4A-4

情報セキュリティサービス(1)
–ログ統合管理–

樋口 毅† 村澤 靖† 村田 篤†
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。情報流出事故などが発生した際の原因追及や、情報漏洩対策が正しく運用されていることの証明に各種アプリケーションや OS が出力するアクセスログや操作ログが利用されている。

我々は、情報漏洩防止ソリューションにてログの収集管理を行うアーキテクチャを設計し、ログ収集管理システムの開発を行った[1]。

ログ収集管理システムでは、ログ取得や送信を行うための処理をコンポーネントとして登録することにより、ログの収集・統合管理を実現可能としている。本稿では、ログの統合を実現するための共通化の処理を行うコンポーネントにより実現したログ統合管理システム開発について報告する。

2. 課題

アプリケーションや OS は多種多様であり、企業にとって守りたい対象に合わせてログの出力設定の実施が行なわれることになる。これらのアプリケーションや OS が出力するログは、通常個別に管理されている。そのため、ユーザが実施したログオンや印刷などの一連の行為を一元的に管理することができない。

ログの一元管理を実現するために、各種ログの構成を共通化することにより、事故が発生した場合の原因追求や運用状況の確認を行うことが可能となる。

しかし、単に各種ログの取得処理の際に、共通の構成に変換する方式にて実装した場合、新規アプリケーションの導入やログを利用するサービスが変更になった場合に、以下の課題がある。

- 新規アプリケーションが導入された場合、そのアプリケーションが出力するログを取得する処理にて取得したログを共通構成に変換するための処理を実装する必要がある。
- ログを利用するサービスが変更になった場合、共通構成が変更になる可能性があり、その変更をすべてのログ取得処理に実施する必要がある。

Information Security Service (1) – Integrated Log Management –
† Tsuyoshi Higuchi, Yasushi Murasawa and Atsushi Murata
Mitsubishi Electric Corporation.

我々は、これらの課題を解決したログ統合管理システムの開発を実施した。以下に開発したログ統合管理システムの内容を示す。

3. システム構成

ログ統合管理システムの構成を図 1に示す。

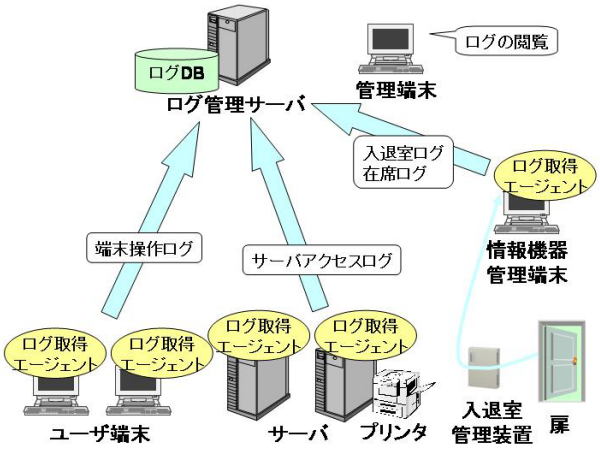

図 1：システム構成

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、ログ管理サーバ上で管理されているスケジュール情報に従い実施される。スケジュール情報には、収集するログの種類、収集するタイミング、収集や蓄積を行うために必要なコンポーネントの種類が登録されている。

4. 実現方式

今回開発したログ統合管理システムは、ログの統合を実現するための共通化の処理を行うコンポーネントを開発することで実現した。

アプリケーションや OS が出力するログの保存形式は以下の 2 種類に分類される。

表 1：ログ保存形式

ログ保存形式	例
バイナリ形式	Windows イベントログや DB に格納されたログ
テキスト形式	Apache が出力するアクセスログなど

それぞれの保存形式ごとに以下の方式にて実現

した。

表 2：ログ保存形式とその共通化実現方式

ログ形式	バイナリ形式	テキスト形式
ログ取得部	バイナリログ取得 I/F を利用したログ取得。	ファイル I/F を利用したログ取得。
	取得したログを共通のログ保存形式に変換。	
ログ構成共通化部	ログの種類に応じた設定ファイルの指定により、共通構成のログに変換。	

ログ取得部をエージェント側、ログ構成共通化部をログ管理サーバ上で実現する構成とした。

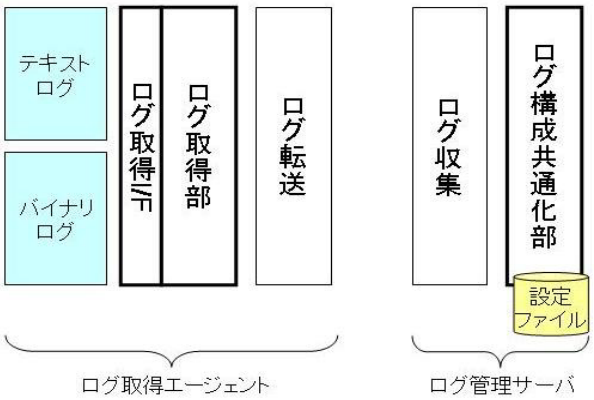

図 2：共通化実現構成

本構成により、2章に示した課題を解決した。

- 各ログ固有の保存形式の違いをエージェント側で吸収し、共通の保存形式のログとして扱うようにした。これにより、新規に収集対象のログを追加する際、統合化に必要な共通の構成を意識することなく、ログ取得を実施し、共通のログ保存形式に変換するのみでよい。
- ログの共通構成への変換をログ管理サーバ側で吸収した。これにより、共通構成の変更が発生した場合、ログ構成共通化部にて使用する設定ファイルの変更のみで対応が可能となる。

5. 評価

本ログ統合管理システムにより、テキスト形式とバイナリ形式のログの統合化の評価を行った。

表 3：共通構成例

カラム	内容
1	年月日
2	時間
3	マシン名
4	ユーザ名
5	読み取り情報
6	書き込み情報
7	アクセス内容
8	接続相手

ログの共通構成は表 3のように定義した。

テキスト形式のログとして Web サーバのアクセスログとして Apache の access.log を利用した。デフォルト設定時に acces.log に出力される内容は以下の通りである。

```
192.168.1.11 - - [21/Dec/2005:12:02:31 +0900] "GET /apache_pb.gif HTTP/1.1" 200 2326
```

バイナリ形式のログとしてイベントログを使用した。イベントログに出力される内容は以下の通りである。

日付	2005/12/21
時刻	12:1:30
種類	情報
ユーザー	testuser
コンピューター	Client1
ソース	MsInstaller
分類	なし
イベント ID	11707
説明	”Product: WMI Tools – Installation operation completed successfully.”

これらのログを表 3に示したログの共通構成に統合化することにより、以下のようにアクセス内容を同じカラムで確認することが可能となる。

内容	イベントログ	Web サーバ
年月日	20051221	20051221
時間	120130	120231
マシン名	Client1	
ユーザ名	testuser	-
読み取り情報		
書き込み情報		200
アクセス内容	”Product: WMI Tools – Installation operation completed successfully.”	"GET /apache_pb.gif HTTP/1.1"
接続相手		192.168.1.11

以上のように、各種ログ取得部の開発と対応した設定ファイルの定義により、テキスト形式である Web サーバのアクセスログとバイナリ形式であるイベントログの内容を共通構成に変換し、統合化を実現できることを確認した。

6. おわりに

多種多様なログを統合化するためのログ構成の共通化を実現する方式の検討を行い、ログ統合管理システムを開発した。本ログ統合管理システムの評価を行い、新規収集対象のログの追加や共通構成の変更に対応可能であることを確認した。

参考文献

[1] 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