3F-3

セキュリティログ統合管理システム(3)
―時刻補正―

山田　将史　　村澤　靖
三菱電機株式会社

1．はじめに

複数の装置を含む大規模なシステムのセキュリティ監査などのセキュリティ運用の確認のためには、システム全体にわたるログの収集・蓄積が必要である。セキュリティ運用の確認時には、システム内におけるログの発生時刻の順序を把握できることが望ましい。ログ収集の際にログ発生時刻として記録される時刻は、通常ログを出力するプログラムが動作する機器で設定された時刻である。しかしながら、システム内の全ての機器間において時刻が一致しているとは限らない。例えば、通常の PC では、時刻精度が低く[1]、時間の経過とともに各端末間の時間差が拡がっていく。そこで、ログの収集・蓄積にあたり、機器からの収集ログ発生時刻順序を確保する技術が必要となる。本稿では、我々が開発したログ統合管理システム[2]の時刻補正機能について報告する。

2．従来技術と課題

本稿におけるセキュリティログ統合管理システムの全体構成図は図 1の通りである。ログ管理サーバと、ログ収集対象機器からなり、各機器にはログ取得エージェントと呼ばれるログ収集ソフトウェアが常駐している。

このシステムにおいて各ログ収集対象機器の時刻を一致させる一手法として、Network Time Protocol(以下 NTP)サーバを用いてシステム内の機器間の時刻を合わせ、収集ログの発生順序を確保する方法がある。しかしながら、入退室管理装置やデジタル複合機のように NTP サーバに対応していない機器がシステム内に含まれる場合や、NTP サーバを導入できない環境もあり、その場合各端末の時刻を一致させることは困難である。そのため NTP サーバを用いずに収集ログの順序性確保を実現する方法が求められる。

また、端末の時刻はユーザによって容易に変更することが可能である。機器の時刻が変更されることで、同一機器内での時刻変更直後のログと変更前のログに記録される発生時刻の順序が逆転するなど、ログの発生順序の一貫性が保たれなくなる。

そのため、機器の時刻変更が発生した場合にもログの順序性を確保する方法が求められる。

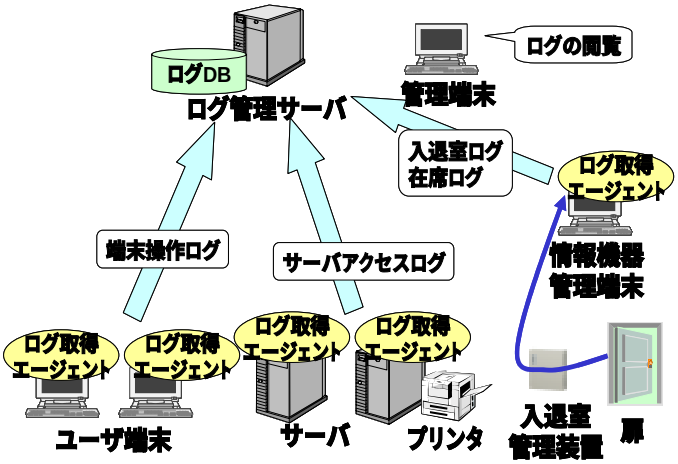

図 1　セキュリティログ統合管理システム全体図

3．解決策

NTP サーバを用いずに収集ログの順序性確保を実現するためのログ発生時刻の補正手段として次の二つ考えられる。

A)　システム内のある一台の時刻を基準としてシステム内機器の時刻を一致させる。

B)　ログ管理サーバとログ取得エージェントの時刻の差分を用いて発生時刻の補正時刻を生成する。

手段 A を用いた時刻の補正は、機器の時刻を直接変更するため、機器で動作する様々なアプリケーションに影響を与える恐れがある。手段 B は、機器側に時刻を問い合わせるだけで実際の時刻補正は管理サーバで行うので機器側に影響を与える可能性は低く、B を用いることとする。

手段 B において補正時刻を生成する方法には、ログ取得エージェント側の時刻をサーバ側に通

Security Log Management Systems(3)
Time Correction
Masafumi Yamada and Yasushi Murasawa
Mitsubishi Electric Corporation

知してサーバ側で補正値を生成する方法と、サーバ側の時刻をログ取得エージェント側に通知しログ取得エージェント側で補正値を生成する方法がある。

数千台規模の大規模システムにおけるログ収集では、サーバ側からの時刻を各機器に通知する際にネットワークトラフィックや、セキュリティ上の問題があるため、本システムでは前者の方式をとる。

機器の時刻変更が発生した場合にもログの順序性を確保するため、ログ取得エージェントが時刻変更を検知し、そのイベントと発生時刻をログ管理サーバに通知する。ログ管理サーバは、時刻変更のイベントを受けて、時刻変更時の補正処理を行う。

4．実現方式

本章において前章の解決法に基づく実現方式について述べる。

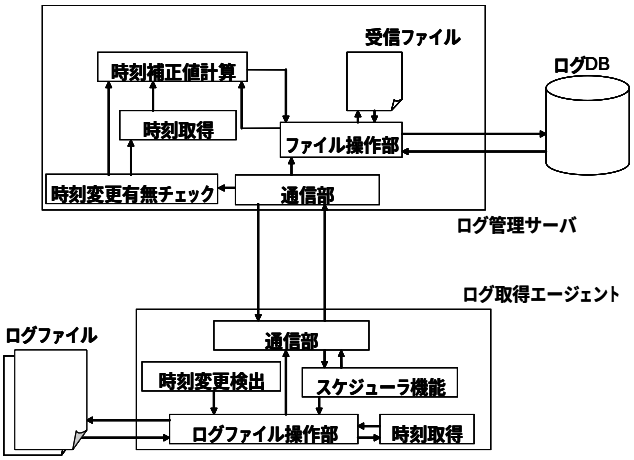

図 2　システム構成図

本提案のシステム構成図を図 2に示す。

ログ取得エージェント及びログ管理サーバは、ともに自身の時刻を取得する機能を持つ。また、ログ取得エージェントには時刻変更があったことを検知する機能を備える。これは、前述時刻変更に対応するための機能である。

次に提案システムの動作について述べる。

① ログ取得エージェントが起動すると、管理サーバはスケジュール情報などの情報を配布する。
② ログ取得エージェントは受け取った情報を元に設定時刻になるとログファイルを読み込む。
③ ログ取得エージェントはログ取得対象機器の時刻を取得し、送信時刻としてログファイルとともに転送する。
④ 管理サーバはログファイルを受信すると、自身の時刻を取得し受信時刻とする。
⑤ 送信時刻と受信時刻を元に時刻補正値を算出する。
⑥ 補正値を受信ログファイルとともに DB 投入する。

時刻補正情報はビューアで反映され、各機器から収集したログ情報は順序性を確保される。

課題点である時刻変更のイベントに関しては、次のように解決する。

① ログ取得エージェントの時刻変更検出機能で時刻変更イベントが検知される。
② 時刻変更を検知すると、スケジュールに関係なくログファイルを収集し、時刻変更があったことを示すフラグをログファイルとともに転送する。
③ 管理サーバ側はファイル受信の後、時刻変更の有無をチェックする。
④ 時刻変更により送られたログファイルであれば、前回算出した時刻補正値とともに DB 投入を行う。

以上の方法で、ログ収集対象機器の時刻変更時においてもログの発生時刻順序を確保することができる。

5．効果

ログ転送時にログ取得エージェント側の送信時刻と、管理サーバ側の受信時刻とを用いて、発生時刻の補正値を生成することでログの発生時刻順序性の確保を可能とした。また、ログ取得エージェント側機器の時刻が変更されたことを検知する仕組みを導入することで、時刻変更による発生時刻の順序性を崩すことなくログを収集することが可能となった。ログビューアで、ログ内の発生時刻と補正値との和に基づいてログを表示することにより、NTP サーバなどの時刻同期システムを導入せずに収集ログの発生時刻順序性の確保を可能とした。

6．終わりに

ログの順序性を確保したログ統合管理システムの開発を行った。これによって、大規模なセキュリティ運用の確認時にも収集ログの発生順序を把握できる。

7．参考文献

[1] 北口　他，PC における時刻精度の精密計測とその評価．電子情報通信学会ネットワークシステム研究会 (Vol.NS2003)，No.160，pp.67-70 2003
[2] 樋口　他、”情報セキュリティサービス(1)-ログ統合-”，第６７回情報処理全国,A4-4，Mar.2006