3F-1

セキュリティログ統合管理システム(1)
–大規模ログ収集–

樋口 毅　　村澤 靖　　相浦利治
三菱電機株式会社

1. はじめに

2005 年 4 月に施行された個人情報保護法により、企業における情報漏洩対策に関する重要性が認識されている。

情報流出事故が発生した場合の損失は、７億円以上と推定[1]されており、端末上の操作ログ、サーバへのアクセスログ、入退室管理装置などの機器のログ等、システムを構成する各種機器からセキュリティログを収集し、管理することが必要となってきている。

こういった背景から、我々は、ログの収集・統合管理を行うログ管理システムの開発を行ってきた[2][3]。本稿では、ログの収集を実施するログ管理サーバの性能特性を分析し、ログ収集要件に応じたログ管理サーバの台数の見積りを可能とした大規模ログ収集について報告する。

2. 課題

ログ収集を行う場合、目的や収集対象のログの種類により、ログ収集の要件が異なる。例えば、大量のログを保存することができない機器などの場合、短い周期でログの収集を実施したいという要求が考えられる。また、サーバなどのように１日１回、業務に影響のない時間帯にログ収集を実施したいという要求もある。

これらの機器やサーバが混在するシステムでログ収集を実施する場合、１回に送信されてくるログの量の変化が大きくなる。通常、一括処理の方が余分なオーバヘッドが少なく、高速に処理ができることから、１回に送信されてくるログの量により、処理可能なトータルのログの量は変化することになる。

このため、ログ収集の要件に応じ、１台のログ管理サーバでの処理可能なログの量を見積もることができなければ、安全を見越して、必要以上のログ管理サーバの設置を行う可能性があるという課題があった。

我々は、本課題を解決したセキュリティログ統合管理システムの開発を実施した。

Security Log Management System (1)
Management of Large Scale Log Collection
Tsuyoshi Higuchi, Yasushi Murasawa, and Toshiharu Aiura
Mitsubishi Electric Corporation.

3. システム構成

セキュリティログ統合管理システムの構成を図 1 に示す。

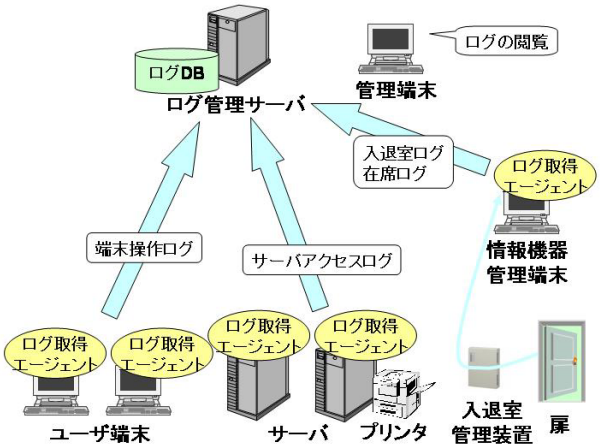

図 1：システム構成

セキュリティログ統合管理システムは、収集対象のログへのアクセスが可能なユーザ端末やサーバ上で動作し、ログ取得を行うログ取得エージェントと、取得されたログを収集し、蓄積するログ管理サーバから構成される。

ログの収集は、ログ取得エージェントに配布されているログ取得のタイミングが記録されているスケジュール情報に基づき実施される。スケジュール情報は、ログ管理サーバ上で管理され、ログ取得エージェントからの定期的なポーリングにより、各ログ取得エージェントに配布される。

4. 解決策

ログ収集要件に応じたログ管理サーバの台数の見積りを可能とするための解決策を示す。

4.1. 性能特性の明確化

ログ管理サーバは、ログを収集し、収集したログを DB に格納する処理を実施するため、DB に格納する処理が性能面でのボトルネックとなる。

DB に格納可能なレコード数は、１回のログ収集時のレコード数に影響を受ける。1,000 レコードを格納する場合であっても、1 レコードのログ格納を 1,000 回実施するのに対し、1,000 レコードのログ格納を１回実施する方が高速に処理可能である。

このことから、１回のログ格納時のレコード数と処理可能件数の測定を行い、ログ管理サーバの

性能特性の明確化を実施した。

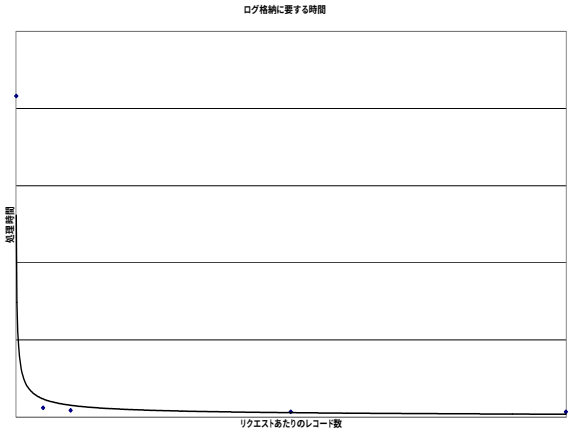

図 2：性能測定結果

性能測定結果を示した図 2の関係は、１リクエストあたりのレコード数と単位時間当たりの処理レコード数の関係にて近似することが可能である。

この関係をログ管理サーバの性能特性とし、１リクエストあたりのレコード数により、ログ管理サーバの必要台数の見積もりを可能とした。

4.2. ログ管理サーバの実現方式

ログ管理サーバは、ログ収集スケジュール取得のためのポーリング受付などログ収集以外の処理も実施することになる。また、ログ収集のリクエストが集中することによるオーバヘッドが発生し、処理性能を落とすことが考えられる。このため、以下の方式にてログ管理サーバを実現する。

- DB 格納処理の高速化

本ログ管理サーバは、コンポーネント指向ログ収集・統合管理により、DB へのログの格納などの機能をコンポーネントとして管理していた。この方式の場合、ログ収集のタイミングでコンポーネントを起動する動作となる。今回、DB へのログの格納処理をコンポーネント管理部の内部機能として、常駐化させることにより、コネクションプールの利用やコンポーネント起動負荷の低減を実現する。

- ログ収集スケジュールの自動分散

ログ取得エージェントからのログ収集が集中した場合、ログ管理サーバの負荷が上がり、ログの格納の失敗などが発生する。ログ管理サーバの負荷の平準化を実現するため、１日のトータルのログ送信回数から単位時間当たりのログ送信回数を決定する。この単位時間当たりのログ送信回数に基づき、ログ収集スケジュールを動的に変更し、ログ取得エージェントに配布することにより、ログ収集スケジュールの自動分散を実現する。

- 処理の優先度制御

ログ取得エージェントからのログ収集スケジュール取得のための定期的なポーリングとログ送信が多数重なった場合には、ポーリングに対する処理を制限し、ログ収集ならびに DB へのログの格納処理を優先させる。

5. 評価

ログ収集対象マシンごとに異なる、台数、ログ収集頻度、１回のログ収集にて送信されるレコード数の要件を定義する。

表 1：要件

ログ収集対象マシン	台数(台)	単位期間当たりの収集回数	送信レコード数
ユーザ端末	m_1	c_1	r_1
OA サーバ	m_2	c_2	r_2
入退室管理装置	m_3	c_3	r_3

要件から、１リクエストあたりの収集レコード数(R_a)は以下のように加重平均により計算することが可能となる。

$$R_a = \sum_{i=1}^{n} m_i c_i r_i \Big/ \sum_{i=1}^{n} m_i c_i$$

表 1に示した要件の場合、n=3 にて計算を実施し、計算によって求められた１リクエストあたりの収集レコード数とログ管理サーバの性能特性から導き出される１リクエストあたりの収集レコード数を比較する。比較した結果、要件を基にした計算値が、性能特性の値を下回っている場合には、１台のログ管理サーバにて対応が可能であると判断でき、必要なログ管理サーバの台数の見積りを実施できることを確認した。

6. おわりに

ログ収集要件に応じたログ管理サーバの台数の見積りを可能とするため、ログ管理サーバの性能特性を明確にした。

この性能特性を用いて、ログ収集要件から求められる収集対象のマシンの台数、単位期間あたりの収集回数、送信レコード数の情報から得られる１リクエストあたりの収集レコード数を基に、必要なログ管理サーバの台数の見積りが可能であることを確認した。

参考文献

[1] JNSA,“2005 年度個人情報漏洩インシデント調査結果”

[2] 樋口他,“情報漏洩防止ソリューション(4)-ログ収集管理-”,情報処理学会第 67 回全国大会,3A-7,2005

[3] 樋口他,“情報セキュリティサービス(1)-ログ統合管理-”,情報処理学会第 68 回全国大会,4A-4,2006