

ライブラリの置き換えによる VM 外部への安全なログ転送方式における 応用プログラムを用いた性能評価

Performance Evaluation with APs for Secure Log Transfer Method Using Library Replacement

佐藤 将也[†]
Masaya Sato

山内 利宏[†]
Toshihiro Yamauchi

1. はじめに

計算機の動作を把握するには、計算機上のログが重要である。しかし、攻撃や問題の発生により、ログの改ざんや消失が起こる可能性がある。攻撃者は、攻撃の痕跡を消すために、ログを改ざんする。

この問題へ対処するために、ログを保護する手法が研究されている。しかし、これらの研究では、カーネル内におけるログの改ざんには対処できないものが多い。我々の既存研究 [1] は、これらの攻撃へ対処できる。しかし、多種の OS への対応や性能低下の問題がある。

そこで、複数 VM 上の多種の OS に、最小限のプログラムの修正により対応可能な、VM 外部への安全なログ転送方式を提案した [2]。本稿では、提案方式の AP を対象とした性能評価について述べる。

2. 研究背景

2.1. syslog を用いたログの保存

Linux では、ログの保存に syslog が広く用いられている。Linux において、AP が syslog を用いてログを保存する際の手順は以下の通りである。

- (1) AP は、ログを生成
- (2) AP は、syslog デーモンへログを送信
- (3) syslog デーモンは、受信したログを書き出し

syslog デーモンは、AP から受信したログを、ログの書き出しポリシーに従い、ログファイルへ書き出す。また、受信したログを暗号化した通信路でリモート計算機に転送する機能を持つものもある。

2.2. 想定される攻撃

ログの改ざんの契機は、以下のように分析できる。

- (契機 1) AP がログを生成し、syslog デーモンへログを送信するまでの間
- (契機 2) AP が syslog デーモンへログを送信し、syslog デーモンがログを受信するまでの間
- (契機 3) syslog デーモンが AP からのログを受信し、ファイルへの書き出し処理を開始するまでの間
- (契機 4) ファイルへ書き出す処理を行っている間
- (契機 5) ファイルへ書き出された後

(契機 2) ~ (契機 4) は、ログの書き出しで共通する処理に含まれるため、攻撃者は、syslog を用いたログの書き出しを検知し、改ざんできる。

2.3. 既存手法の問題

ログの改ざんを防止するには、すべての契機における攻撃を防止するか、早期に計算機外部へログを転送し、

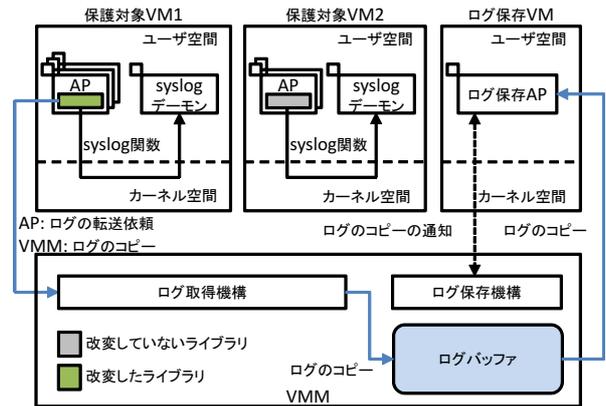


図 1 提案方式の全体像

改ざんの契機を少なくする必要がある。既存手法の組み合わせにより、すべての契機におけるログの改ざんを防止できる。しかし、実装や運用管理のコストが高い。また、OS の種類やバージョンの差異への対応が難しい。さらに、処理手順の増加に伴う性能低下が予測される。

3. ライブラリの置き換えによる VM 外部へのログ転送方式

3.1. 目的と課題

2.3 節の問題を解決するための課題を以下に示す。

- (課題 1) できるだけ早期にログを保護し、計算機外部へ転送すること
- (課題 2) OS の種類やバージョンの差異への対応
- (課題 3) ログ転送のオーバーヘッドの抑制

(課題 1) により、攻撃者がログを改ざんする契機を少なくする。(課題 2) により、多種の OS への適用やバージョンの違いへの容易な対応を実現する。(課題 3) により、より実用的な機構を実現する。

3.2. 全体像

図 1 に文献 [2] で提案した方式の全体像を示す。提案方式では、仮想化技術を用い、VM 上の AP が生成したログを VMM により取得する。(課題 1) へ対処するには、計算機外部へログを転送する必要がある。しかし、通常のプロセス間通信では、通信機能をカーネルが提供するため、カーネル内にマルウェアを挿入された場合に対処が難しい。そこで、VMM を用い、VM 上のログの送信を検知し、ログがカーネルへ到達する前にログを取得する。

提案方式では、ライブラリの置き換えにより、カーネル到達前に VM 外部へログを転送し、異なる VM 上で保

[†] 岡山大学大学院自然科学研究科, Graduate School of Natural Science and Technology, Okayama University

表1 提案方式の導入による syslog 関数の性能の変化

	処理時間 (μs)	オーバヘッド (μs (%))
Xen	31.47	—
提案方式	33.38	1.91 (6.08%)

存する。本稿における実装では、libcを置き換え、syslog関数にログの転送を依頼する命令を挿入した。置き換えたlibcのsyslog関数は、カーネルを介さずにVMMへログの転送を依頼する。これにより(課題1)へ対処できる。できるだけ早期にログを保護するには、(契機1)における対処が有効である。しかし、その場合、AP毎の対処となり、(課題2)への対処より工数が大きくなる。提案方式は、ライブラリの置き換えにより、ライブラリを用いたログの転送処理すべてに対応できるため、(課題2)へ対処できる。また、処理手順をできるだけ簡略化し、(課題3)へ対処している。置き換えたライブラリの完全性の保証は、文献[3]の手法の利用を想定している。

4. 評価

4.1. 目的と評価環境

提案方式では、APにおけるsyslog関数の呼び出しにおいてのみ、性能低下が起こる。本稿では、提案方式の導入によるsyslog関数とAPの性能への影響を評価する。APは、PostgreSQLを用いる。PostgreSQLは、データベース管理システムであり、I/O負荷が高い。本評価では、提案方式の導入によるI/O負荷が高いAPの処理性能への影響を評価する。これらの評価対象について、提案方式を導入していないXenと性能を比較する。

評価は、Core i7-2600 (3.40 GHz, 4コア)、16 GBメモリを搭載した計算機上で行なった。CPUのハイパースレッディングは無効にし、VMには仮想CPUを1ずつ割り当て、各仮想CPUは物理CPUコアに固定して割り当てた。これにより、同じ物理CPUコア上で走行するVM数の違いによる性能のばらつきを抑制する。

4.2. syslog 関数

表1に、syslog関数における測定結果を示す。提案方式は、syslog関数に挿入した命令を検知し、ログを取得するため、syslog関数の呼び出しでのみ性能が低下する。

表1より、syslog関数の呼び出し1回あたりの性能低下は、 $1.91\mu\text{s}$ であり、提案方式を導入していない場合の約94%の性能である。6%の性能低下は、性能が重視される環境では、問題になり得る。そこで、syslog関数の性能低下がAPの性能へ与える影響を調査した。thttpd Webサーバに同じページを100回リクエストした場合において、ライブラリ関数の呼び出し回数と処理時間を調査し、syslog関数が占める割合を調査した。調査には、ltraceコマンドを用いた。調査結果より、syslog関数の処理時間がリクエスト1回あたりの処理時間に占める割合は、約0.18%であり、syslog関数の性能が6%低下しても、その影響は十分小さいといえる。

4.3. PostgreSQL

pgbenchを用い、PostgreSQLにより1秒間に処理されたトランザクション数(TPS)を測定した。測定時の

表2 PostgreSQLにおける評価結果

tmpfs	VMM	TPS	相対性能
あり	Xen	1,448.80	—
	提案方式	1,372.60	0.95
なし	Xen	400.37	—
	提案方式	395.76	0.99

クライアント数は1とした。提案方式が性能に影響を与えるのは、syslog関数を用いた場合である。このため、測定では、1回のトランザクション毎に処理時間をログとしてsyslogへ出力するよう設定した。また、ディスクアクセスによる性能のばらつきを抑えるために、tmpfs上にファイルを作成し、性能を測定した。tmpfsはメモリ上にファイルを作成するため、ファイルアクセス時にディスクへアクセスしない。このため、ディスクのシーク待ち時間の差による性能のばらつきを抑制できる。また、処理時間に占めるCPU処理の割合が増加するため、CPU処理の性能への影響を評価できる。

表2に測定結果を示す。tmpfsを用いた場合の結果より、PostgreSQLにおけるCPUオーバヘッドは約5%である。これは、PostgreSQLにおいて、トランザクション処理の処理時間に対し、syslog関数の処理時間の占める割合が低いためである。測定結果より、提案方式がPostgreSQLの性能に与える影響は小さいといえる。

また、表2より、tmpfsを用いない場合には、I/O待ちによりCPUオーバヘッドが隠ぺいされるため、相対性能が向上している。PostgreSQLを実際に運用する際は、ディスクアクセスなどによりI/O待ちが生じる。このため、トランザクション毎の処理時間が増加する一方で、提案方式の導入による性能への影響は小さくなる。

PostgreSQLにおける評価では、提案方式の導入による性能低下は最大でも5%程度であり、運用方法によっては、更に小さくなる。

5. おわりに

ライブラリの置き換えによるVM外部への安全なログ転送方式におけるAPを用いた性能評価について述べた。性能評価より、提案方式の導入によるPostgreSQLの性能低下は0~5%程度であり、I/O処理を行なうAPの性能への影響が十分小さいことを示した。残された課題として、ライブラリの完全性を保証する機構の実現と評価がある。

参考文献

- [1] Sato, M. and Yamauchi, T.: VMM-Based Log-Tampering and Loss Detection Scheme, *Journal of Internet Technology*, Vol.13, No.4, pp.655-666 (2012).
- [2] 佐藤 将也, 山内 利宏: ライブラリの置き換えによるVM外部への安全なログ転送方式の提案, *情報処理学会研究報告*, Vol.2012-CSEC-59, No.6, pp.1-8 (2012).
- [3] Dewan, P., Durham, D., Khosravi, H., Long, M., Nagabhushan, G.: A Hypervisor-Based System for Protecting Software Runtime Memory and Persistent Storage, *Proc. 2008 Spring Simulation Multiconference (SpringSim '08)*, pp.828-835 (2008).