実、研究室単位とかでも気軽に導入・運用しているケースは前者が圧倒的に多いことを見聞きするが、このローカルストレージの代表格が NAS である。

３．NAS について

少し PC 関係に詳しい人であれば、NAS(ナス)と聞けば、どういうものか何となく頭に思い浮かぶのではないかと思うので手短に説明するが、NAS（Network Attached Storage）とは、ネットワーク接続型のストレージのことで、ネットワーク経由でファイルを保管・共有するためのディスク筐体のことである。広義にはファイルサーバの一種で、導入のし易さや機能性、カスタマイズ性、導入・管理コストなどから、両者は大別される。

ネットワーク越しの利用を前提に、ファイルの保管・共有をするためのローカルストレージとして一般的なものと言えば、既述した通り NAS が挙げられる。NAS には家庭用もあれば、大容量・堅牢タイプの SOHO・大規模事業者向けなど多様に存在する。筐体内の共有設定や RAID 構築なども含め、最近の製品は一般ユーザでも手軽に設定でき、共有ドライブとして複数名でネットワーク利用できる点が特長である（逆に設定が緩く間違うと大変な事態に)。一方、製品の技術仕様や価格帯によっては、カスタマイズ性やセキュリティ強度の設定などで制限や限界があるため、運用時に望む技術要件や利用形態などを満たすことができる製品選択の見極めが重要になってくる。

４．NAS 構築に係る諸条件・構築事例

昨今、ゼロトラスト[2]の概念に基づいた防御モデルに移行しつつある中、境界型防御として外部ネットワークと内部ネットワーク（ローカルネットワーク）の境界領域にファイアウォール（FW）を配置して、当該機能によるポート開閉などで通信制御できることは承知している。しかし本稿の主旨は、仮に FW が存在しない運用下、すなわちインターネット（外部ネットワーク）から直接利用できる環境下であってもセキュアな本格運用を可能とする NAS の設計・構築に関することなので、その前提で進める。（NAS の前段に FW を配置し多層防御すれば、更に安全な NAS 運用環境を構築できるのは自明であるため触れない）

また、外部ネットワークから FW を超える VPN 接続を成功させた上での内部ネットワーク下の NAS 利用は、認証と暗号化で通信路の安全性が担保されているので特段問題なく推奨されるものだが、この方法は本旨から外れるため触れない。

４-１．機種選定について（１）

現在、NAS は様々なメーカーから多種多様な製品がリリースされているが、今回は運用時に望む技術要件や利用形態など（これらの詳細は割愛）を満たすことを大前提に、導入機種の選定を慎重に行った。その結果、検討時点では自身での利用経験や設定経験はなかったものの、様々な期待や可能性（技術的な拡張性や要求実現性）を感じた DSM（DiskStation Manager）機（Synology）を NAS の実機として採用し、外部ネットワーク上で運用することを想定したセキュアな高機能 NAS の構築を目指した。

なお、RHEL（RedHat Enterprise Linux）機（Newtech）の NAS の設計・構築をする機会があり、DSM 機と同様に外部ネットワーク上で運用することを想定したセキュアな NAS 環境構築

を試行したので、併記する。

ちなみに両案件は、今まで技術的に未経験の課題で、難儀する場面に何度も遭遇したが、自身の成長を期した挑戦的課題としては最適であった。

4-2．機種選定について（2）

一般的に機種選定を行うにあたり、まずNASの候補として選択肢に挙がりやすい製品は、身近で運用されていて評判がよかったり、自身に使用実績があったり、名の知れたメーカー品であったりしないだろうか。例えば、有名な TeraStation（BUFFALO）や LAN DISK（I/O DATA）などは大体 SMB や NFS などのプロトコルが利用できる仕様であるため、クライアント OS の種類（Windows, MacOS, Linux など）を特段気にすることなく、汎用性の高いファイル共有（ファイルサーバ機能）を実現することができる。

しかしながら、単一認証（ID/PW 認証）方式のためにセキュリティ面で不安を残す上、柔軟性や拡張性に乏しく、高度で精緻な詳細設定（ユーザ管理認証、セキュリティ制御、アクセス権限制御など）の実施・適用に難しい面が出てくる。例えば、多要素認証、接続元 IP アドレス制限、認証連続失敗の回数制限による自動フィルタリングなどの機能である。

そのため、外部ネットワークから直接利用できる環境下での運用を想定した NAS の設計・構築を目指す上で、上述したような仕様の製品は検討候補から早々に除外することになり、結果として前項の判断に至った次第である。

4-3．NAS の設置場所（ネットワーク上の位置）

インターネットで検索すると、「NAS の外部公開は安全に利用できるのか」「NAS をネットから直接接続できる環境にして大丈夫なのか」といったネガティブな記事が目に入る。一方で、上位に FW を置いて、ポート制御で FTP やファイル共有機能などのサービスを外部公開している NAS の運用事例や、DDNS を利用して外部ネットワークから内部ネットワーク下の NAS への接続を実現している運用事例があることも承知している。

この辺りは、NAS で取り扱うデータの価値や利便性、データ共有範囲などを含めた運用ポリシーにも関わってくることなので一概には言えないものの、少なくとも RIAM ネットワーク管理下では、このような運用には責任が持てない（恐ろしくて運用できない）のが実情である。そのため、NAS 自体のカスタマイズ設定だけで、外部ネットワーク上での運用を想定したセキュアな NAS 構築を実現するために、様々な角度から取り組んだ。

4-4．利用環境条件（設計指針）

NAS の利用環境は、便利で直感的に分かりやすい GUI 環境での操作を基本とするものが一般的に多いが、今回における DSM 機の構築はコマンドやシェルの実行を可能とする CLI 環境でも安全かつ簡便に利用したいとの要望に応えるべく、GUI 利用環境に加え CLI 利用環境での実現も課した（DSM 機における GUI 利用環境の基本整備は難しくなく、詰める必要がある要件は非常に限定的）。また、RHEL 機は CLI 環境の構築に限る。

今回、CLI 利用環境におけるセキュアなファイル転送方式（プロトコル）には、一般的によく利用されている SCP（Secure Copy Protocol）ではなく、SFTP（SSH File Transfer Protocol）を選択した。SFTP と SCP はプロトコルが異なるものの、ファイル転送をする上では転送中のデータの暗号化プラットフォームとして長らく利用されている。コマンドの使い勝手や高速性などから SCP の方がファイル転送に多用されている印象であるが、数年前から SCP の利用を控えるべきとの警鐘が鳴らされている[3]。

安全なファイル転送などを実現する接続ツール OpenSSH には SCP が実装されているが、SCP クライアントの脆弱性が複数発見されている。未だ既知のセキュリティ脆弱性を抱えているため、最新の RHEL 9 では SCP は非推奨となり、実際 SCP モードを使っても内部で SFTP モードに置換されるほど、安全性が憂慮されている。

また最新の Ubuntu 22.04 LTS においても、SCP モードの代わりに SFTP モードを使用するオプションがサポートされるようになっている[4]。このことは、SFTP は SCP よりも安全性が高く、将来的に様々な Linux ディストリビューションにおいて、SFTP がデフォルトのファイル転送プロトコルになることを示唆している。

なお割愛するが、ファイル転送の代表プロトコルに FTP があり、よりセキュアな通信を行う FTPS（FTP over SSL/TLS）、rsync があることは承知した上で、本件を進めていることを付記する。

4-5．構築事例

以下に、両 NAS（DSM 機・RHEL 機）の構築において定義・設定した内容や、利用環境のイメージ（図 1・図 2）などについて簡単に示す。

なお、今回の NAS 構築にあたって、技術的な工夫や発見、苦労が多々あったが、紙面の都合と安全上の観点から、技術的な詳述は控えておく。

<u>両 NAS 共通</u>　＊以下の実現方法は各機で異なる

・利用可能サービス／ポートの厳格管理
・SSH 接続不可（限定例外あり）
・指定時間内での連続ログイン失敗による IP アドレス遮断／アカウント保護
・接続元 IP アドレス制限
・NAS 内 FW 機能の有効化
・マルウェア／ウイルス対策

<u>GUI 利用環境</u>（DSM 機）

・webUI を通じた HTTPS での暗号化通信によるファイル転送（操作性重視）
・多要素認証方式によるログイン認証

<u>CLI 利用環境</u>（DSM 機・RHEL 機）

・ターミナル等を通じた SFTP での暗号化通信によるファイル転送（get/put）
・公開鍵暗号方式によるログイン認証

図 1　GUI 利用環境のイメージ図

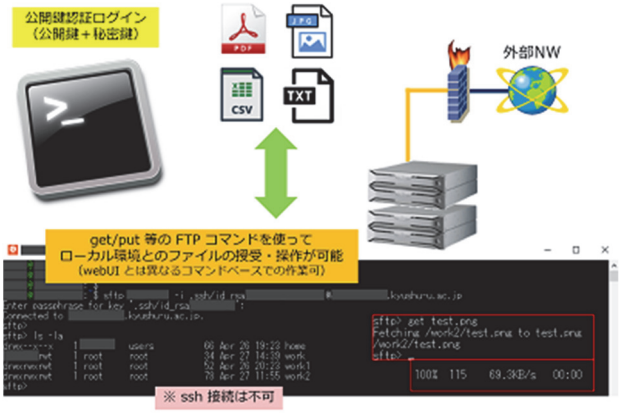

図 2　CLI 利用環境のイメージ図

5．おわりに

昨今におけるデジタル化の潮流の中、我々が日々取り扱うデジタルデータは、質・量ともに高度化（高品質化・高機密化）・肥大化していく傾向にあり、その勢いは増すばかりである。このようなデータ群が、国内の大学・研究機関等において安全に超高速でやり取りできる通信環境（SINET 6）も整備され、デジタル社会を取り巻く国内の情報インフラ環境は発展の一途を辿っている。

予期せぬウイルスの出現で世の中が激変し、勤務形態なども一変した現在において、我々が携わる大学業務で考えてみると、「リモート」「共同研究」「データ共有」「セキュア」「自動化」「冗長化」「高速化」「利便性」「汎用性」など、様々なキーワードを組み合わせたシステムやサービスの構築・運用が暗に求められているのかもしれない。

大それた革新的な技術開発や基幹構築などは軽々に実現できるものではないが、本稿で紹介したような NAS 構築の技術要素や NAS 環境の本格運用が、今後の学術振興や研究・教育の進展などに少しでも貢献することになれば幸いである。

参考文献

[1] https://business.ntt-east.co.jp/content/bcp/data_backup/
[2] https://www.ntt.com/bizon/glossary/j-s/zero-trust.html
[3] OpenSSH SCP deprecation in RHEL 9: What you need to know, Red Hat Inc., https://www.redhat.com/ja/blog/openssh-scp-deprecation-rhel-9-what-you-need-know
[4] Jammy Jellyfish Release Notes, Ubuntu, https://discourse.ubuntu.com/t/jammy-jellyfish-release-notes/24668

謝辞

本学応用力学研究所長の大気物理分野 岡本創主幹教授と気候変動科学分野 竹村俊彦主幹教授には、本開発に係る貴重な機会とご配慮を賜りました。この場をお借りして、御礼申し上げます。