BUFFALO Value Chain Engineering　PATLITE　VVAULT AUDIT

# 情報資産の確実な保全に向けて

## ― バッファロー、ソリトン、パトライトの3メーカーで取り組む、危機を「見える」「聞こえる」形で捉えるソリューション ―

### 目次

企業の業務環境において、重要なデータをいかに保全するかは、安定した事業運営を支えるうえで欠かせないテーマです。業務データは日々の業務を支える基盤であり、ひとたび利用できなくなれば、業務そのものが停止してしまう恐れがあります。

まず想定すべきリスクとして挙げられるのが、ハードウェア障害です。サーバーやストレージに障害が発生すると、必要なデータにアクセスできなくなり、業務が滞るケースがあります。

さらに近年では、サイバー攻撃もデータ保全を脅かす大きな要因となっています。特にランサムウェア攻撃では、データが暗号化され、復旧までに長い時間を要するなど、業務継続に深刻な影響を及ぼす事例が増えています。
こうした障害や攻撃に早期に気付くことができれば、被害を最小限に抑えることが可能です。一方で、IT人材不足が続く中、とりわけ中小企業では、常にシステムを監視できる専任の担当者を配置することが難しい現実もあります。

そこで、業務データを守る基盤を担う株式会社バッファロー、異常な挙動を検知する株式会社ソリトンシステムズ、そして検知した異常を光と音で知らせる株式会社パトライトの3社は、それぞれの強みを組み合わせ、障害や攻撃の発生を誰にでも直感的に把握できるソリューションに取り組んでいます。

## バッファローが提供する障害に強い「NAS」

最初に紹介するのは、株式会社バッファロー(以下、バッファロー)が提供する、業務利用を想定したWindows OS搭載のNASです。

NASとは「Network Attached Storage」の略で、日本語ではネットワーク接続型ストレージと呼ばれます。PCに直接接続する外付けハードディスクとは異なり、ネットワークを介して複数の利用者や端末から同時にアクセスできる点が特長です。

企業の業務環境では、日常的に利用するファイルを複数人で共有し、継続的に運用するケースが一般的です。

そのため、データを保存できるだけでなく、障害が発生した場合でも業務を継続できることが重要になります。

この点について、同社 法人戦略推進部の小山 真氏は、次のように説明します。

**小山氏：法人の業務環境では、ファイルを共有しながら日常的に利用するケースが多くあります。そのためNASには、安定して稼働し続けることに加え、ハードウェア障害が発生した場合でもデータを守れる仕組みが求められます。**

**バッファローでは、こうした業務利用を前提にNASを提供しており、今回のソリューションではRAID 6に対応することで、障害への備えを強化しています。**



**株式会社バッファロー**
**法人戦略推進部**
**小山　真氏**

今回のソリューションに組み合わせるバッファローのNASの特長の一つが、RAID 6に対応している点です。

RAIDとは、複数のハードディスクを組み合わせて運用し、障害発生時の影響を抑えるための技術です。

RAID 6では、構成するハードディスクのうち2台に障害が発生しても、データを保全できます。保存するデータと復元に必要な情報を分散して記録することで、万が一の障害が発生した場合でも、業務データを失うことなく運用を継続できる点が特長です。
また、障害発生したハードディスクは交換することで長期的なデータ保全が可能となります。

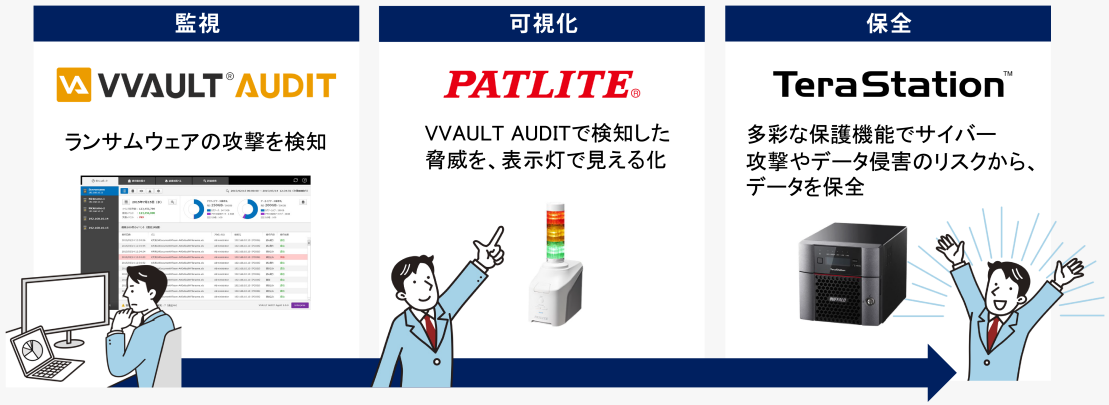
近年では、企業規模を問わずリモートワークを導入するケースが増えています。そうした環境において、NASは業務データを一元管理し、場所を問わずアクセスできる基盤として高い利便性を持ちます。

ハードウェア障害への備えを含め、NASは重要な業務データを保全するための基盤としての役割を担っています。

## 攻撃を「振る舞い」で検知する、ソリトンの「VVAULT AUDIT」

次に取り上げるのは、株式会社ソリトンシステムズ(以下、ソリトン)のプロダクト「VVAULT AUDIT」です。

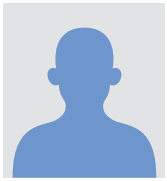
【図1】



VVAULT AUDITは、ファイルサーバーのログを管理し、異常なファイル操作を検知・通知するための製品です。近年被害が拡大しているランサムウェア攻撃についても、検知の対象としています。

業務データをNASで安全に保全していても、その上で不審な操作が行われていないかを把握できなければ、被害の拡大を防ぐことは困難です。そこで重要になるのが、ファイル操作の内容そのものを監視する仕組みです。

この点について、ソリトン ITセキュリティ事業部の木下 智雄は、次のように説明します。



株式会社ソリトンシステムズ
IT セキュリティ事業部

**木下　智雄氏**

**木下氏：外部から不正にアクセスされた場合でも、サーバー上で行われる操作自体は、内部の利用者と大きく変わらないケースがあります。そこでソリトンでは、攻撃者特有の行動パターンに着目し、それを見分ける技術を開発しました。これを『振る舞い検知』と呼んでいます。**

**ランサムウェア攻撃では、短時間に大量のファイル操作が発生するなど、通常とは異なる挙動が見られます。VVAULT AUDITは、こうした異常な振る舞いを検知することで、攻撃の兆候を捉えます。**

VVAULT AUDITはログ管理を担う製品でもあるため、検知した異常をもとに、感染したPCの特定や攻撃経路の把握といった分析にも活用できます。
検知して終わりではなく、その後の調査や対策につなげられる点が特長です。

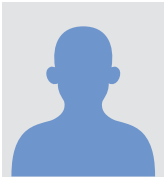
なお、バッファローのNASとVVAULT AUDITは、これまでもファイル操作の監視や異常検知を目的として連携して利用されてきました。
今回の取り組みでは、この検知結果を、さらに分かりやすく人に伝える仕組みへとつなげていきます。

## 検知した異常を「気付き」につなげる
## ― パトライト表示灯の通知・可視化

パトライト社は、パトカーや消防車などに搭載される警光灯やスピーカーで広く知られるメーカーです。一方で同社は、工場やオフィスといった業務現場において、光と音で状態を知らせるための製品も長年提供してきました。

VVAULT AUDITによって異常なファイル操作や攻撃の兆候を検知できたとしても、それに人が気付かなければ、迅速な対応にはつながりません。そこで重要になるのが、検知した異常を分かりやすく通知する仕組みです。

この点について、同社 東京営業課の西本 久信氏は、次のように説明します。



株式会社パトライト
東京営業課

**西本　久信氏**

**西本氏：パトライトの製品は、現場で何かが起きたことを、専門知識がなくても誰にでもすぐ分かる形で伝えることを目的としてきました。**

**たとえばネットワークや機器の状態に変化があった場合でも、画面を常に監視していなくても、光や音によって“何か起きている”と気付けることが重要です。**

実際の業務現場では、管理画面を常時確認できる体制を前提とできない場合も少なくありません。特に中小企業では、IT専任の担当者が常駐していないケースも多く、メール通知だけでは異常に気付くまでに時間がかかってしまうこともあります。

本ソリューションでは、VVAULT AUDITが検知したサイバー攻撃の兆候や、NASで発生したハードウェア障害を、表示灯の光や音で通知します。視覚と聴覚に訴えることで、専門知識がなくても異常の発生を直感的に把握できます。

このように、「監視する人」を前提とせず、「気付ける環境」をつくることが、今回のソリューションにおいてパトライト表示灯の技術が果たす役割です。検知と通知をつなぐことで、現場での初動対応を支援します。

## 3社の協力で実現する、攻撃と障害が「見える」「聞こえる」ソリューション

今回の取り組みは、バッファローとソリトンによる連携に、パトライトが加わることで実現しました。その背景について、バッファロー 法人戦略推進部の小山氏は次のように語ります。

**小山氏：NASとVVAULT AUDITの連携により、異常なファイル操作や攻撃の兆候を早期に検知できる点は、これまでも評価されてきました。一方で、異常を検知した後の通知手段はメールが中心で、必ずしも気付きやすいとは言えない場面もありました。**

**そこで、より直感的に異常を伝える方法として、光や音による通知を取り入れることを検討し、パトライト社に加わっていただきました。**

本ソリューションでは、大きく分けて2種類の異常を利用者に知らせます。
近年被害が拡大しているランサムウェア攻撃についても、検知の対象となります。

1つ目は、VVAULT AUDITが検知したサイバー攻撃の兆候です。メール通知だけでは他の連絡に埋もれてしまい、初動対応が遅れる可能性もあります。表示灯による通知を組み合わせることで、視覚や聴覚を通じて異常を把握しやすくなります。

この点について、ソリトン ITセキュリティ事業部の木下は、次のように話します。

**木下氏：パトライトの技術は、光だけでなく音による通知にも強みがあります。今回の協業では、攻撃の兆候やハードウェア障害が発生した際に、表示灯の点灯や音声によって異常を知らせます。これにより、メールだけでは気付きにくかった課題を改善できます。**

2つ目は、NASにおけるハードウェア障害です。RAID 6に対応したNASは、複数台のハードディスクに障害が発生した場合でもデータを保全できますが、障害の発生に早く気付けなければ、障害発生したハードディスク交換などの復旧対応が遅れる可能性があります。

表示灯による通知によって障害を「見える化」することで、現場での初動対応を早め、復旧までの時間短縮につなげることができます。

この点について、パトライト社の西本氏は次のように述べます。

**西本氏：攻撃や障害に迅速に気付けることは、利用者にとって大きな意味があります。早期に対応できれば、被害の拡大や復旧の遅れを防げるケースもあります。**

**3社はいずれもメーカーであり、販売店とも連携しながら、現場に合った形で、セキュアな環境づくりを支援していきたいと考えています。**

なお、どのような異常を通知するか、どのタイミングで表示灯を動作させるかといった設定は、利用環境に応じて調整できます。運用に合わせて柔軟に構成できる点も、本ソリューションの特長です。

## まとめ

バッファロー、ソリトンシステムズ、パトライトの3社による本ソリューションは、ハードウェア障害やサイバー攻撃といった重要なリスクに、いち早く気付くための仕組みです。

業務データを保全する基盤としてのNAS、ファイル操作の異常を検知するVVAULT AUDIT、そして検知した異常を光と音で知らせる通知の仕組みが、それぞれの役割を担います。それぞれの役割を組み合わせることで、メール通知だけでは見落とされがちな異常にも、現場で気付きやすい環境を実現します。

ハードウェア障害であっても、ランサムウェアをはじめとしたサイバー攻撃であっても、早期に気付くことができれば、被害や業務への影響を最小限に抑えることができます。一方で、対応が遅れれば、復旧に時間を要し、企業の信頼に影響を及ぼすリスクも高まります。

IT人材不足が続く中、とりわけ中小企業では、システムを常時監視する体制を整えることが難しいケースも少なくありません。そうした環境において、本ソリューションは専門知識や常時監視を前提とせず、「気付ける」仕組みを補完する一つの手段となります。

3社の取り組みは、企業の重要な情報を守り、安定した業務継続を支えるための一つの選択肢として、今後も現場に寄り添いながら取り組んでいきます。


### 株式会社バッファロー

**東京本社**
〒100-6215　東京都千代田区丸の内一丁目11番1号 パシフィックセンチュリープレイス丸の内
https://www.buffalo.jp/
TEL:03-4213-1122（代表）

### 株式会社パトライト

**東京本社**
〒141-0032　東京都品川区大崎 1-6-1
https://www.patlite.co.jp/
TEL:：03-6866-8008（代表）


### ネットアテスト

「ネットアテスト」は、企業ネットワークに関わる全ての方のためのサイトです。安心・安全な環境を実現したい情報システム担当者様、確かなシステムを提案されたいインテグレータ様に向けて、運用の効率化やセキュリティ強化の方法などをお届けしていきます。

サイトはこちら