

# エアギャップバックアップでより 安全なランサムウェア対策を実現！

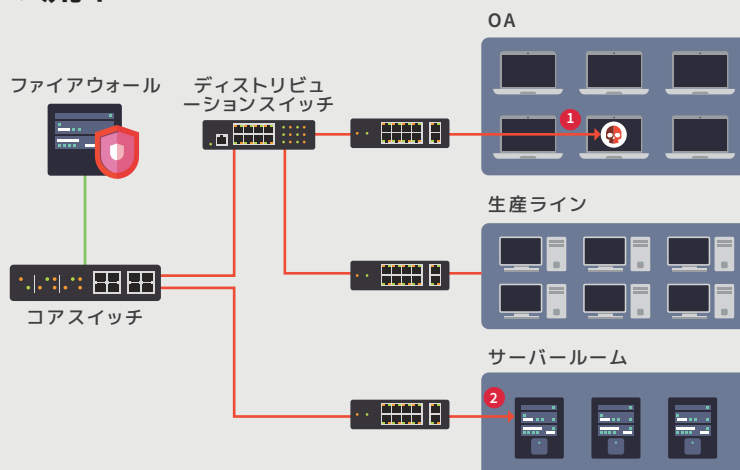
万が一ランサムウェア被害にあったしまった場合、メイン機のデータが暗号化されることで気づき、バックアップから復旧することになります。その時にバックアップデータも暗号化されてしまっていると、データを復旧できませんので、バックアップデータは安全なエアギャップ領域に保管する必要があります。QNAPでは様々なエアギャップソリューションをご用意し、お客様が安全にバックアップデータを保管することをサポートします。

## ランサムウェアによる被害発生の流れ

ランサムウェアはセキュリティが緩い端末に、社員宛のメールの添付ファイルを開いてしまったり、持ち込んだUSBディスクを接続することで、社内に侵入します。

一度社内に侵入すると、ネットワークを通じて他のより権限の高い端末、ファイルサーバーやMESシステムなどへのアクセスを試みます。

→大切なデータは  
“ネットワーク経由でアクセスできない状態”  
＝“エアギャップ状態”にすることが重要です！



## ランサムウェア対策で大切なポイントとは？

### エア ギャップ(Air Gap)

物理的に隔離されたエリア



- ・オフラインのテープ
- ・サーバー・アクセスから完全分離された隔離エリア

ランサムウェアはネットワークに接続されているデバイスにしかアクセスができないため、“**ネットワークから切り離して保存する**”ことがランサムウェア対策として非常に効果的です。

ネットワークから切り離してバックアップデータを保管することを、“**エアギャップを作る**”、“**エアギャップバックアップ**”といいます。

ネットワークから切り離すことで、“**ランサムウェアは装置やデータを発見することができず、その装置上のデータを暗号化することもできなくなる**”ため、非常に安全になります。

## QNAPのエアギャップバックアップソリューション

QNAPではお客様の要件に合わせて、3種類のエアギャップバックアップソリューションをご提供しています。データの重要度や、予算に合わせて、最適なエアギャップソリューションをご利用いただくことが可能です。

# QNAPのNASで利用できるエアギャップバックアップソリューション

## USB エアギャップバックアップ

QNAPのNASでは、USBポートにUSBディスクを取り付けてご使用いただけます。USBディスクを”**ネットワークドライブの非表示**”に設定し、アクセス権をすべて”**アクセス拒否**”に設定することで、共有フォルダ一覧から見つめることができず、見つけたとしても誰もアクセスできない状態にすることができます。

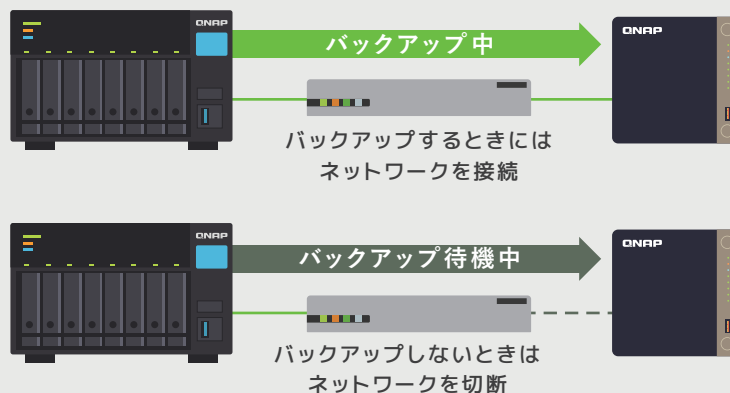
そのうえでNASのデータをUSBディスクにバックアップすれば、NASのデータを”**誰にもアクセスできないUSBディスクにバックアップできる**”ため、バックアップデータを安全に保管することができます。



## AirGap+ バックアップ

QNAPのNAS製品とルータ製品“QHora”を組み合わせることで、**バックアップを実行するときだけネットワークを接続するAirGap+バックアップ**を実現できます。

必要がないときはネットワークが切断されているので、ランサムウェアの感染リスクを大きく低減することができます。



データを書き出して  
オフラインで保管

## LTOバックアップ

QNAPのLTOドライブバンドルソリューションをご利用いただくことで、**簡単にLTOテープにデータを書き出し、保存**することができます。

LTOは磁気テープにデータを保存する技術であり、**30年を超えてデータを保管可能**です。テープを取り出して保管しておくことで、**ランサムウェアに攻撃されることもありません**。

法定要件にしたがった長期のデータ保管や、遠隔地にテープを運んで保管する場合に特におすすめです。



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。

**QNAP**