

Synology QuickConnect ホワイトペーパー

—
Synology 製品との接続を便利に



目次

エグゼクティブサマリー	02
消費者と企業にとっての接続の未来	03
有望なネットワーク接続ストレージ	
静的外部 IP アドレスに不足している点	
ポート転送の問題	
NAS のためのシンプルで安全な Web 管理	04
QuickConnect とは？	
お客様とお客様の業務のための安全なソリューション	
QuickConnect の仕組み	05
単一の Web ポータルで接続性が向上	
QuickConnect 接続手順	
QuickConnect サービス	
QuickConnect のセキュリティ	
まとめ	10

エグゼクティブ サマリー

ネットワーク接続ストレージ (NAS) システムは、中小企業 (SMB) で大きなことを成し遂げるのに貢献しています。フリーランサーから従業員数百人の繁盛しているスタートアップ企業まで、貴重なデータにさまざまなデバイスや場所からアクセスできることは、どの企業にとっても成功に不可欠です。SMB では、大企業のようなわけにはいかず、常時リモート アクセスを実現しつつセキュリティ保護したくても、一般に IT リソースが限られています。

静的パブリック IP アドレスの構成、ポート転送ルールや複雑なネットワーク設定の手動での定義も、小規模企業にとっては負担となりえ、ひいてはデータセキュリティの低下につながりかねません。幸い、Web ベースの接続を簡素化した手順で使いやすい NAS サーバーにより、これらの課題が克服され、重要な業務ファイルへのリモート アクセスの実現とセキュリティ保護がスムーズになるため、中小企業はベストを尽くして目標を達成することに集中できるようになります。

消費者と企業にとっての接続の未来

今どきの SMB では業務も人員も、もはや 1 つのオフィスや地域に限られたものではありません。従業員も消費者も、オフィス空間のデスクトップ コンピュータに留まらず、個人のモバイルデバイスで日々の仕事を遂行することにますます慣れてきつつあります。

この変わりゆく環境で競争力を保つためには、誰もが協力し合い、いつでもどこでも情報を安全に共有できることが必要です。今日では、小規模企業も、より規模が大きい企業とまったく同様に、ドキュメント、動画、画像などの各種ファイルを直ちに保存したりアクセスしたりできることが求められています。これらのファイルをセキュリティ保護するだけでなく、小規模企業では、複数のデバイスとさまざまな権限レベルを持つ従業員にアクセス権を付与することも必要です。

有望なネットワーク接続ストレージ

NAS は、エンタープライズ クラスの専用データ センターを必要としない小規模企業の間で普及してきました。現に、NAS のグローバル市場は急速に成長しており、2016 ~ 2023 年で 21% の年間成長率 (CAGR) が見られることが予想されています。ただし、非公開の NAS サーバー上のファイルにリモート コンピュータやモバイル デバイスからインターネット経由でアクセスできるようにすると、SMB にとっての難題がいくつか生じます。

社外にいる従業員が NAS サーバー上の作業ファイルなどの資産に社内のプライベート LAN 外からアクセスするためには、パブリック ネットワークから接続するための信頼できる手段が存在する必要があります。ですが、一般的な手法、例えば静的パブリック (外部) IP アドレスやポート転送は、実装と維持に手間がかかるうえ、組織を新たな脅威にさらします。

静的外部 IP アドレスに不足している点

外部インターネット サービス プロバイダ (ISP) から組織のルーターに割り当てられた IP アドレスを使用すると、プライベート ネットワークとパブリック インターネットの間で通信できるようになります。外部 IP アドレスは静的か動的のどちらかですが、企業の大半が静的 IP アドレスを好みます。リモート デバイスにとって、永続的なアドレスのほうが絶えず変わる (動的な) アドレスより、見つけて接続しやすいか

らです。しかし、割り当て可能なパブリック IP アドレスの数には限りがあり、ISP はサポートを年中無休で提供する必要があることから、静的パブリック IP アドレスは動的パブリック IP アドレスより割高です。

そのため、多くの小規模企業を含め、顧客の大半に動的パブリック IP アドレスが割り当てられています。静的パブリック IP アドレスを所有することの別の欠点としては、デバイスを手動で構成する必要があり、多くの小規模企業にとって、そのために必要な労力と IT リソースが負担できる範囲を超えていることも挙げられます。静的 IP アドレスを持つことは、プライベート ネットワークをセキュリティの脅威にさらすことにもなります。というのも、固定アドレスの場合は、絶えず変化するアドレスの場合と比べて、潜在的な攻撃者に IP アドレスを特定し脆弱性を悪用する余地を与えてしまうからです。

ポート転送の問題

SMB は静的外部 IP アドレスを使用することのほかに、ルーターでネットワーク アドレス変換 (NAT) を使用するポート転送ルールを構成して、外部の IP アドレスとポートをプライベートの IP アドレスとポートにマッピングすることもできます。ポート転送は、プライベート ネットワーク内に隠蔽されているエンドポイントにリモート アクセスできるようにする効果的な手法ですが、プライベート ネットワーク上のすべてのデバイスと内部リソースについて、ルールを手動で作成および構成する必要があります。

ルールの変更や新しいルールの追加にも手動での複雑な構成が必要で、多くの小規模企業の限られた IT リソースにさらなる負担をかけることとなります。また、ポート転送は、静的外部 IP アドレスを使用する場合と同様、プライベート LAN をより大きなサイバーセキュリティリスクにさらす可能性があります。なぜなら、ハッカーはプライベート ネットワークに侵入して内部システムにアクセスするのに使用できるオープンポートのみをスキャンすればよいからです。

NAS のためのシンプルで安全な Web 管理

静的パブリック IP アドレスの使用と複雑なポート転送規則の構成という難点を克服するために、Synology QuickConnect では、Synology NAS サーバーにインターネット経由で簡単かつ安全にアクセスできるようにしています。QuickConnect を使用することで、IT 管理者がデバイスや複雑なポート転送ルールを手動で構成することなく、社外の従業員が自社のプライベート LAN 上のリソースにアクセスできるようになります。

QuickConnect とは？

名称からうかがえるように、QuickConnect は Synology NAS サーバーに簡単迅速に接続できるように設計されています。サーバーを立ち上げ、そのサービスを適切に提供するには、通常は IT 管理について一定レベルの知識が必要です。QuickConnect ではその必要はなく、ネットワークのオーバーヘッドを最小限に抑えるテクノロジーを通じて、Synology NAS サーバーへの接続を誰にとっても容易にします。

つまり、QuickConnect は NAS サーバーを立ち上げようとするユーザーが多く直面するいくつかの障壁を取り除きます。具体的には、QuickConnect ユーザーは静的外部 IP アドレスの所有、NAT ポート転送ルールの設定、クライアント デバイスの位置が変わった場合の WAN/LAN アドレス切り替えが不要です。

QuickConnect では当初から、ポート転送が可能でないネットワーク環境も含めて、どのようなネットワーク環境からでも特定の Synology NAS サービスに常時アクセスできるように設計されました。現在では、サービスに常時アクセスできるだけでなく、労力とネットワーク オーバーヘッドを最小限に抑えてアクセスできるような、包括的なソリューションを提供しています。それを実現しているのが QuickConnect の次のような機能です。

1. 永続的な簡単に覚えらる決まったサーバー ID (QuickConnect ID) - LAN 内でもインターネット経由でも使用可能
2. サーバーの場所の検出 (LAN/WAN 検出)
3. QuickConnect ホールパンチング
4. UPnP を通じた自動ポート転送
5. QuickConnect リレー サービス

6. QuickConnect Web ポータル

これらの機能により、QuickConnect ユーザーは他にはない次のようなメリットを受けることができます。

- パーソナライズされたサーバー ID
- ネットワーク環境によらず、どこからでもアクセス可能
- クライアント デバイスが QuickConnect 経由で NAS にアクセスする場合に必ず最短経路を選択

お客様とお客様の業務のための安全なソリューション

Synology QuickConnect では、NAS サーバーの統合 Web 環境が持つ利便性に加え、データの漏洩や傍受を防ぐのに必要なすべての予防対策が取られています。これらのセキュリティ対策で、静的パブリック IP アドレスやポート転送の使用に絡む主な不足分を克服しています。これらのセキュリティ対策には、次のものが含まれます。

- NAS サーバー情報とログイン情報をセキュリティ保護
- NAS とクライアント デバイスの間のデータ転送をエンド ツー エンドで暗号化
- Web ポータル セッション用の信頼できる証明書
- 高セキュリティのデータ センター

NAS 用の統合された、高セキュリティの Web 管理サービスを提供することで、Synology は、小規模企業に世界規模の接続を実現するための、使いやすさと強力を両立させたソリューションを消費者と SMB に提供しています。大企業のような IT リソースを必要としません。

QuickConnect の仕組み

QuickConnect は、大きく分けて次の 3 つのサービスを提供します。モバイル/PC クライアントユーティリティ、接続とポート転送を簡単にこれ 1 か所で構成できる QuickConnect Web ポータル、そして DSM ファイル共有です。これらのサービスはいずれも、QuickConnect が効率的な接続を保証する必要があります。QuickConnect は、QuickConnect 接続手順を完了しても接続先 NAS と接続できなかった場合、その接続を Synology Cloud Services 経由でルーティングします。QuickConnect の仕組みについては後ほど詳しく説明します。

単一の Web ポータルで接続性が向上

QuickConnect Web ポータルは、ユーザーに単一の便利な Web アドレスを提供します。ユーザーは、これを使用して NAS に簡単にアクセスできるほか、ポート転送を有効にして効率的な接続を確保することもできます。Synology Cloud Services 経由の接続にルーティングし直す場合も、QuickConnect リレー サービスに頼る必要はありません。消費者はポート転送の構成を望まないことがあります。小規模企業の場合、QuickConnect Web ポータルでのポート転送を有効にして、より高速に接続することは最も効率の良い方法です。QuickConnect リレー サービスは、すべての接続試行が失敗した場合の最終的な頼みの綱です。接続先 NAS への接続には時間がかかることがあります。一部の消費者はやはり設定をせずに接続できるリレー サービスを好みます。

QuickConnect 接続手順

QuickConnect は、ユーザーの QuickConnect ID を使用して、クライアント Web ポータルから接続先 NAS への一連の接続試行を実行します。接続手順では、まず、LAN 検出と WAN 検出を実行して、QuickConnect サーバーに登録済みのネットワークアドレスでサーバーにアクセスできるかどうかを確認し、続いて、Synology NAS の存在する環境の、ホールパンチングの互換性をテストし、最後に、これらの方法でアクセスできなかった NAS があれば、リレー サービスを提供します。

LAN/WAN 検出

クライアントが Synology NAS に、サーバーの QuickConnect ID を使用してアクセスを試行すると、その NAS の登録済み情報を求めるリクエストが Synology QuickConnect サーバーに送信されます。これにより、クライアントはサーバーに関するネットワーク情報を取得して、サーバーに接続できる方法を特定できます。この情報には、パブリック IP、LAN IP、NAT タイプが含まれます。どれもリンクに必要ですが、NAS のセキュリティを低下させるわけではありません。与えられた情報で、クライアントは、その IP アドレスまたはドメイン アドレスとの直接接続を LAN ないし WAN 経由で確立できるかどうかを特定できません。

QuickConnect ホールパンチング

確立できる直接接続がない場合、クライアントは、データ転送用の一時的な直接リンクを可能にする、QuickConnect 経由でのクライアント - NAS 間の仮想トンネルの構築を試行します。このテクノロジーによって得られるサーバー - クライアント間のインターネット同期性能は、WAN IP/DDNS の物理環境なしでありながら、そのような環境ありで接続した場合に非常に近くなります。

ホールパンチングは、QuickConnect サーバーの助けを借りてクライアントから NAS への仮想トンネルを開始するという形で機能します。

1. NAS は、QuickConnect サーバーにリクエストを送出し、ホール、つまり、NAS の前にある NAT へのリクエストによってパンチングされたランダムな外部ポートを開放したままにして、ホールパンチングリクエストを受信します。
2. 同様に、クライアントは、リクエストを QuickConnect サーバーに送出して、クライアントの前にある NAT に別のホールを作成します。
3. QuickConnect サーバーは、NAS のホール情報をクライアントに、クライアントのホール情報を NAS に、それぞれ配信します。
4. NAS は、クライアント側のパンチングされたホール経由でクライアントとの接続の確立を試みます。
5. クライアントは、ホールパンチングリクエストを NAS から受信すると、ホールパンチング応答が NAS に、NAS 側のパンチングされたホール経由で返信されます。

6. ホールパンチング応答が NAS に到着すると、仮想トンネルが正常に作成されます。

QuickConnect リレー サービス

仮想トンネルが正常に構築されると、リモートクライアントはこの接続を使用して NAS と直接通信でき、ネットワークリレーは不要です。

仮想トンネルを作成できなかった場合、データ転送にはリレーサービスを利用できます。トラフィックは、リレーされる場合、Synology リレーサーバーを経由してから接続先に到着します。直接接続や QuickConnect ホールパンチングに比べれば時間はかかりますが、QuickConnect リレーサービスは、NAS とクライアントの間でデータをやり取りするための最終的なオプションとして機能します。

ホールパンチングで接続を作成できなかった場合、クライアントは最後に、QuickConnect リレーサービスを使用して仮想ネットワークトンネルを作成して、接続を 1 回試行します。このサービスは、次のように機能します。

1. リレーサービスを開始するために、クライアントが QuickConnect サーバーにリクエストを送信します。
2. QuickConnect サーバーが NAS に対して、NAS とリレーサーバーとの間に仮想トンネルを作成するように通知します。
3. リレーサーバーでポートが割り当てられ、このポートへの全ネットワークトラフィックが、NAS への構築された仮想トンネル経由でリダイレクトされます。
4. リレーサーバーの準備が整ったら、QuickConnect サーバーがその情報をクライアントにリレーします。
5. これで、クライアントがリレーを経由して NAS と通信できるようになりました。

リレーサーバー経由の通信は、データ配信に著しい遅延が生じることがあるため、クライアントがサーバーへのアクセスを試行するうえでの最後の手段となっています。

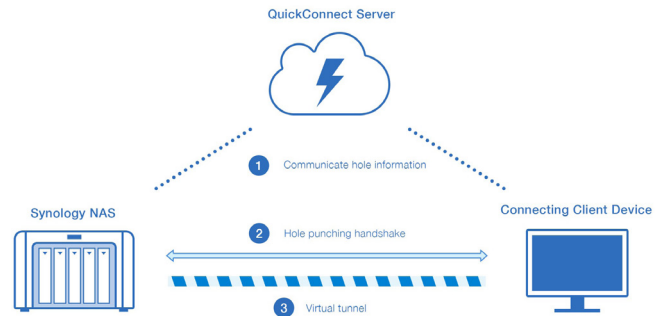


図 1： QuickConnect ホールパンチングの仕組み

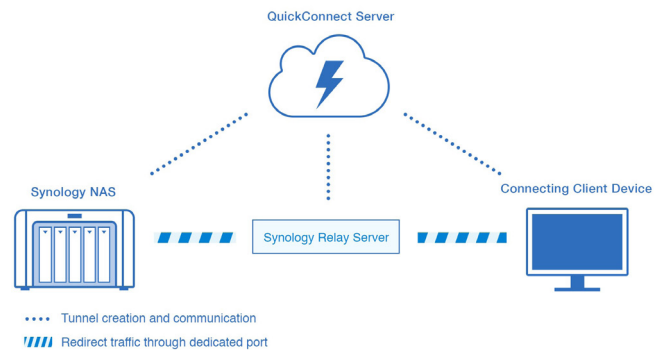


図 2： QuickConnect リレー サービス

QuickConnect サービス

Synology では、QuickConnect を各 Synology アプリケーション (モバイル /PC クライアント ユーティリティ アクセス、QuickConnect Web ポータル、DSM ファイル共有) 向けにカスタマイズしています。これらのアプリケーションは、QuickConnect のさまざまな長所を活かして、同じ利便性と効率を実現しています。

モバイル /PC ユーティリティ

QuickConnect を使用することで、Synology Drive など Synology クライアント ソフトウェアや、DS file などモバイル アプリケーションが、IP アドレスや DDNS の代わりに QuickConnect ID を使用して Synology NAS にアクセスできるようになります。この実現のため、QuickConnect は、クライアントの PC またはモバイル デバイスが、LAN、WAN、ホール パンチングを利用して、またはこれらのいずれも利用できない場合は Synology のリレー サービスを通じて、NAS にアクセスできるようにします。

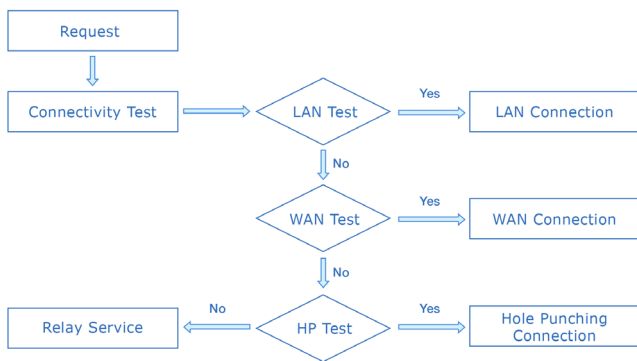


図 3 : QuickConnect を経由したモバイル /PC ユーティリティ アクセスのワークフロー

QuickConnect Web ポータル

QuickConnect Web ポータルを使用することで、DSM 管理インターフェイス、Photo Station、各種アプリケーション ポータルなど、Synology NAS の Web インターフェイスに、ブックマークできる一貫したアドレスを使用してどこからでもブラウザでアクセスできます。

QuickConnect Web ポータルを使用する DSM 管理インターフェイスの典型的なアドレスは、次のようになります。

quickconnect.to/[QuickConnect ID]

例: quickconnect.to/tenni

Photo Station アドレスは次のようになります。

quickconnect.to/[QuickConnect ID]/photo

例: quickconnect.to/tenni/photo

DSM アプリケーション ポータルに QuickConnect アドレスでアクセス

するには、アプリケーションの別名が必要です。File Station のアプリケーション ポータルの典型的なアドレスは、次のようになります。

quickconnect.to/[QuickConnect ID]/[別名]

例: quickconnect.to/tenni/file

これらのアドレスはユニバーサルです。QuickConnect サーバーは、これらのアドレスへのリクエストを受信すると、QuickConnect 接続手順を開始して、NAS の場所とアクセス可能かどうかを確認します。QuickConnect がブラウザのリダイレクト先の LAN または WAN アドレスを特定できなかった場合は、Synology が、Synology NAS と接続元 Web ブラウザの間のプロキシとして機能する QuickConnect ポータル サーバーを用意します。

QuickConnect 接続手順がブラウザのリダイレクトを補助し、開きたい Web ページへの最善のパスを確立します。例えば、ポータル サーバーは、クライアントのブラウザを LAN アドレス (例: http://192.168.17.99:5000/) や WAN アドレス (例: http://tenni.synology.me:5000) にリダイレクトします (これらのアドレスがアクセス可能な場合)。

接続元クライアントが、これらの Web インターフェイスに HTTPS (例: https://quickconnect.to/tenni) を使用して接続しようとしている場合、NAS サーバーの証明書 (個人向け NAS では多くの場合、自己署名済み) を信頼するよう求められます。ブラウザが LAN アドレスにリダイレクトされるのは、クライアントが証明書を信頼することを選択した場合のみです。信頼しないことを選択した場合、代わりにリレーポータルが有効化され、すべての転送データがリレーされます。

次の図は、QuickConnect Web ポータルで採用されているプロセスを示しています。

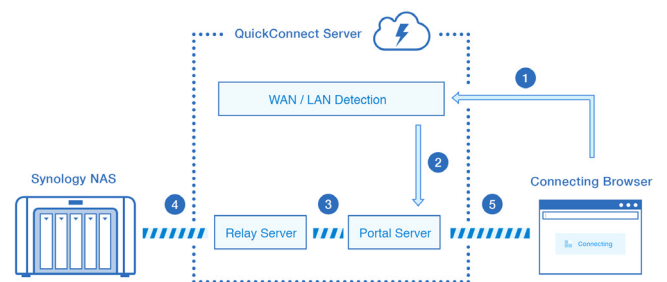


図 4 : QuickConnect Web ポータル

1. クライアントが QuickConnect 接続手順を実行します。
2. LAN/WAN 接続手順の結果が失敗である場合、ブラウザがポータルサーバーにリダイレクトされます。
3. ポータルサーバーが、リレーサーバーから NAS への仮想ネットワークトンネルを起動します。
4. ポータルサーバーが、プロキシの役割を果たして、NAS とクライアントブラウザとの間の全トラフィックを仮想ネットワークトンネル経由

で処理します。

- これで、クライアント ブラウザが、所期の NAS Web ページにポータルサーバー経由でアクセスできるようになりました。

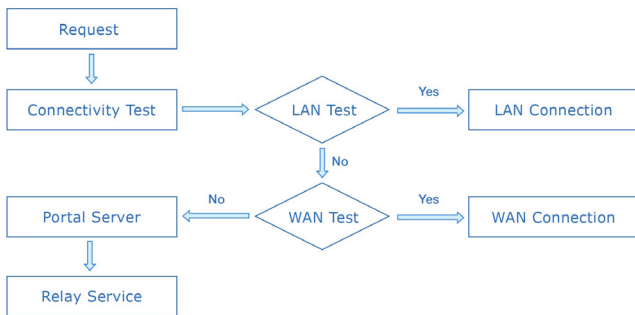


図 5 : QuickConnect Web ポータルのワークフロー

QuickConnect Web ポータルのメリットは、次のようにまとめられます。

- QuickConnect 接続手順により、効率的な接続が保証されます。
- Web ポータルは、Web ブラウジングにファイアウォールに親切的な標準的なポートを使用します。
- ブックマークできる永続的な URL が用意されます。

QuickConnect を経由したファイル共有サービス

ファイル共有は、ファイルを URL で共有できる、ネイティブの DSM サービスです。共有リンクは、次のいずれかの形式を取ります。

<http://gofile.me/2dRzN/lt1zrMTz>

QuickConnect が有効

<http://nnicole.synology.me:5000/fbsharing/ljl5jbs>

DDNS が有効

<http://192.168.17.99:5000/fbsharing/pDWQYwqJ>

リンクは、サーバーの IP アドレスで始まります。

QuickConnect が有効の場合、ファイル共有リンクは常に、gofile.me ドメインの形式を取ります。接続手順としてこのリンクを使用すると、接続元ブラウザは共有ファイルへのアクセスに考えられる最善の経路を取ることができます。言い換えると、クライアント ブラウザは共有リンクに LAN/WAN アドレスがあればそれにリダイレクトされ、リレー トンネルを通じた試行はその後になります。

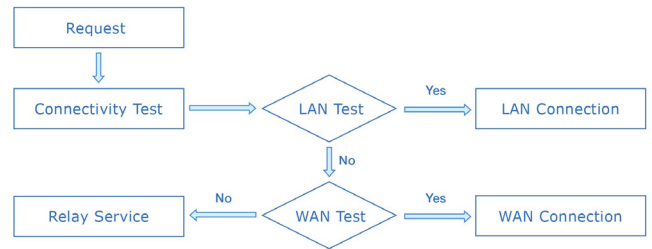


図 6 : QuickConnect を経由したファイル共有のワークフロー

対応サービス

対応サービス / アプリケーションは次のとおりです。

PC ユーティリティとモバイルアプリケーション 1	DSM 内蔵サービス	QuickConnect Web ポータル
Drive PC クライアント	ファイル共有	DiskStation Manager
DS audio	CMS	Photo Station
DS cloud		アプリケーションポータル
DS cam		File Station
DS download		Audio Station
DS file		Download Station
DS finder		Note Station
DS note		Surveillance Station
DS photo		Video Station
DS video		
MailPlus		
Chat		
Moments		

QuickConnect のセキュリティ

QuickConnect は便利な NAS 管理を Web 経由で提供しますが、企業の皆様は非公開データがすべて常時保護されているのでご安心できます。実際、Synology では NAS サーバーデータ、データ転送、Web ポータルはもちろん、Synology QuickConnect サーバーのデータセンターについても、労をいとわずセキュリティに万全を期しています。

Synology NAS に関する情報

QuickConnect サービスを有効にするには、QuickConnect サーバーで Synology NAS が登録されていることが必要です。これは、Synology NAS がネットワーク環境や対応サービスなどのステータスを QuickConnect サーバーに報告することを意味します。

報告された情報（例：パブリック IP アドレス、LAN アドレス、NAT タイプなど）は接続手順に必要です。Synology は、ユーザーのデジタルプライバシーを保護します。取得された情報は、Synology によるのみ、QuickConnect サービスの提供を目的として使用します。

リレー トンネル

SSL が有効な場合、ネットワーク仮想トンネル経由のデータ転送はエンド ツー エンドの暗号化でセキュリティ保護されます。したがって、QuickConnect では Synology NAS- クライアント デバイス間のデータ転送の機密性と整合性が保証されます。

QuickConnect Web ポータル

QuickConnect Web ポータルは、ブラウザが LAN または WAN 接続を使用して Synology NAS にリダイレクトされる場合、エンド ツー エンドの暗号化でセキュリティ保護します。そうでない場合、リクエストはポータル サーバーに転送されます。

このような条件では、ポータル サーバーは、接続元ブラウザがポータル サーバーの身元を確認するための信頼できる証明書を提供します。こうすることで、ポータル サーバーを装うデバイスによるメッセージの傍受が防止され、中間者攻撃の対策となります。

次に、ポータル サーバーは、特定の HTTP ヘッダーを解釈して変更し、接続先 NAS に接続元クライアントの身元を通知します。その後、ポータル サーバーは、データをネットワーク仮想トンネル経由で接続先 Synology NAS に送信します。ここでも、仮想ネットワーク トンネル経由のデータ転送は、SSL が有効な場合、エンド ツー エンドの暗号化でセキュリティ保護されます。



図 7：QuickConnect Web ポータルのセキュリティの仕組み

QuickConnect では、約束されているサービスを提供しますが、そのようなサービスの提供以外で登録済み Synology NAS サーバーから収集したデータを利用することはありません。詳細については、公式 Web サイトの「プライバシーに関する声明」をご覧ください。

施設のセキュリティ

Synology QuickConnect サーバーは、世界で合計 8 か所のデータセンターでホストされており、高品質で安定したサービスを提供しています。すべてのデータセンターは、スタッフが年中無休で常駐しており、監視システムと、個人アクセスを管理する厳格なポリシーで保護されています。また、施設には、停電や防ぎえな災害が発生しても電源とネットワークの可用性を確保できる十分な設備も整っています。

まとめ

企業というものは、規模を問わず大志を抱いています。しかし、大企業のような大きな予算も大がかりな IT リソースもない個人消費者や小規模企業にとって、従業員がどこからでも貴重なデータにアクセスできるようにすることは、ハードルが高くなっています。多くの中小企業が NAS サーバーをプライベート LAN 上に設置しようとしています。インターネット経由でリモート アクセスできるようにするためには多くの場合、さらなる IT 知識が必要となりますし、デバイスや複雑なポート転送ルールを手動で構成しなければなりません。

Synology の QuickConnect を使用すると、どのようなユーザーや企業も、Synology NAS に保存されているデータや QuickConnect Web 管理インターフェイスに、ネットワーク環境を問わずどこからでもアクセスできるようになります。Synology QuickConnect なら、ネットワーク間の接続用に複雑なポート転送やファイアウォール規則を設定する必要がなく、シンプルなパーソナライズされた QuickConnect ID で上記のすべてが可能となり、接続元デバイスをネットワーク上の最短ルートで接続先 NAS まで安全に導きます。

お客様の業務で NAS のメリットを受け始める方法の詳細については、www.synology.com にアクセスするか、次に挙げるリンクをご覧ください。

- Synology eNews を購読して最新の知見を得るには、お客様の Synology アカウントを <https://account.synology.com> にご登録ください。
- 最新の DSM のライブデモを試す場合は、<https://demo.synology.com> にアクセスしてください。



**SYNOLOGY
INC.**

9F, No. 1, Yuan Dong Rd.
Banqiao, New Taipei 22063
Taiwan
電話 : +886 2 2955 1814

**SYNOLOGY
AMERICA CORP.**

3535 Factoria Blvd SE, Suite #200,
Bellevue, WA 98006
USA
電話 : +1 425 818 1587

**SYNOLOGY
UK LTD.**

Unit 5 Danbury Court, Linford Wood,
Milton Keynes, MK14 6PL,
United Kingdom
電話 : +44 0 1908048029

**SYNOLOGY
FRANCE**

102 Terrasse Boieldieu (TOUR W)
92800 Puteaux
France
電話 : +33 147 176288

**SYNOLOGY
GMBH**

Grafenberger Allee 295
40237 Düsseldorf
Deutschland
電話 : +49 211 9666 9666

**SYNOLOGY
SHANGHAI**

200070, Room 201,
No. 511 Tianmu W. Rd., Jingan Dist., Shanghai,
China

**SYNOLOGY
JAPAN 株式会社**

〒 101-0031 東京都
千代田区東神田 3-1-2
ユニゾ東神田三丁目ビル 4F

Synology®



synology.com

Synology では仕様・製品説明を随時予告なく変更する場合があります。Copyright © 2019 Synology Inc. All rights reserved. * Synology および Synology 製品のその他の名称は、Synology Inc. の商標または登録商標です。本書に記載されているその他の製品名および会社名は各所有権利者の商標です。