C-001

ランサムウェア対策に向けたストレージシステムの Redirect on Write Snapshot 方式の提案と評価
A Study on Redirect on Write Snapshot Method of Storage Systems for Ransomware Protection

山賀 祐典† 松下 貴記† 出口 彰†
Yusuke Yamaga Takaki Matsushita Akira Deguchi

1. はじめに

年々、ランサムウェアなどのマルウェアによるセキュリティ被害が増加している[1]。攻撃者はランサムウェアを使用して企業のデータを暗号化することで使用できなくし、データを復元する代わりに身代金を要求する。標的型攻撃メールの開封による感染など、人を介することもあるため、完全にランサムウェアの侵入を防ぐことは困難である。そのため、侵入されることを前提とした対策を行い、攻撃を検知した場合に迅速な復旧ができるように準備をしておくことが重要となっている。

ランサムウェアが侵入し、データが暗号化されてしまった場合は、暗号化されていない安全なバックアップからの復旧が必要となる。本研究が対象とするストレージシステムでは、論理的なデータ複製機能である Snapshot 機能を提供しており、バックアップされている暗号化前のデータを使って復旧させることが可能である。データ損失被害を小さくするためには、バックアップ頻度を増やすことが求められる。また、ランサムウェア被害に気付くまでに時間を要する場合もあるため、作成したバックアップを一定期間保持することが必要となる。高頻度で作成された Snapshot を一定期間保持する必要があるため、ランサムウェア対策では Snapshot の数が増加する傾向がある。本研究では、ランサムウェア対策に求められる、高頻度・多数バックアップ可能な Snapshot 方式を検討する。

2. ストレージシステムの Snapshot 機能の概要

図 1 を用いてストレージシステムの Snapshot 機能の概要を説明する。Snapshot 機能は、論理的なデータ複製機能であり、複製時刻のデータを保持し続けることが可能である。ストレージシステムでは、ホストからアクセス可能な論理ボリュームの論理アドレスと、HDD や SSD を RAID などの技術によって束ねた物理的な記憶領域である容量プールのデータ格納アドレスの対応関係をメタデータで管理している。また、一般的な Redirect on Write (RoW) Snapshot 方式では、ライト処理や Snapshot 作成処理の効率化のため、メタデータをツリー構造で管理している[2]。Snapshot 作成処理では、複製元ボリュームのメタデータを作成した Snapshot から参照(S1)することで、複製元ボリュームと Snapshot でメタデータ及びデータを共有し、複製元と同じデータを Snapshot からアクセスすることが可能になる。

また、Snapshot 作成後に複製元ボリュームにデータ更新する場合の処理を以下で説明する。ストレージシステムは、ホストから論理ボリュームへのデータ書き込み要求を受領すると、キャッシュメモリに書き込みデータを格納した(W1)後、ホストに書き込み完了のレスポンスを返す(W2)[3]。その後、データの圧縮処理などを実施したあと、容量プールの更新前データとは別のアドレスにデータを格納する(W3)。最後に、格納したデータを参照するようにメタデータを更新するのだが、Snapshot と共有しているメタデータを書き換えないよう、メタデータの更新単位であるノードを新規確保し、格納データを直接参照するように更新を行う(W5)。このように、ライト処理契機で、更新前データとは別のアドレスに更新データを格納し、格納データを参照するようにメタデータを書き換えるため、RoW 方式と呼ばれている。

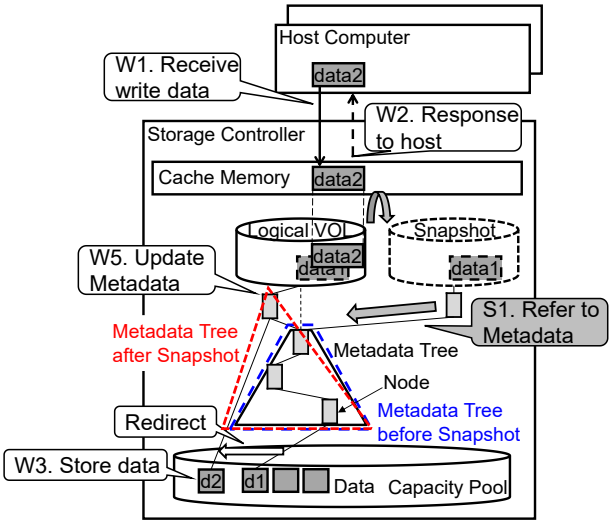

図 1 従来 Redirect on Write Snapshot 機能の概要

3. Redirect on Write Snapshot 機能の課題

前章で説明した通り、RoW Snapshot 方式では、Snapshot を作成すると、複製元ボリュームのメタデータツリーを Snapshot から参照する。即ち、複製元ボリュームのメタデータツリーの最上位ノードが Snapshot から参照され、書き換え不可(ReadOnly)になる。このため、その後のライト処理契機で、複製元用に新たにメタデータノードを確保し、そのノードから ReadOnly ノードを参照するため、メタデータツリーの段数が増加する(図 1)。データ読み出し処理では、読み出し対象論理アドレスに対応する格納データを、メタデータのノードを辿って探索する。このため、メタデータのノードの段数が増えると、複製元ボリュームのリード性能が低下する問題がある。本研究では、多数の Snapshot を作成しても性能維持が可能な方式を検討する。

4. 提案方式

従来方式では、Snapshot 作成により複製元ボリュームの最上位のメタデータを共有するため、ライト処理時にメタデータの新規確保が必要になり、メタデータの段数が増えてしまっていた。

そこで本方式では、Snapshot 作成契機で、複製元ボリュームのメタデータを Snapshot 用にコピーし、最上位のメタデータを共有しないようにする。また、メタデータは 2 段固定構造とし、データの管理単位が大きい 1 段目の粗粒度

† 株式会社 日立製作所 研究開発グループ
Hitachi, Ltd. Research & Development Group

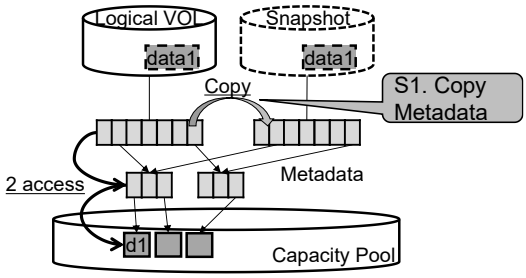

図 2　提案する RoW 方式の Snapshot 作成概要

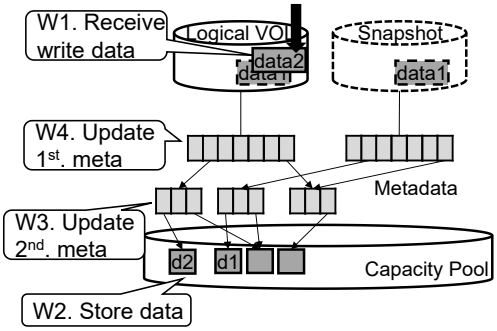

図 3　提案する RoW 方式のライト処理概要

メタデータのみをコピーし、データを直接ポイントする 2 段目の細粒度メタデータは複製元ボリュームや Snapshot 間で共有するようにした。本方式では、2 段固定構造により最上位のメタデータのコピー時間がかかるのだが、コピー中でも複製元ボリュームや Snapshot の IO を可能にすることで、従来方式同等の Snapshot 作成操作時間を実現することが可能となる。

5. 評価方法

本研究では、論理ボリュームから Snapshot を多数取得した場合における複製元ボリュームの IO 性能をシミュレーションにより評価する。調査会社のレポートによると、約 6 割の組織が 15 分未満の RPO (Recovery Point Objective)を、約 8 割の組織が 30 未満の RPO を求めている[4]。また、ランサムウェア侵入から検知までの平均日数は 6 日[5]であることから、15 分、及び、30 分間隔で作成した Snapshot を 1 週間保持する想定で評価を行う。

ベースとなる Snapshot 機能未使用時の IO スループット性能(IOPS：Input Output per Second)は、日立製ブロックストレージ装置の公開情報[6]を使用する。また、1 つのメタデータノードにアクセスする処理時間は、メタデータツリーのノードのサイズ等に依存するため、複数の値(0.5us/1us/2 us)を仮定し、評価を行う。即ち、従来方式では、Snapshot 取得数に応じてメタデータノードのアクセス回数及び処理時間を増加させる。一方、提案方式では、メタデータノードのアクセス回数を 2 回固定とし、メタデータコピー中の IO を想定した評価を行う。その他の評価条件については、表 1 に示す。

6. 評価結果

図 4 に評価結果を示す。横軸に仮想ボリュームから取得した Snapshot 数を、縦軸に Snapshot 機能未使用時を基準とした IO スループット性能低下率を示している。従来 RoW 方式では、Snapshot 数が増加するにつれてメタデータのアクセス回数が増加するため、IO スループット性能が低下する。30 分間隔(336 Snapshots)では 3 割~6 割、15 分間隔(672 Snapshots)では、2 割~5 割まで IO 性能低下してしまうことがわかった。

一方、提案方式では、メタデータコピー処理中は 1 割程度 IO 性能が下がるものの、Snapshot 数が増加しても IO スループット性能を維持することができている。

表 1 評価条件

項目	*条件*
Snapshot 数	15 分間隔:4 個/hour ×24hour ×7day=672 個 30 分間隔:2 個/hour ×24hour ×7day=336 個
メタデータアクセス単価	0.5us、1us、2 us
IO パターン	IO 長 =32KB 、 Read:Write 比 =7:3 [6] 、Random
仮想ボリューム容量	32 TB

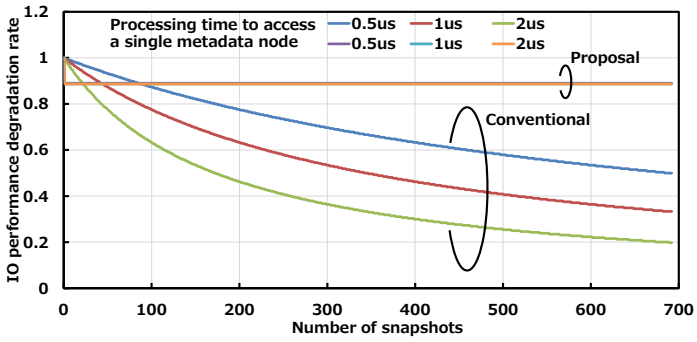

図 4　評価結果

7. おわりに

本研究では、ランサムウェア対策に求められる、高頻度・多数バックアップ可能な Snapshot 方式を検討した。提案する RoW 方式では、メタデータを 2 段固定構造とし、1 段目の粗粒度メタデータのみをコピーし最上位のメタデータが共有しないようにすることで、メタデータの段数が増加しないようにした。評価の結果、Snapshot 取得数が増加しても IO 性能を維持できることがわかった。

参考文献

[1] Cyber Security Ventures, Global Ransomware Damage Costs Predicted To Exceed $275 Billion By 2031, https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.
[2] John Colgrove, John D. Davis, John Hayes, Ethan L. Miller, Cary Sandvig, Russell Sears, Ari Tamches, Neil Vachharajani, and Feng Wang. Purity: Building fast, highly-available enterprise flash storage from commodity components. In Proceedings of the 2015 ACMSIGMODInternational Conference on Management of Data (SIGMOD), 2015.
[3] 山賀 祐典, 松下 貴記, 弘中 和衛, 川口 智大, “高性能・高圧縮率を両立するストレージシステムのデータ圧縮機能の検討”,電子情報通信学会, Vol.119, No.76, (2019).
[4] Enterprise Strategy Group, “Real-world SLAs and Availability Requirements”, https://www.purestorage.com/content/dam/pdf/en/analyst-reports/protected/ar-real-world-slas-and-availability-requirements.pdf, (2020).
[5] Mandiant, M-Trendes, https://services.google.com/fh/files/misc/m-trends-2025-en.pdf.
[6] Hitachi Vantara, “Virtual Storage Platform E590 and E790: High Performance With a Low Profile”, https://community.hitachivantara.com/blogs/charles-lofton/2021/04/21/virtual-storage-platform-e590-and-e790-high-performance-with-a-low-profile.