3A-7

情報漏洩防止ソリューション(4)
–ログ収集管理–

樋口 毅† 菅野 幹人† 村田 篤† 近藤 誠一† 遠藤 淳‡
三菱電機株式会社† 三菱電機インフォメーションシステムズ株式会社‡

1. はじめに

情報漏洩防止ソリューションは、情報システムのセキュリティ対策と入退室管理システムを統合し、機密情報の漏洩などを防止するものである。ログ収集管理は、情報漏洩防止ソリューションにおいて出力される各種セキュリティログの収集、統合管理を行うものである。

従来のログ収集管理は、システム毎に個別に特化した目的で端末やサーバからログを収集管理するものとなっている。

しかし、端末と異なり、入退室管理装置などログ取得機能の導入ができない専用の情報機器からのログ収集ができない、システムごとに異なる収集対象のログの統合ができない等の課題があった。

これらの課題に対して、我々はコンポーネント指向ログ収集・統合管理アーキテクチャを設計し、ログ管理システムの開発を行った。

本ログ管理システムによって、上記の課題を解決し、情報セキュリティマネジメントシステム(ISMS)[1]対応の運用などが可能となった。

2. 現状と課題

従来のログ管理システムは、システム毎に個別に特化した目的で端末やサーバからログを収集・管理するものであり、各拠点内のログの収集に対応したものである。従って、以下の課題がある。

- ログ取得機能の導入ができない情報機器からのログ収集やシステムに固有のフォーマットが異なるログの統合管理を行うことができない。
- イントラネットの拠点を越えたログの取得などを行う場合、システムによってファイアウォールやプロキシを経由したログ収集を行う必要があるが、それらに対応していない。
- 多数の情報機器からログを収集する際、収集タイミングが集中した場合に、ネットワークの負荷が上がり、業務への影響が発生する。

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

Information Leak Prevention Solution (4) – Management of Log Collection –
† Tsuyoshi Higuchi, Mikihito Kanno, Atsushi Murata and Seiichi Kondo
Mitsubishi Electric Corporation.
‡ Jun Endo
Mitsubishi Electric Information Systems Corporation.

3. システム構成

ログ管理システムの構成を図 1に示す。

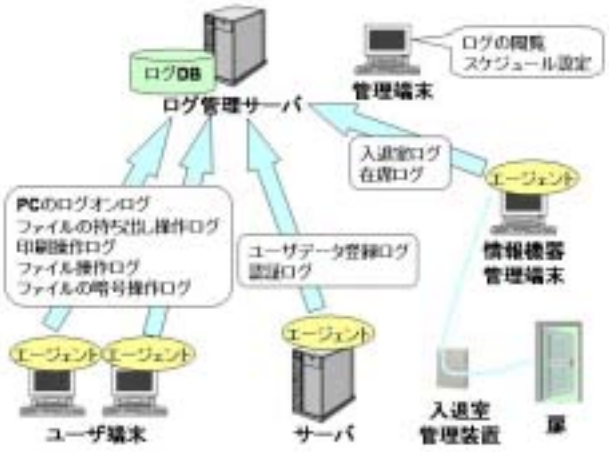

図 1：システム構成

ログ管理システムは、ログ収集対象の端末やサーバ上にログファイルを取得するログ取得機能を実現するエージェントを導入し、ログの収集、統合管理を実現する。エージェントで取得するログの種類やスケジュール、ログ収集ロジックはスケジュール情報としてログ管理サーバ上で管理する。

各エージェントは、このスケジュール情報をログ管理サーバより取得し、スケジュール情報に基づきログの取得、送信を行う。

ログ管理サーバは、エージェントから送信されたログを収集し、ログ DB に収集ログを蓄積する。

4. 実現方式

今回開発したログ管理システムは前述の課題を解決するために以下の実現方式にて実装した。

- コンポーネント指向ログ収集・統合管理
- HTTP(S)プロトコルによるログ収集
- ログ収集スケジュールの集中管理

4.1. コンポーネント指向ログ収集・統合管理

対象となるログを取得する手段は、情報機器によって異なる。例えば、本ログ管理システムにてログを取得している入退室管理装置などはエージェントを導入することができない。また、収集したいログはシステムごとに異なり、そのフォーマットは異なる。

これらの課題に対応するため、システムに依存するログ取得やフォーマット変換などのコンポー

ネントとそれらのコンポーネントを制御するロジックを分離することとした。アーキテクチャを図 2 に示す。

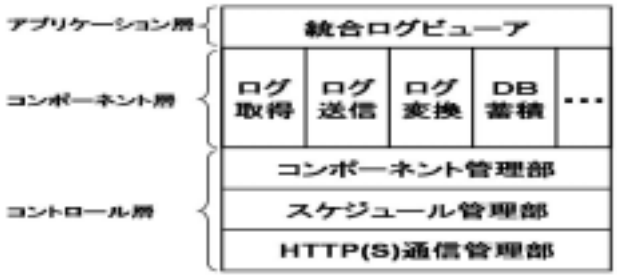

図 2：アーキテクチャ

本アーキテクチャは、アプリケーション層、コンポーネント層、コントロール層から構成される。

アプリケーション層は、収集されたログや I/F を利用して開発されたアプリケーション群である。

コンポーネント層は、システムに依存するログ取得やログ変換などの処理を行う各コンポーネントから構成される。コンポーネントは、システムごとに追加・削除・変更することを可能としており、ユーザがシステム対応にて開発したコンポーネントの登録、実行が可能である。

コントロール層は、以下で構成される。

コンポーネント管理部	スケジュール情報に記述されたログ収集ロジックに従い、対応コンポーネントの実行を制御
スケジュール管理部	スケジュール情報に記述されたスケジュール情報を基に、ログ収集ロジックの実行時間の管理
HTTP(S)通信管理部	収集したログの転送を実施する通信処理の管理

本アーキテクチャにより、入退室管理装置などエージェントが導入できない情報機器からの情報取得は、以下のステップにて情報機器管理端末が情報機器の代理でログ取得、送信を実施することが可能となる。

(1) 情報機器管理端末上にエージェントを導入
(2) 情報機器からの情報取得コンポーネントの登録
(3) 収集管理ロジックの設定

同様に、独自のフォーマットのログファイルを収集する場合には、統一フォーマットに変換するコンポーネントの登録により可能となる。

4.2. HTTP(S)プロトコルによるログ収集

システムごとに異なるネットワーク構成に対応可能にするため、スケジュール情報やログの転送の際のエージェントとログ管理サーバとの間の通信は HTTP(S)を利用した。これらの通信はすべて、エージェント主導で実現し、ログファイルは標準フォーマットに変換して転送する方式とした。

この方式により、以下が可能となる。

- エージェント側は特別なサービスポートを開く必要がなくなるため、システムのセキュリティポリシーへの対応が可能
- ログ管理サーバと監視対象の間に F/W やプロキシがあるなど、システムごとに異なるネットワーク構成への対応が可能
- 転送対象のファイルのフォーマットに依存せず、バイナリファイルなどの転送が可能

4.3. ログ収集スケジュールの集中管理

多数のエージェントから同時にログ送信が行われた場合、ネットワークの負荷が上がり業務への影響が発生することが考えられる。

本課題を解決するために、ログ管理サーバ上でログ収集スケジュールを集中管理し、ログ収集の多重度が高いスケジュールが検出された際には、動的にスケジュールを変更し、変更したスケジュールを各エージェントに配布する方式とした。

スケジュールの集中管理を行うことにより、多重通信が発生する時間や多重度が管理可能となり、対象となるエージェントとスケジュールの組み合わせに対してのみ、多重度に応じたスケジュールの動的変更を実施することが可能となる。

さらに、管理者は同時に実行されるエージェント数の数を意識することなく、単にエージェント上で収集したいログの設定を実施するのみでよくなり、設定の容易性を実現することが可能となる。

例えば、1000 台の端末から、10KB のログを同時に転送した場合、10MB のデータ転送が発生し、100Mbps の LAN 環境の場合、50%以上のネットワーク使用率となる。同時転送端末数を動的に 50 台とすることにより、ネットワーク使用率が 10%以下となり、業務への影響が抑えられる。

5. 効果

本ログ管理システムにより、ログの統合管理が実現され、セキュリティ管理の実施を証明することが可能となり、ISMS 対応の運用が可能となる。さらに、情報漏洩が発生した場合であっても、認証履歴や操作履歴の統合管理が行われているため、ユーザごとの操作やファイルごとの操作の履歴管理が可能となり、問題の特定が可能となる。

6. おわりに

情報機器からのログ収集、システムごとに異なるログのフォーマットやネットワーク構成への対応、スケジュール集中時の業務への影響などの課題を、コンポーネント指向ログ収集・統合管理アーキテクチャ、HTTP(S)プロトコルの利用、スケジュールの集中管理方式により実現したログ管理システムにて解決した。

参考文献

[1] 情報セキュリティマネジメントシステム(ISMS)適合性評価制度
http://www.isms.jipdec.jp/