ソリューション概要

FlashArray による ランサムウェア対策

悪意のある攻撃からの迅速なリカバリを可能にする FlashArray™ SafeMode™

ランサムウェア攻撃に関するニュースが連日のように報じられています。ランサムウェアをはじめとするサイバー攻撃は、世界中のあらゆる業界の脅威となっています。ビジネスにおけるリスクは急激に増大しており、世界全体での損失は、2025 年までに 10 兆 5 千億ドルに達すると予測されています。[1] ビジネスが受ける被害は、ダウンタイムや金銭的な損失だけではありません。攻撃が大きなニュースにならない場合でも、企業のレピュテーションが損なわれる危険があります。

ピュア・ストレージの FlashArray と SafeMode スナップショットを利用することで、重要なデータをロックしてサイバー攻撃後のリカバリに備え、ビジネスの迅速な再開を可能にします。攻撃者の要求に屈する必要はありません。

ピュア・ストレージのモダン・データ保護に対するアプローチは、単なる損害の補填ではありません。現代のデータセンター運用に不可欠な要素の 1 つです。ピュア・ストレージのソリューションは、複数のプラットフォームとテクノロジーを包含しており、重要なデータとアプリケーションの効率的な保護、超高速リストア、ビジネスにおけるデータの徹底的な活用を可能にします。プライマリ・ワークロードの可用性確保からスナップショット、バックアップ・コピー、さらにはクラウド上の長期アーカイブに至る一連の保護テクノロジーです。

リカバリ・データを保護してビジネスを守る

ランサムウェアに対抗するには、ハッカーの裏をかく周到な計画が必要です。攻撃者が標的を絞り込む傾向にある昨今では、このことは極めて重要です。攻撃者は、一般的に、攻撃の数週間前からシステムへの侵入を開始し、脆弱性を探ります。その後攻撃を開始し、独自のキーで本番データを暗号化して、そのキーと引き換えに金銭を要求します。同時に、システムを攻撃前の状態に戻すためのスナップショットやバックアップ・データに対しても、暗号化や破壊行為を行います。

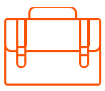
SafeMode は、リカバリに不可欠なスナップショットとバックアップ・データを 2 つの方法で保護します。第一に、常時オンのイミュータビリティ（変更不可）機能によって、リカバリ・データの破損や暗号化を阻止します。第二に、タイマー付き消去ポリシーによって、リカバリ・データの完全破壊を阻止します。たとえ管理者権限が乗っ取られても、データの変更や削除ができません。

エンタープライズ・データに対する脅威

ランサムウェア攻撃の 73% で、サイバー犯罪者がデータの暗号化に成功している。[2]

財務面のリスク

IT サービス大手の Cognizant がランサムウェア攻撃を受け、損失額を 5,000万～7,000万ドルと見積もる。[3]



生産性の低下

米メリーランド州ボルティモア郡の公立学校がランサムウェア攻撃によって休校となり、11万5,000 名の生徒に影響が及んだ。[4]

高効率なイミュータブル・スナップショットによるリカバリの迅速化

Pure FlashArray は、事業継続性とディザスタ・リカバリの幅広いオプションを提供しています。迅速なリカバリを可能にするスナップショットもその 1 つです。スナップショットとは、データ保護やディザスタ・リカバリの際に参照できるよう、ある時点の状態を丸ごと保存したものです。データベース・ボリュームなどのボリューム・イメージのスナップショットを作成しておけば、すぐにリカバリができます。また、バックアップ・データとメタデータ・カタログのスナップショットを作成し、データ保護のレベルを高めることもできます。スナップショットは、データのイミュータブル（変更不可）なコピーです。たとえランサムウェア攻撃によって管理者アカウントが侵害された場合でも、データの搾取や改ざんはできません。

ピュア・ストレージのスナップショット機能は、全ての FlashArray に無償でバンドルされており、設定も容易です。ピュア・ストレージのスナップショット機能は、次のような特長を備えています。

- **イミュータブル（変更不可）：**いったん作成したスナップショットは、管理者権限を持つユーザーでも変更や暗号化ができません。
- **高効率：**前回のスナップショットからの差分だけ（変更のあったブロックだけ）を保存するため、スナップショット作成時間の短縮と、全データを複製しないことによるストレージ・コストの削減を可能にしています。
- **通常のボリュームとして機能：**スナップショットは通常の新規ボリュームとして機能します。元のボリュームと同様の性能で、マウント、読み取り、書き込みができます。スナップショットからさらにスナップショットを作成することもできます。
- **柔軟性：**任意のスナップショットで任意のボリュームをリカバリできるため、ロールバック／フォワードを直ちに行い、業務を再開できます。
- **自動化：**エンドツーエンドの保護ポリシーによってスナップショットの作成を自動化し、柔軟性と信頼性を備えた不安のない運用を可能にします。

図1：SafeMode は、サイバー攻撃による暗号化や消去を阻止し、FlashArray スナップショットを保護します。

攻撃者が消去できないスナップショット

攻撃者による SafeMode スナップショットの暗号化や改ざんを防げたとしても、それだけでは十分ではありません。攻撃者は、暗号化したデータをシステムから消去（完全破壊）することでリカバリの妨害を試みるかもしれません。FlashArray は、消去タイマーによって一定期間データをロックダウンし、データの完全破壊を防ぐという方法で、これに対抗しています。消去タイマーの機能により、管理者権限を持つユーザーを含め、誰もデータを消去できなくなります。

消去タイマーはデフォルトで 24 時間に設定されています。SafeMode を有効にすると、最大 30 日まで延長できます。消去タイマーの設定をカスタマイズすることで、FlashArray 上のセキュアなイミュータブル・スナップショットを使用してシステムをロールバックする場合に、時間的な余裕が得られます。スナップショットの格納場所は、ローカル、リモートを問いません。FlashArray//X、FlashArray//C、Pure Cloud Block Store™ のいずれでもサポートされています。

身代金を支払わずに迅速にリカバリ

ランサムウェア攻撃を検知し、不正アクセスの防御策を講じたら、直ちにリカバリ手順に取り掛かりましょう。このような状況に備えて、SafeMode がスナップショットをセキュアに保護しています。したがって、まずは、攻撃者によって暗号化あるいは侵害されたデータを全て消去します。次に、セキュアな SafeMode スナップショットから、ボリュームを直ちにリストアします。システムは速やかに、攻撃を受ける直前の状態に戻ります。身代金を支払う必要はなく、組織のレピュテーションが損なわれることもありません。

関連リソース

- ホワイトペーパー：FlashArray Security and Compliance（FlashArray のデータ・セキュリティとコンプライアンス）
- ソリューション概要：Ransomware Mitigation with FlashBlade SafeMode（FlashBlade と SafeMode によるランサムウェア対策）

1「Cybercrime to Cost the World $10.5 Trillion Annually By 2025」、Cybersecurity Ventures（2020年11月）
2「The State of Ransomware 2020」、Sophos（2020年5月）
3「Cognizant expects to lose between $50m and $70m following ransomware attack」、ZDNet（2020年5月）
4「Ransomware Attack Closes Baltimore County Public Schools」、New York Times（2020年11月）

ピュア・ストレージ・ジャパン株式会社
お問い合わせ：03-4563-7443（代表）
https://www.purestorage.com/jp/contact.html

PS2028-01 03/2021