

D-034

入退管理・映像監視システム向け統合ログ管理方式 Integrated Log Management Method for Access Control and CCTV Security Systems

山岸 義徳[†]
Yoshinori Yamagishi

郡 光則[†]
Mitsunori Kori

1. はじめに

近年、機密情報や個人情報などのセキュリティ管理意識の高まりを背景に、入退管理・映像監視システムが出力する入退室ログと映像データを関連づけて一元管理し、事件・事故発生時の原因究明や不審者の調査などを効率的に行う統合ログ管理システムが求められている。

しかし、入退室ログや映像データは従来、各システムで個別に管理されることが多く、事件・事故の原因究明や追跡調査に時間を要するという課題があった。

この課題解決のため、入退室ログのレコード（以降、イベント）から関連づく映像データのスナップショット画像（以降、画像）を算出し、イベントと画像とを関連づけて保存する統合ログ管理システム（図 1）を開発した。この統合ログ管理システムの実現方式について報告する。

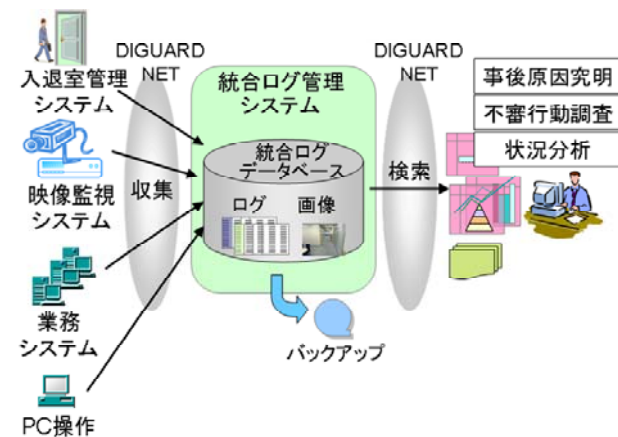


図 1 統合ログ管理システムの概念

2. システム要件

統合ログ管理システムのシステム要件を説明する。

2.1 収集・蓄積

入退管理システムと映像監視システムを対象に、各システムからそれぞれ収集したイベントと画像を関連づけて蓄積し、一元管理することが求められている。

2.2 検索

大規模システムでは、ログの蓄積容量は年間数十テラバイトにも及ぶ事例がある。これら大量のデータの中から事件・事故の迅速な原因究明・調査を行なうため、イベントと画像を連携した高速な検索が求められている。

2.3 運用管理

単に大規模ストレージを備えるだけでなく、日々蓄積・保存される大量のイベントや画像を日単位や週単位など任意の期間でバックアップ/リストア、削除など、効率的な運用管理が求められている。

3. システム構成

図 2 に統合ログ管理システムと入退管理・映像監視システムの構成を示す。

統合ログ管理システムは統合ログ管理サーバと統合ログデータベースからなる。また、入退管理システムは、認証装置、電気錠（扉）、電気錠制御盤からなる。さらに映像監視システムは、扉付近を撮影する監視カメラと映像レコーダからなる。各システムは LAN により接続されている。

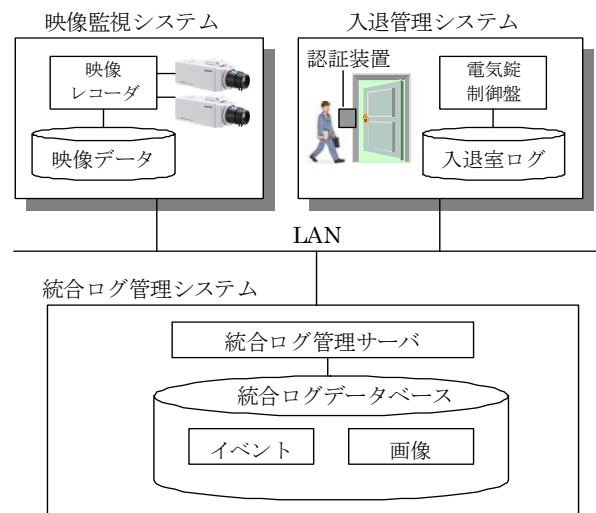


図 2 システム構成

4. 機能

統合ログ管理サーバが実現する収集・蓄積機能、検索機能、運用管理機能について説明する。

4.1 収集・蓄積機能

統合ログ管理サーバは、入退管理・映像監視システムからイベントと画像を収集し、イベントの時刻や機器 ID など関連づけて統合ログデータベースに蓄積する。

4.2 検索機能

特定の時刻、人物、場所などを条件に統合ログデータベースから関連するイベントと画像を高速に検索し、結果を表示・出力する。

[†] 三菱電機（株）情報技術総合研究所、
Mitsubishi Electric Corp.
Information Technology R&D Center

4.3 運用管理機能

イベントや画像を時系列的な“範囲”で管理し、任意のタイミングで範囲を追加・削除できる。また、範囲を単位としたバックアップ/リストアが可能である。

5. 統合ログ管理方式

イベントと画像の関連づけモデルと、入退管理・映像監視システムへの適用について説明する。

5.1 イベントと画像の関連づけモデル

図 3に示すように、一般的にイベントと画像は 1 対多の関係にある。この関係は、イベントや画像を生成する機器のレイアウト情報や画像取得条件によって決まる。

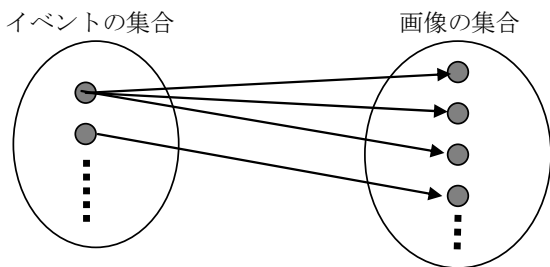


図 3 イベントと画像の関係

ここでは、イベントの発生時刻 t とイベントの属性項目 a から写像 f によって算出される画像取得時刻の集合 Y を次の式(1)で定義する。

$$Y = f(t, a) \dots\dots (1)$$

5.2 入退管理・映像監視システムへの適用

イベントと画像を関連づけるため、まず入退室ログ(表 1)のイベントから扉付近を撮影する監視カメラを決定する。次にその監視カメラが接続された映像レコーダから関連する画像を時刻により特定する必要がある。

表 1 入退室ログの例

発生時刻(t)	扉番号(a)	状態	ユーザ ID
2008/01/01 12:20:11.021	2	警戒	0001001
2008/01/01 14:13:08.001	1	入室	0001002
2008/01/01 14:55:32.240	3	不正操作	0002011

この実現のため、写像 f として機器のレイアウト情報を加味した画像取得条件テーブルを定義した(表 2)。ここで、扉番号 1 の扉はRecorder1 に接続された 2 台の監視カメラ(監視カメラID=1, 2)に対応し、それぞれの映像データの中からイベントの発生時刻 t を基準に 4 枚(1+3)の画像を取得してイベントと関連づけることを意味する。このように、イベントの発生時刻 t と扉番号 a から画像取得条件テーブル f によりイベントに関連づく画像の集合 Y を特定する。

表 2 画像取得条件テーブル

扉番号(a)	監視カメラID	映像レコーダ	画像取得時刻
1	1	Recorder1	t
1	2	Recorder1	$t-1, t, t+1$
2	3	Recorder2	$t-2, t-1, t, t+1, t+2$
:	:	:	:

6. 実現方式

統合ログ管理サーバの実現方式について説明する。入退室ログと画像の保存・検索プラットフォームとしてログ専用データベース管理システム[1](LDB)を利用した。LDBは画像を含む多様な形式のログに対応し、かつ SISA[2]技術により数十テラバイトのログにも対応可能なスケーラビリティを有する。

6.1 ソフトウェア構成

図 4に統合ログ管理サーバのソフトウェア構成を示す。

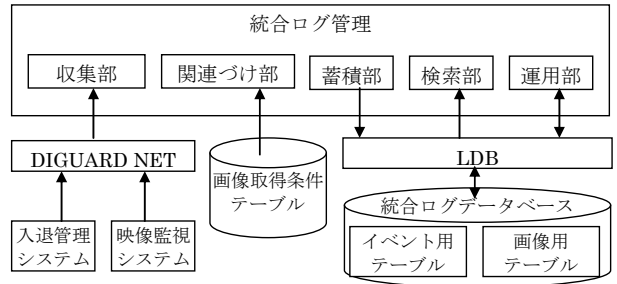


図 4 ソフトウェア構成

6.2 処理

6.2.1 収集・蓄積(収集部、関連づけ部、蓄積部)

- (1) 当社セキュリティ機器を共通プロトコルで扱えるセキュリティ構築プラットフォーム DIGUARD NET[3]を介して、入退管理システムから入退室ログを収集する。
- (2) 入退室ログのイベントに関連づく画像を画像取得条件テーブルから算出し、DIGUARD NET を介して映像監視システムから画像を取得する。
- (3) 収集したイベントと画像を時刻や機器 ID で関連づけて統合ログデータベースのイベント用テーブル、画像用テーブルに蓄積する。

6.2.2 検索(検索部)

- (1) イベントに関する検索条件を入力し、イベント用テーブルから該当するイベントを抽出する。
- (2) 抽出したイベントから時刻や機器 ID を条件に関連づく画像を抽出し、イベントとともに表示・出力する。

6.2.3 運用(運用部)

- (1) 追加・削除などの範囲の管理はファイル内の区切られた領域をスパースファイル機能によって実現する。
- (2) 範囲単位のバックアップ/リストアは、特定の範囲データを対象にしたファイル入出力により実現する。

7. むすび

入退室ログのイベントから関連づく映像データの画像を算出し、イベントと画像とを関連づけて保存する統合ログ管理システムを開発し、その有効性を確認した。

参考文献

[1] 中村 他、大規模ログデータベースの実現、情処学会第 68 回全国大会、1D-2 (2006).
 [2] 郡 他、検索機能を備えたストレージシステムによる大規模並列全文検索、信学技報、Vol.102、No.276、pp.41-46 (2002).
 [3] 笹川 他、セキュリティ構築プラットフォーム“DIGUARD NET”、三菱電機技報、2008年4月号(2008).