QNAP × veeam

ホワイトペーパー
Veeam Agent 連携ソリューション





要約

本ホワイトペーパーは、ランサムウェア時代に求められるバックアップの考え方と実践をわかりやすく解説するものです。 従来の「短期保管・復旧前提のバックアップ」では、現在の高度化した攻撃には対応できません。

今後は「長期保管」「不変性（Immutable）」「隔離（AirGap）」「迅速な復旧（Fast Restore）」が不可欠となります。

主なポイントは以下の通りです。

従来の課題

- 短期間しか保持していないバックアップ
- 簡単に削除されてしまうデータ
- 複雑で時間のかかる復旧
- 感染後にアクセスできない保存先

これから必要な機能

- 容量を効率的に使った長期保存
- 情報漏えいを防ぐ暗号化
- 管理者でも削除できない不変性（Immutable）
- 誰でもすぐ行える簡単な復旧手順

最終目標

「消せない・感染しない・すぐ戻せる」バックアップを実現することで、事業を止めない強靭な体制をつくることです。

01 ランサムウェア時代に必要となるバックアップ

これまでバックアップといえば、次のような目的で行われてきました。

- 操作ミスによるファイル削除への備え
- システム更新や改修によるトラブルからの復旧
- 災害時に事業を継続するための冗長性（BCP：Business Continuity Plan）

これらのケースでは、数日から1週間程度のバックアップを保持していれば十分とされていました。 しかし、ランサムウェアの時代においては、少なくとも3 0日以上のバックアップ保管が必要です。

なぜなら、ランサムウェアは即座にシステムを暗号化するわけではなく、侵入から数週間〜1か月以上潜伏して拡散するケースが多いためです。 感染を検知した時点では、過去のバックアップもすでに汚染されている可能性があります。

その結果、復旧に1か月以上かかる事例も増えており、システム停止が長引くことで以下のような深刻な被害が発生します。

- 業務の中断による売上減少
- 顧客や取引先への影響
- 社会的信用の失墜

これらの被害が起きてしまう主な原因

■ 長期のバックアップを取っていない

ランサムウェアの潜伏期間は30〜40日（金融機関や医療機関ではさらに長期）といわれています。 そのため、7日分のバックアップしかない場合、攻撃が発覚した時にはすべての世代が感染済みでリストア不能となります。

■ バックアップデータが破壊または削除される

攻撃者は、バックアップの存在を前提に攻撃を行います。 バックアップサーバに同一ネットワークからアクセスできると、攻撃者は容易に侵入し、バックアップを削除してしまいます。 実際、攻撃の初期段階で「最初に狙われるのはバックアップ」です。

■ バックアップデータがあっても使えない

感染が確認されると、調査のためにネットワークやストレージを遮断することが多く、安全なバックアップが内部に残っていても、データセンターの封鎖中は物理的に取り出せなくなります。 このため、「3 -2-1ルール（3つのコピー・2種類のメディア・1つはオフサイト）」が重要ですが、「1つのオフサイト」が実践されていないケースが多く見受けられます。

また、オフサイトにバックアップを取ってあったとしても、早期に復旧を目指す場合、復旧先は別の環境となることがほとんどで別のハードウェア基盤やクラウド環境を用意する必要があります。したがって、確保したリソースに対してリストアが可能かどうかが鍵となります。もし、取得したバックアップがリストアに使えないとなると、バックアップなしで初めからの再構築となってしまいます。

■ リストアが複雑すぎて実行できない

バックアップの目的が「保存」になっており、「復旧」が考慮されていないケースがあります。

- リストアの手順が煩雑で、担当者が実行できない
- 復旧リハーサル（演習）が行われていない
- テープメディアなどで安全と思しきデータを探すのに時間がかかる
- システム全体ではなくデータのみのバックアップで、OSや設定を再構築しないと動かない。

多くの組織がランサムウェア攻撃を受けても、依然として復旧に時間がかかっています。これは、バックアップが「保存の手段」にとどまり、「復旧の手段」として機能していないためです。特に大規模な環境では構成が複雑化しており、復旧作業が困難になっています。

そのため、今こそ原点に立ち返り、シンプルな構成と容易な復旧方法を重視する必要があります。従来型のバックアップでは、ランサムウェア時代において「バックアップを取っていても復旧できない」という致命的な課題が残っています。

しかし、実際にランサムウェア攻撃の被害者になったとしても、対応ができなくても当然であり、今の時点で極度に心配する必要はありません。　大切なのは、常に最新の情報を仕入れ、実際にランサムウェア攻撃を受けた場合を想像して運用をアップデートし続けることです。 むしろ、ランサムウェア攻撃を日頃から想定し、定期的に準備点検を行うことこそが、最も現実的で効果的な対策となります。

02 バックアップ環境に最低限必要な機能

1.容量を効率的に使いながら長期保管できること

ランサムウェア対策として最低でも30～40日のバックアップを保持するには、ストレージの容量が大きくなります。 したがって、重複排除（重複データをまとめる技術）やブロック単位の増分バックアップなどを活用し、 データ量を抑えながら効率的に保存する仕組みが必要となります。さらに取得時間やネットワーク負荷も軽減できます。

2.バックアップデータを暗号化しておくこと

暗号化はランサムウェア感染の直接防止策ではありませんが、万一バックアップデータが盗まれても、 暗号化されていれば機密情報の漏えい（二重脅迫）を防ぐことができます。暗号化していたおかげで情報流出を防げた医療機関が実際にあります。 ただし、暗号鍵やパスフレーズはバックアップと同じ場所に置かないことが重要です。

3.バックアップデータを削除・改ざんできないこと

ランサムウェア攻撃の最初の標的はバックアップです。 そのため、管理者であっても削除できない領域にデータを保存する必要があります。 その代表的な仕組みが以下の2つです。

- Immutable（不変性） 一定期間、データを変更･削除できないように保護する仕組みです。 WORM（追記型）メディアのように永続保存ではなく、指定期間のみ上書き禁止とします。 保管期間が過ぎれば自動削除されるため、柔軟な運用が可能となります。
- AirGap（隔離） ネットワークから切り離した場所にバックアップを保存する手法です。 物理的または論理的に接続が遮断されるため、攻撃者は到達できません。 オフライン保存やクラウド･オフサイトへの転送もAirGapの一種です。

4.簡単に、すぐリストアできること

バックアップが複雑すぎると、復旧（リストア）に時間がかかり、事業再開が遅れてしまいます。 仮想マシンや物理サーバを丸ごとバックアップする方式を採用すれば、ワンクリックで全体を戻すことも可能です。また、ランサムウェア被害時には「どのバックアップが安全か」を見極める必要がありますが、テープのように視認性が低い媒体では中身を確認するために都度リストアを繰り返す必要があり、復旧が大幅に遅れます。データ復旧にかかる時間だけでなく、システム全体の稼働再開までの時間（RTO：復旧目標時間）を短縮でき、取得した環境と別の環境やパブリッククラウドへリストアができる手段があることも重要となってきます。



03 Veeamを使ったバックアップ

近年のバックアップソフトウェアの中でも、ランサムウェア対策において高い信頼性を持つ製品の一つが Veeam社製のバックアップソリューションです。 Veeamは「VMware仮想環境専用のバックアップ製品」という印象を持たれることが多いですが、実際には物理環境･クラウド環境･仮想環境を横断して対応できる総合バックアップ製品です。また、Veeam製品で取ったバックアップファイル形式は製品によらず共通で、取得したバックアップを別の仮想基盤やパブリッククラウドへリストアができるため、ランサムウェアからの復旧に対して様々な手段をとることができます。

Veeam製品の種類と特徴

Veeamには環境に応じて使い分けられる2つの主要製品があります。

- Veeam Backup & Replication（仮想環境向け） 仮想マシンを「エージェントレス（専用ソフト不要）」でバックアップ VMware、Hyper-V、KVM（Nutanix AHV、Oracle Virtualization、Proxmoxなど）など主要な仮想化基盤をサポートしています。 また、AWS･Azure･GCPなどのクラウド環境や、NAS／ファイルサーバのバックアップにも対応しており、 物理サーバ用のVeeam Agentを集中管理することも可能です。
- Veeam Agent（物理環境向け） 物理サーバやスタンドアロンPC、ノートPCなどを対象としたエージェントベースのバックアップ Windows、Linux、macOSに対応し、物理マシンだけではなく、仮想マシンにインストールして利用することもできます。

バックアップ方式

どちらの製品もホストに対してはイメージバックアップ方式を採用しています。 初回はシステム全体を丸ごとバックアップし、2回目以降は変更されたブロックのみを増分バックアップします。 この方式により、

- バックアップ時間の短縮
- ストレージ容量の削減 が可能となります。

また、復元（リストア）はシステム全体だけでなく、ドライブ単位や必要なファイル単位での復旧も可能です。

バックアップデータの保存先

Veeamのバックアップデータは、以下のような複数の保存先に柔軟に対応しています。

- 内蔵ディスクまたはディスクアレイ
- ネットワーク共有（SMB／NFS／iSCSI）
- クラウドストレージやS3互換のオブジェクトストレージ

既存のインフラを活用しながら、コストを抑えた柔軟なバックアップ構成を設計することができます。

バックアップデータは、Veeam AgentのバックアップデータをVeeam Backup＆ Replicationでも扱うことができます。

主なランサムウェア対策機能

Veeamは単なるバックアップ製品ではなく、ランサムウェア被害を想定した保護機能を備えています。イミュータブル以外の機能は、Veeam Backup ＆ Replicationサーバが必要となります。

以下の機能は、Veeam Backup & Replicationのみ搭載されています。

- Immutable（不変性バックアップ） LinuxのxfsファイルシステムやS3互換オブジェクトストレージなどを用いることで、 一定期間データを削除･改変できない「不変性（Immutable）」を付与できます。 管理者であっても期間中は削除できないため、バックアップの破壊を防げます。
- インラインスキャン バックアップ中に暗号化ファイルの兆候をリアルタイムで検知し、感染拡大を早期に防ぎます。
- スキャンバックアップ（アンチウイルス連携） 既存のバックアップデータをスキャンし、マルウェアが混入していないかを後から確認できます。

04 QNAP NASとの親和性

QNAP NASは、Veeamのバックアップデータを保存する最適なストレージ基盤として利用できます。
以下のように複数の接続方式に対応しています。

通常のストレージ

- SAMBA（Windows共有）
- NFS（Linux共有）

イミュータブルストレージ

- iSCSI（ブロックストレージ Veeam Backup & ReplicationのLinux強化レポジトリ）
- オブジェクトストレージ（QuObjects）

これにより、企業規模や既存のネットワーク構成に合わせた最適な方式を選択できます。

QNAPとVeeamを用いた代表的な構成

QNAPとVeeamを組み合わせた構成は、大きく分けて次の2パターンがあります。

1 バックアップサーバ（Veeam Backup & Replication）を利用する構成

特徴

- OSに依存せずに複数台の仮想マシンをエージェント レスでバックアップ可能
- 大規模構成や集中管理を行いたい環境に最適
- バックアップジョブやスケジュールは、Veeamサーバ側で一元管理

QNAPとの連携

- QNAP Virtualization Station上に、Veeamが必要とするリポジトリ用Linuxサーバやプロキシなどのコンポーネントを構築できます。
- QNAP側のQuObjects（S3互換）をバックアップ先とし、イミュータブル機能で「削除できない」データ保護を実現。
- あるいはiSCSI＋Linux XFS構成により、不変性（Immutable）を持つバックアップをQNAP NAS上で構築可能。

2 各サーバにVeeam Agentを導入する構成

特徴

- 物理サーバや中小規模システムで手軽に導入できます。
- Windows／Linux環境のどちらにも対応。
- 各エージェントが自律的にバックアップジョブを実行。

QNAPとの連携

- QNAP側のQuObjects（S3互換）をバックアップ先とし、イミュータブル機能で「削除できない」データ保護を実現。
- QTS hero（ZFSベースOS）では、最大30日保持できる「Immutable Snapshot」を活用可能。 → Veeam Agent単体構成でも「消せないバックアップ」を実現できます。
- QNAP QHoraルータを組み合わせることで、ネットワークを分離した物理的AirGap（隔離）構成を構築可能。

まとめ：Veeam AgentとQNAP NASを合わせることで強固な防御を実現

Veeam Agent構成では、Veeam本体の高度なランサムウェア対策機能と連携できませんが、 QNAPの「QuObjects」、「Immutable Snapshot」と「AirGap構成」を組み合わせることで、 管理者でも削除できない＋外部からアクセスできないバックアップを構築できます。

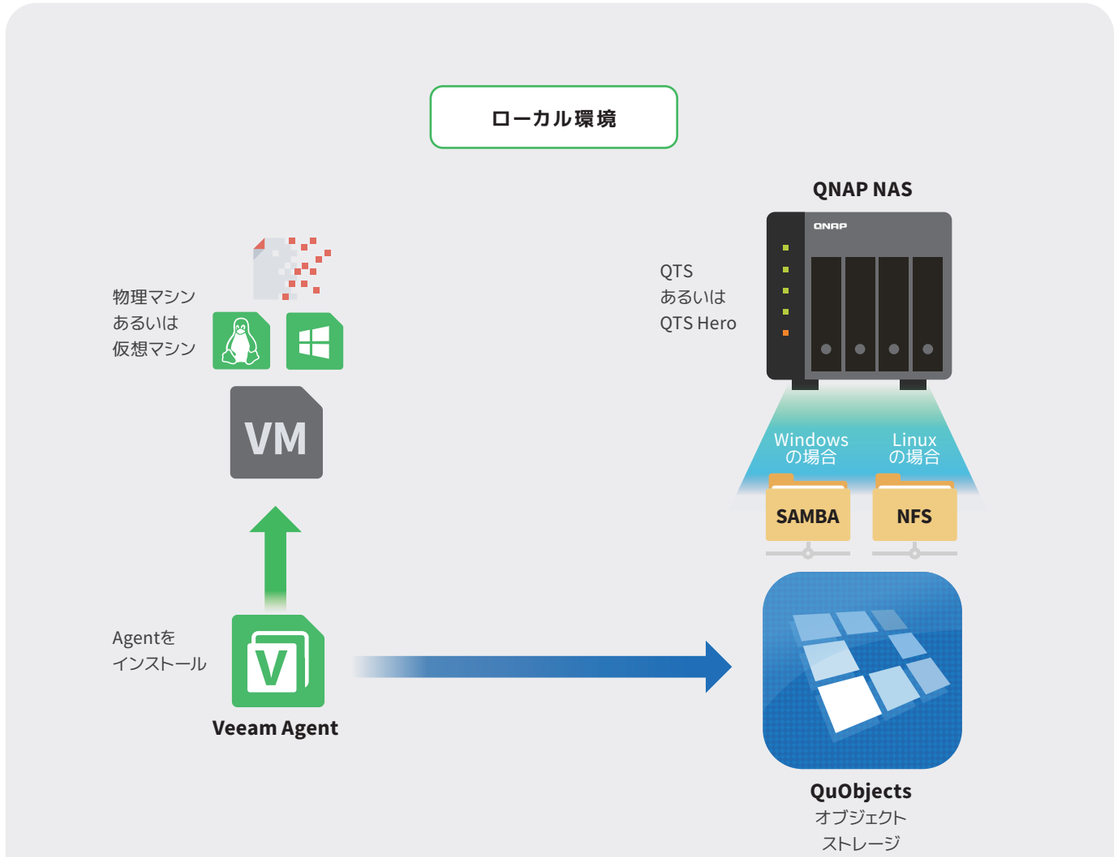


05 QNAPとVeeam Agent を用いた構成

ローカル環境構成

QNAPNASを使えば、Veeam Agentから簡単にバックアップを保存できます。

- Windows環境：SAMBA共有をバックアップ先に指定
- Linux環境：NFS共有をバックアップ先に指定
- QNAP QuObjects（オブジェクトストレージ）をバックアップ先に指定



イミュータブル構成（不変性付きバックアップ）

不変性を確保したい場合は、以下の2つのアプローチを取ることができます。

- オブジェクトストレージ QuObjectsのObject Lock
- Immutable Snapshot機能

必要とするストレージ容量は2つとも大体同じですが、例えば30日保存した場合、イミュータブル構成の場合は、通常のバックアップの30日分以上の容量が必要となることに注意してください。また、それぞれに特徴と制限が存在します。

1 オブジェクトストレージ QuObjectsのObject Lock (QTS/QTS Heroの両方で利用可能)

メリット

- 不変性の日数は、30日以上長期間取ることができます。
- 不変性の管理をVeeamで行います。

デメリット

オブジェクトストレージへのアクセスは、CPU/メモリを多く消費し、ファイル共有へのバックアップと比較すると処理が遅くなります。

2 Immutable Snapshot機能 (QTS heroのみで利用可能)

メリット

- バックアップのパフォーマンスが良好です。
- 不変性の管理をQNAP側で行います。

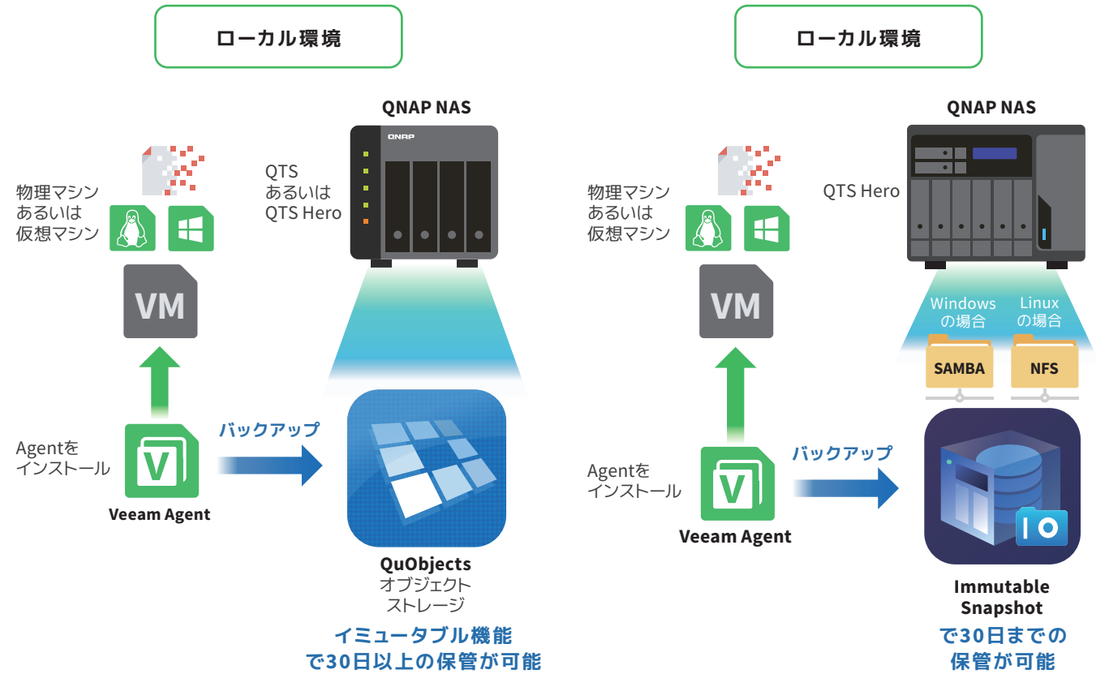
デメリット

- 不変性の日数は最大30日までしか指定できません。

不変性を確保する場合、QuObjectあるいはSAMBAでのバックアップで、Immutable Snapshot機能（ただし、保存期間を30日まで）を使います。

ランサムウェア攻撃後の復旧時には、Veeam Agentのベアメタルリストア（全損時の空のマシンから復旧）を行えば、システム全体を迅速に復旧できます。

- QuObjectsの場合：Veeam AgentのUIから「感染前の日付」を選択してリストア
- Immutable Snapshotの場合：一覧から「感染前の日付」を選択して、バックアップされていた共有を一時的にマウントしてリストア

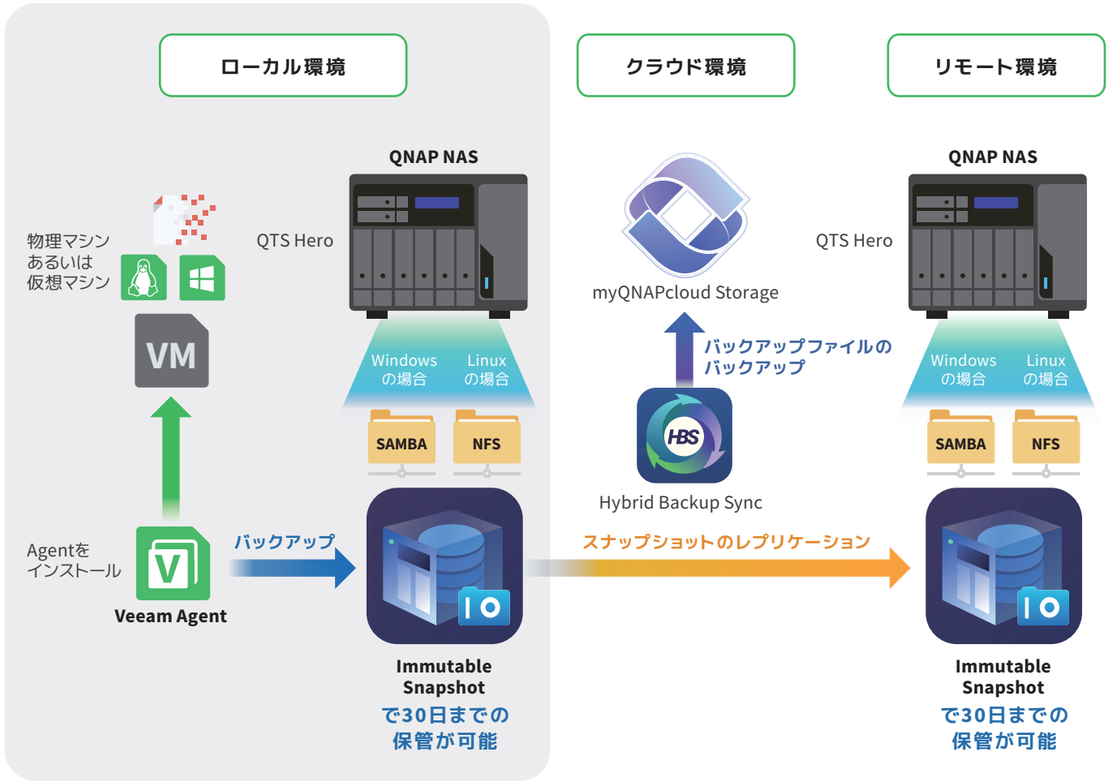


オフサイト保存（遠隔地保管やクラウド保管）

ランサムウェア感染時の落とし穴は、「安全なバックアップがあっても封鎖された環境内にある」という点です。　フォレンジック（原因調査）や再感染防止のためにローカルネットワークが隔離されると、バックアップデータがたとえ安全だったとしても利用できなくなります。

そのため、オフサイト（遠隔地）へのバックアップ転送が重要です。 QNAP NASは、リモートNAS間でバックアップを複製（同期）できるため、ローカルが感染しても、リモート側から復旧環境を構築できます。さらにVeeamでバックアップを取得していれば、元の環境と同じプラットフォームだけではなく、Veeamがサポートしている仮想化プラットフォームあるいは、パブリッククラウド環境にリストアして構築ができます。ランサムウェア攻撃からの復旧で一番ネックとなる復旧先の基盤の選択肢を広げ、早期にリストアすることが可能になります。

また、Hybrid Backup Syncは、myQNAPcloud Storageやクラウド上のオブジェクトストレージへの保管にも対応しているため、QNAP NASが用意できない場合でもバックアップデータだけは少なくともリモート保管ができます。



リモート転送を行う場合は、転送に必要となるネットワーク帯域がバックアップデータの転送に間に合うのか事前に確認をしておくことをお勧めします。

パブリッククラウドにバックアップデータ保管を行う場合は、パブリッククラウドの通信経路やアクセスセキュリティに十分注意を払う必要があります。クラウドのセキュリティ設定に不慣れな場合は、myQNAPCloud Storageを使うことで安全にクラウドストレージを利用することが可能となります。

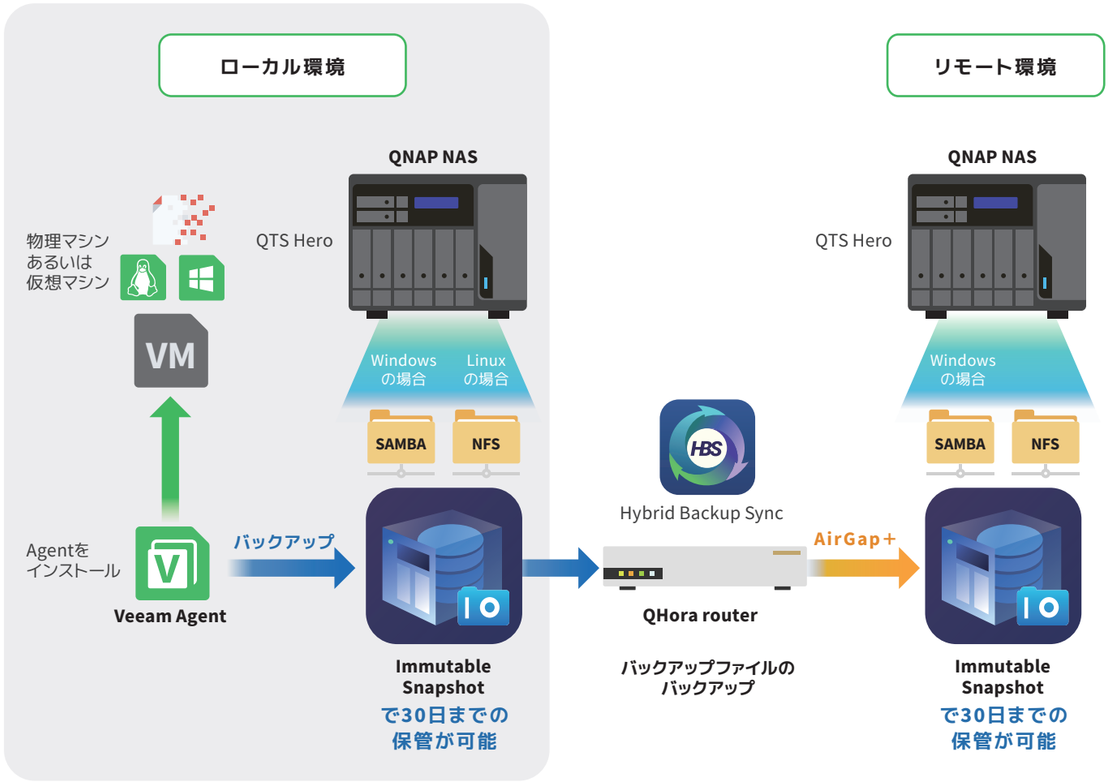
オフサイト＋AirGap構成（最高レベルの防御）

VeeamはSAMBA共有やNFS共有にバックアップを保存する場合、ドライブを常時マウントせず、バックアップ時のみプロトコルを開くため、セキュリティ的には比較的安全です。しかし、バックアップ環境そのものが攻撃される可能性もあるため、より強固な防御を実現するには、QHoraルータのAirGap+機能とHybrid Backup Sync（HBS）を組み合わせた構成が有効です。

この構成では、ネットワーク的にも物理的にもバックアップデータを隔離し、感染経路を完全に断ち切ることができます。 ネットワークを完全に遮断するAirGap構成は、論理的隔離では防げない攻撃をも遮断できる“最後の防衛線”となります。

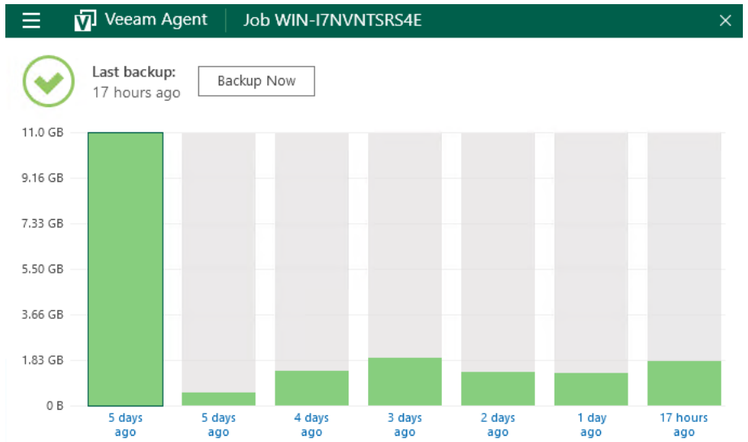
物理的なAirGap機構を備えるソリューションは多くなく、一般的には複数のソフトウェアを連携させる大企業向けの高額な構成となります。一方で、AirGap+はQNAP単体で実現できるシンプルな仕組みであり、他社ソリューションと比較しても圧倒的に安価に導入できます。

一見すると、Veeamのバックアップデータを再び別のバックアップソフト（HBS）でコピーするのは不思議に思えますが、Veeamのバックアップデータはフォルダ単位で移動・再配置しても復元可能という特性を利用しています。 この柔軟性を活かすことで、「Veeamでバックアップ → QNAPで隔離・保護 → 必要時に安全な場所で復旧」という多層防御型のバックアップ体制を実現できます。



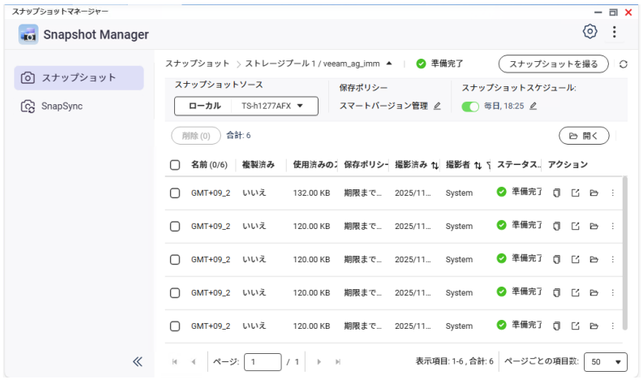


06 QNAPとVeeam Agentを用いた動作例



Veeam Agentは、OSホストのバックアップをQNAP NASの共有あるいは、オブジェクトストレージ QuObjectsに保存をするというシンプルな動きをします。

以下の例は、Veeam Agentのバックアップをを SAMBA共有に保存をし、Immutable Snapshotで保存をしている環境です。



このように、主にVeeam Agentでは、OSホストのバックアップ、QNAP NASでは、イミュータブルやAirGAPをするという分担で行うことになります。役割が分かれているという点でも、疎結合で動作できるので、セキュリティ的には侵入、攻撃されにくいというメリットがあります。

07 まとめ

近年のバックアップは、単なる操作ミスや災害対策にとどまらず、ランサムウェア対策としての長期・不変・隔離型の保護が求められています。従来の「数日〜1週間分のバックアップ」では、侵入後に潜伏し拡散する攻撃には対応できません。感染検知の時点で過去のバックアップまで汚染されている可能性があり、少なくとも30日以上の安全なバックアップ保持が不可欠です。

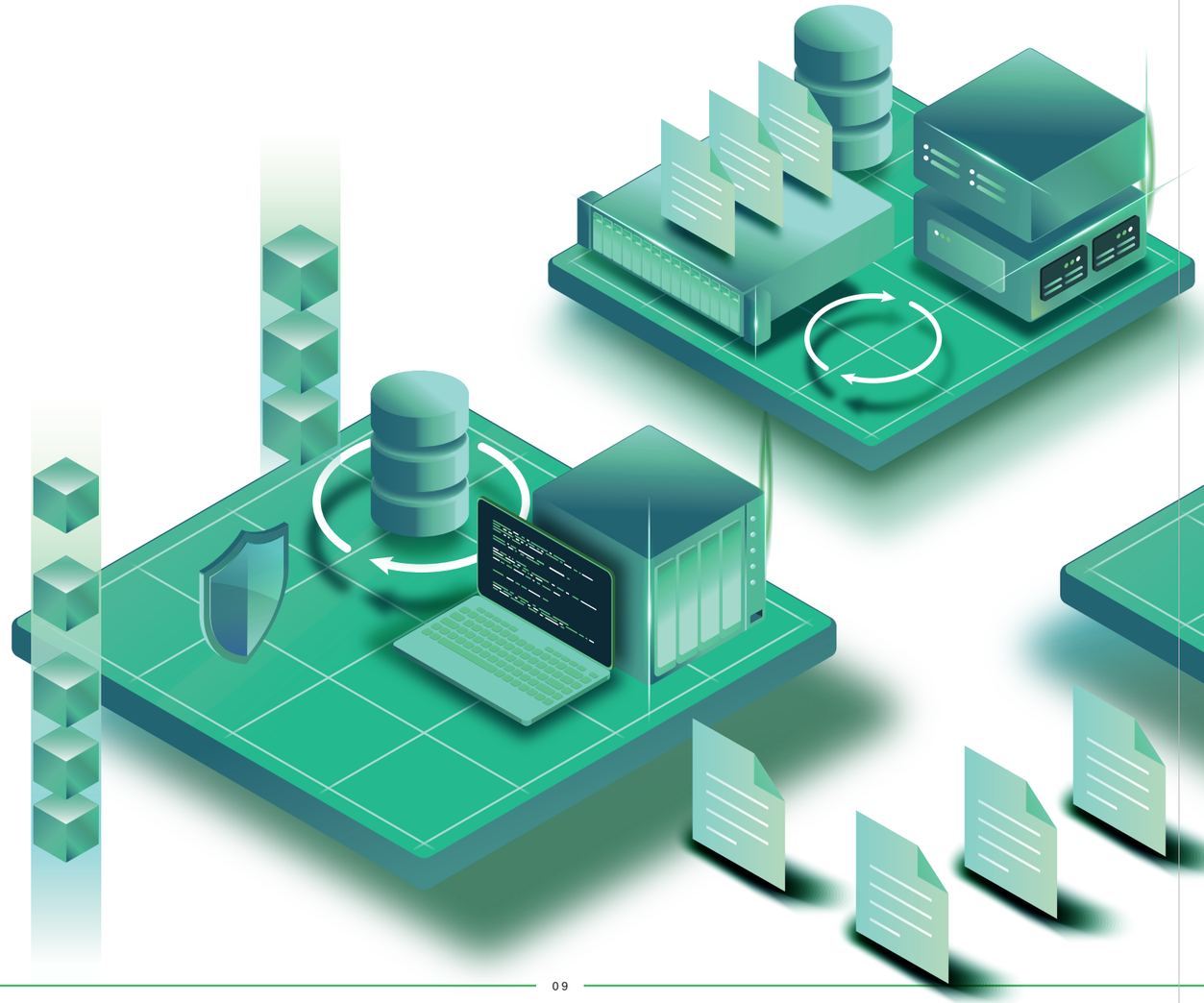
この背景のもと、Veeam AgentとQNAP NASの組み合わせは、実用的かつ導入しやすいランサムウェア対策の解として有効です。

Veeam Agentにより、物理・仮想環境を問わず各端末のデータを柔軟に取得可能

QNAP NASのオブジェクトストレージやスナップショットのイミュータブル機能により、攻撃後でも安全な復旧点を確保可能

複雑なバックアップサーバ構成を構築しなくても、QNAP NASと簡単に使えるVeeam Agentとそのライセンスだけで包括的な保護環境を実現できるのが大きな利点です。

ランサムウェア攻撃は予告なく発生し、復旧までに1か月以上を要するケースも増えています。 被害を受けてから備えるのでは遅く、今すぐに体制を整えることが事業継続を守る唯一の確実な手段です。



ホワイトペーパー
Veeam Agent 連携
ソリューション



お問い合わせ
QNAP株式会社
〒116-0013 東京都荒川区西日暮里 2-20-1 ステーションポートタワー6F

QNAPはいつでも、事前の通知なしに仕様と製品詳細を変更することができます。
QNAPおよびその他QNAP製品の名称はQNAP Systems, Inc.の登録商標です。
本書に記載されているその他の製品と社名は各所有者の商標です。

