ランサムウェア対策ファイルサーバを実現

VVAULT シリーズ

特許取得の攻撃検知・ブロック・復旧を実現する技術のご紹介

株式会社ソリトンシステムズ

IT セキュリティ 事業部

2022 年 3 月

ランサムウェア被害が拡大

独立行政法人情報処理推進機構（IPA）が発表した「情報セキュリティ 10 大脅威 2022」（組織）では、「ランサムウェアによる被害」が昨年度に続き 2 年連続 1 位にランキングした。また、NISC（内閣サイバーセキュリティセンター）からも「ランサムウェアによるサイバー攻撃について」という文書を出し、企業経営者やセキュリティ担当者へ注意喚起している。

ランサムウェア攻撃が活発化している背景には「テレワークの普及」がある。堅牢なファイアウォールで守られた会社での作業と異なり、テレワーク業務は攻撃の対象になりやすい。企業は今一度自社のセキュリティポリシーを見直し、対策を講じなければならない。

IPA 情報セキュリティ10大脅威 2022

順位	「組織」向け脅威	昨年度順位
1	ランサムウェアによる被害	1位
2	標的型攻撃による機密情報の窃取	2位
3	サプライチェーンの弱点を悪用した攻撃	4位
4	テレワーク等のニューノーマルな働き方を狙った攻撃	3位
5	内部不正による情報漏洩	6位
・	・	・

ランサムウェアの主な攻撃経路

ランサムウェアの主な攻撃経路は主に 4 つに大別される。

- **Web サイト経由**
  - ・改ざんされた正規の Web サイトを閲覧することで感染
  - ・不正広告を閲覧することで感染
  - ・ダウンロードしたファイルを開くことで感染

- **メール経由**
  - ・メール本文に記載された URL からアクセスすることで感染
  - ・メールの添付ファイルを開くことで感染

- **RDP（リモートデスクトップ）経由**
  - ・脆弱なユーザのサインイン認証情報（ブルートフォース攻撃）
  - ・無制限のポートアクセス（ポート 3389 へのアクセス：RDP 脆弱性など）

- **OS,ファームウェアの脆弱性経由**
  - ・「SMBv1」などの脆弱性や OS の脆弱性への攻撃
  - ・ VPN ルータ等のファームウェア脆弱性への攻撃

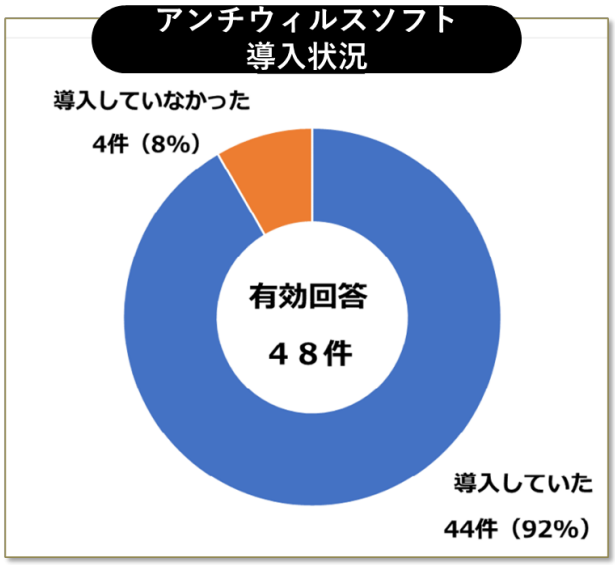
これらの攻撃経路対策としては、一般的には次のような対策が行われている。これらにより、ある程度の対処は可能となる。

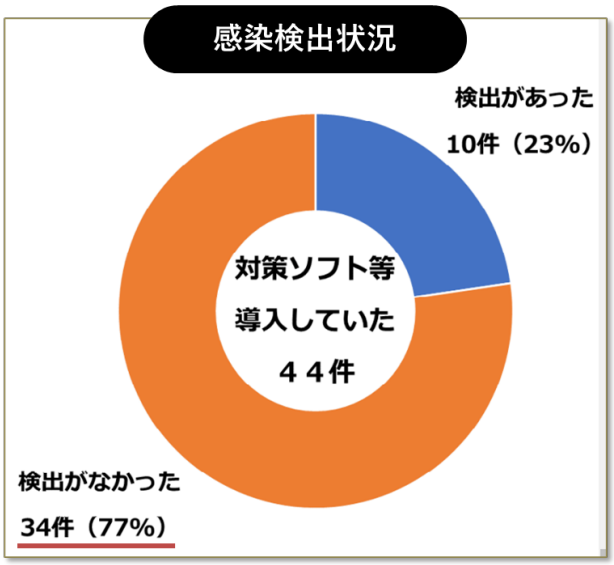
Web サイト、メール経由	**⇐ アンチウィルスソフト**
RDP 経由	**⇐ 運用ポリシー等の見直し**
OS,ファームウェア等の脆弱性経由	**⇐ OS, ファームウェア等の定期的な更新**

一般的な対処方法だけでは危険

OS、ファームウェア等の脆弱性や、RDP 経由の攻撃などは、システムの更新やポリシー等の強化であらかた問題解決できる。一方、ランサムウェア攻撃は高度化しており、一般的なアンチウイルス対策だけでは万全ではない。ランサムウェア攻撃は、アンチウィルスソフトウェアの検知を簡単にくぐり抜けてくる。所謂ゼロディ攻撃だ。端末が乗っ取られると、その端末がアクセス可能なファイルサーバの共有フォルダは、端末が保有する正規の権限を使って簡単にファイルの改ざんなどを行ってしまう。警察庁のレポートでは、90%以上の会社がアンチウィルスソフトを導入していたが、77%がランサムウェアに感染してしまったというレポートがある。このレポートからも、端末からの攻撃を前提としたソリューションが必須となる。

日本のゼロデイ攻撃の被害率は 77% 程度





抜粋：警察庁 令和３年9月9日 広報資料
「令和３年上半期におけるサイバー空間をめぐる脅威の情勢等について」

端末からの攻撃を前提とした環境を提供

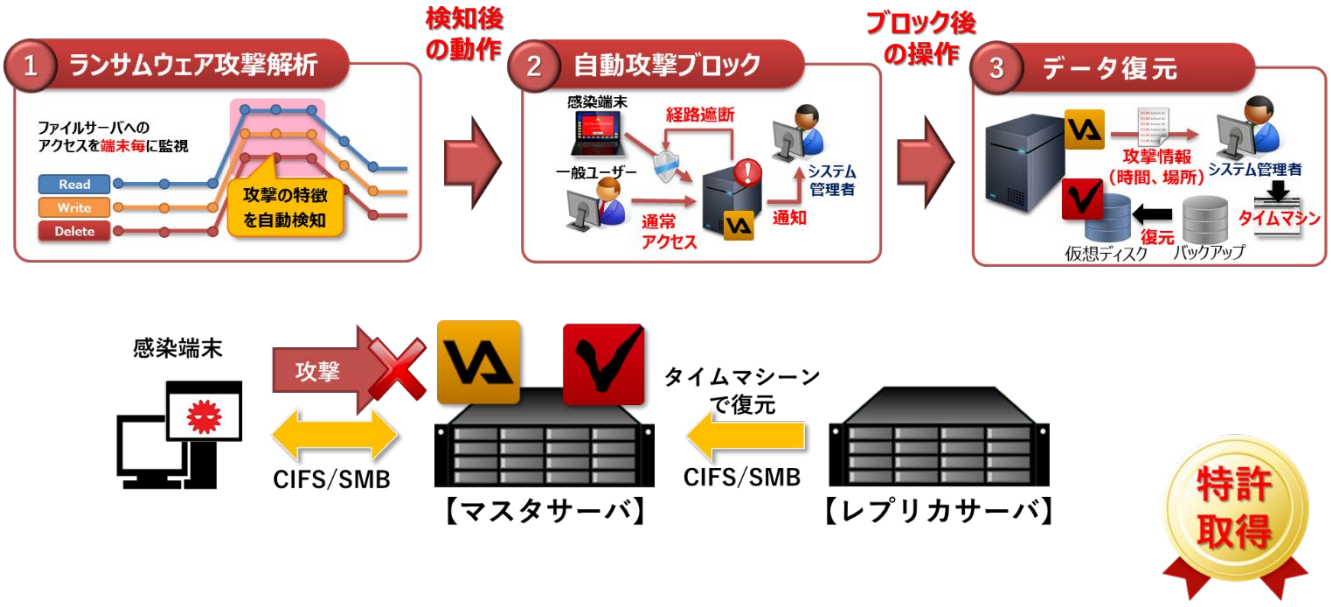
VVAULT シリーズを用いたファイルサーバでは、端末からの攻撃を前提とした安全な環境を作り出すことができる。特許取得のランサムウェア攻撃の「検知」「ブロック」そして「復旧」を提供する技術だ。ランサムウェア攻撃の「検知」「ブロック」は VVAULT AUDIT（ブイボルト オーディット）、データの冗長化や復元は、VVAULT（ブイボルト）で行う。

- **ランサムウェア攻撃の検知＆ブロック「VVAULT AUDIT」**
  ファイルのアクセス履歴や安全管理の証跡としてログを保存するサーバログ管理ソフトウェアに、ランサムウェア攻撃の検知、ブロックの機能が搭載された製品。端末毎にファイルサーバへのアクセスを解析し、ランサムウェア攻撃の特徴を検知した場合に、攻撃端末のアクセスを自動遮断する仕組みを搭載。

- **データ冗長化＆復旧「VVAULT」**
  Windows 上にマウント可能なさまざまなストレージを 1 つに統合して大容量の仮想ストレージ／ファイルサーバを手軽に構築。「ファイルの使用頻度による自動配置（ティアリング機能）」や「過去の任意時点のデータ復元（タイムマシーン機能）」をはじめとした先進的な機能で、ファイルサーバ運用の効率化と業務の継続性を実現する。また、HA 構成を組むこともでき、予備サーバへ SSL 通信でデータを冗長化可能。ランサムウェア攻撃が届かない場所へデータを冗長化できる。

端末からの攻撃を検知･ブロックそして復元

VVAULT AUIDIT は、各端末からのアクセスを常時監視し、ランサムウェア攻撃特有の動きを検知した場合は、サーバ側で攻撃端末だけをアクセス出来ないようにブロック。ブロック後は管理者に攻撃を検知したことを通知。なお、検知からブロックまでの間は、ファイルが攻撃されてしまう。ブロック後は、管理者側で状況を確認把握し、レポート機能で攻撃端末、攻撃開始時間、攻撃範囲を確認し、VVAULT が提供するタイムマシーン機能で攻撃前の攻撃対象ファイル群を復元できる。この一連の機能は、特許も取得している。



① ランサムウェア攻撃解析

端末等からのランサムウェア攻撃は、ターゲットのファイルを参照（Read）、続けて暗号化したファイルの書き出（Write）、最後に、元あったファイルを削除（Delete）する。この一連のアクションがランサムウェア攻撃である。VVAULT AUDIT はこの 3 つのアクションを端末毎にモニタリングし、攻撃判定を行う。

② 自動攻撃ブロック

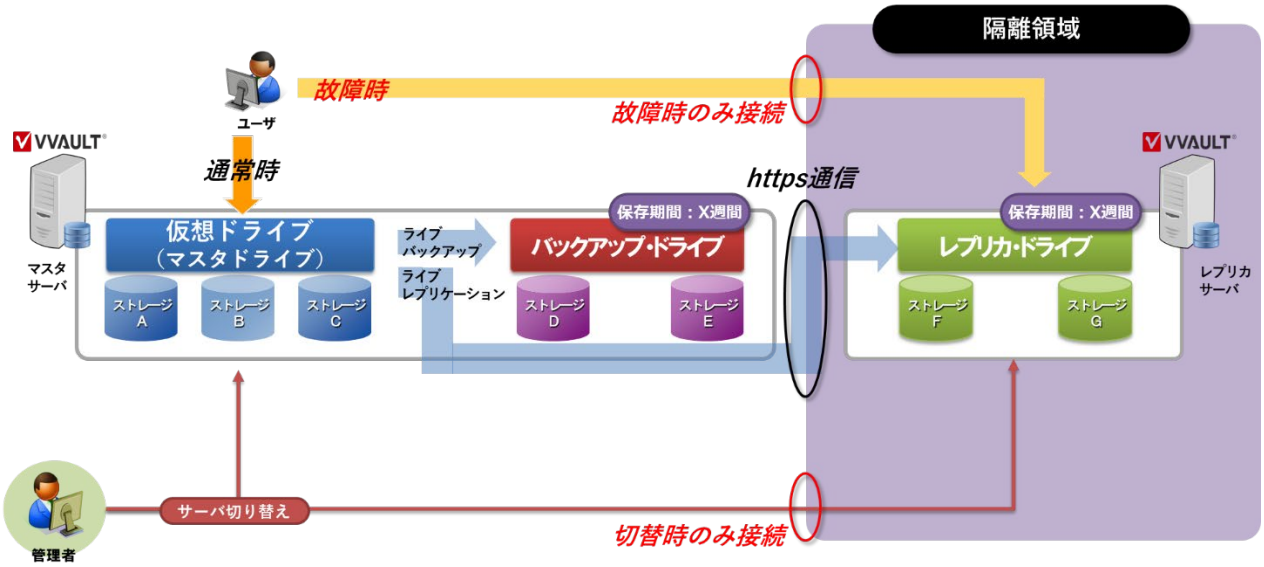
攻撃判定されると、攻撃端末のアクセスをブロックし、管理者に攻撃があったことを通報します。ブロックされている間は、端末からの攻撃は出来なくる。

③ データ復元

VVAULT AUDIT は、いつから、何処を攻撃したかのレポートを出す。あとは、VVAULT のタイムマシーン機能で該当ファイルを復元することで元に戻すことができる。

隔離領域へ SSL 通信でデータ冗長化

ランサムウェア攻撃は、参照可能なサーバ等は全て攻撃の対象となる。リスク回避の為には、予備サーバであるレプリカサーバは、ユーザが普段利用するネットワークから分離された隔離領域に配置し、マスタサーバから SSL 通信だけを許可した状態で運用すれば安全である。VVAULT の HA 構成では、データの冗長化は SSL 通信で転送でき、予備環境を安全に保てる。



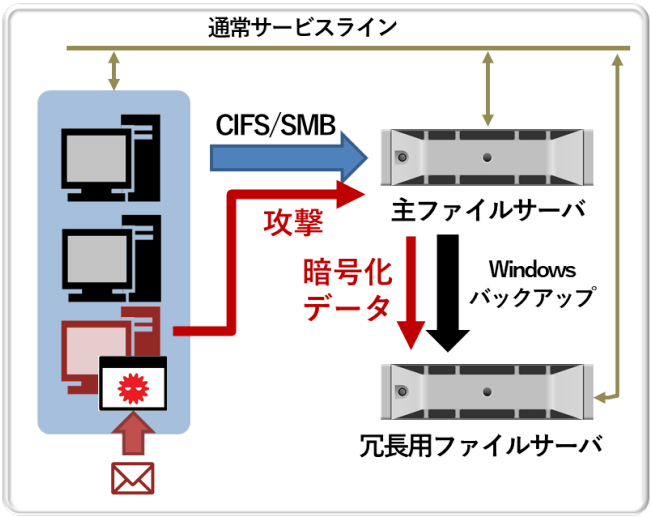
VVAULT タイムマシーンで楽々データ復元

VVAULT のタイムマシーンは、消去された時間が分かれば、それより前に存在していたファイルを簡単に復元できる。冗長化先には、指定した保存期間であれば、消去したデータも保存されており、管理画面で指定し、任意の場所へ復元できる。

VVAULT 改善事例

ランサムウェア攻撃でファイルサーバ内のデータを全て失ってしまったお客様の改善事例を紹介する。ランサムウェア攻撃を受けた環境は以下の環境であった。

【 企業情報 】
業種：不動産業、従業員数：150 名



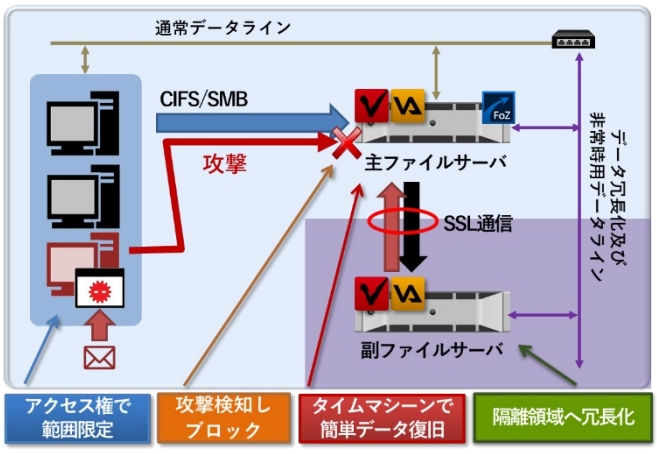
改善前の構成の問題・課題

- ファイルサーバ主副サーバが同一環境
- バックアップ先へ全ユーザがアクセス可能
- アクセス権が設定されていない
- ウイルス対策ソフトのみ導入

サーバへのアクセスが自由に行える状況に加え、ゼロディ攻撃で突破されると、主副の両サーバが同一ドメインでの運用でもあり、簡単に全体を攻撃されてしまう。

VVAULT 導入後の構成ポイント

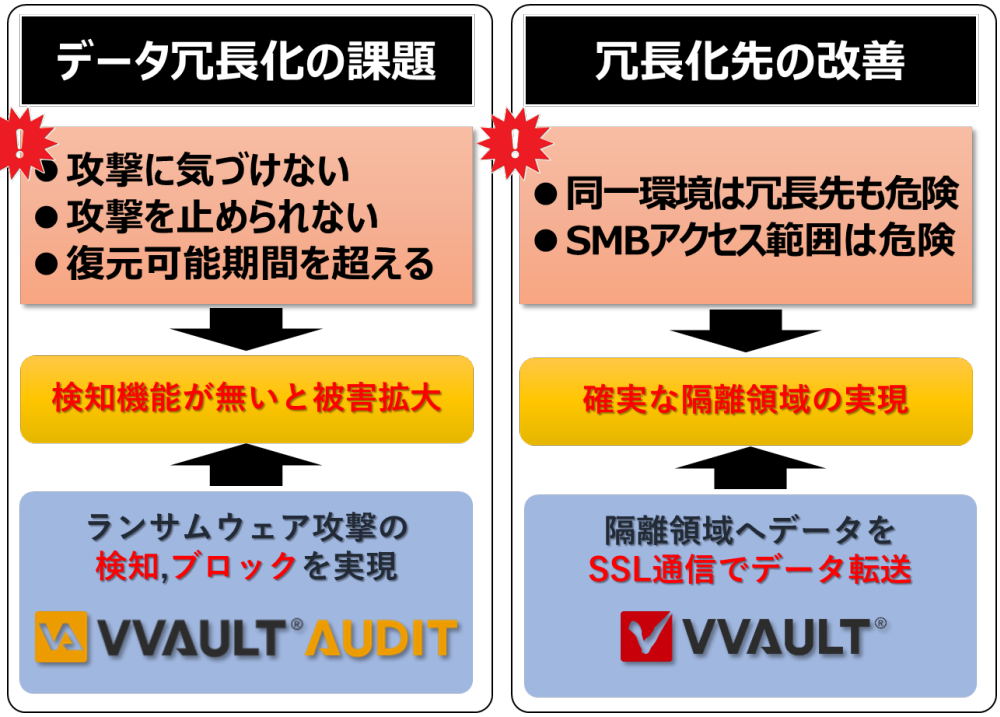
- 副サーバを隔離領域へ配置
- 非常時以外は副サーバへアクセス禁止
- アクセス権でアクセス範囲を限定
- VVAULT で検知・ブロック・復元を実現



今回、改善した構成では、VVAULTAUDIT でランサムウェア攻撃の検知＆ブロックを実現。VVAULT で SSL 通信による隔離領域へのデータ冗長化を実現。また、弊社アクセス権ソリューションの FolderZen によりアクセス権を確実に設定した。

まとめ

ランサムウェア攻撃の被害は拡大し続けている、単純なバックアップだけではデータは守ることが難しい。VVAULTのシリーズは、攻撃を「検知」「ブロック」「復元」できる仕組みと、攻撃されにくい場所へ冗長化することができるソリューションに仕上がっている。



株式会社ソリトンシステムズ

IT セキュリティ事業部

東京都新宿区新宿２－４－３

Tel 03-5360-3809

Netsales@soliton.co.jp