# インタラクティブに要約方法を定義可能なログブラウザ

6X−06

西田 簿　中山 健　笛木 規雄　小林 良岳　前川 守
電気通信大学大学院 情報システム学研究科

## 1　はじめに

計算機システムのログには、障害情報や稼動状況など種々の情報が記録されている。システム管理や障害対応では、大量の各種ログを総合して的確な状況判断を行なわなければならない。さらに、障害対応を専門に行うサポート部隊の場合、スーパーコンピュータからプリンタなどの周辺機器に至る多くの機種のログを解析しなければならない。このため、ログを理解し易く提示する必要がある。

そこで、主としてメインフレーム計算機で用いられている1つの障害が1つのファイル（図1）に書き込まれている形式のログを対象として、ログの内容を見ながらインタラクティブに要約方法を指定・変更できるログブラウザDEISUM-Bを作成した。本システムでは、ログの内容を見ながら要約方法を指定・変更することができる。これによりシステムに精通していないシステム管理者でも容易に要約方法を指定することができる。また、既存の要約方法を編集し、新規の要約方法を作成することにより、独自の要約方法を作成することができる。システム管理者が行った要約方法の履歴はマクロ化され、このマクロを組み合わせることにより、様々な角度から要約方法の評価を行うことができる。

尚、DEISUM-Bはログ情報調査作業支援「見えログ」が行う注目すべきログであることを示す単語の指定は行わず、システム管理者が理解し易い要約を作成する要約方法の指定を行う。

## 2　ログの要約

要約方法とは、大量のログから求めるログを検索し、検索されたログに対し要約を指定する作業を指す。

独自スクリプトを用いてログの検索を行う場合、十分な知識と経験をもっていなければ検索条件の指定が難しい。要約はシステム管理者の熟練度や好みにばらつきがあり、しかも同じログを見る場合でも目的によって適した提示形式が異なる。熟練度の高いシステム管理者は、必要な情報だけの簡潔な要約を望む傾向が強いのに対し、熟練度の低いシステム管理者は、理解を助ける付加情報も提示を求める声が多い。また、OSやアプリケーションに依存し、同じ内容を表すログでも生成元によって出力形式が異なる。

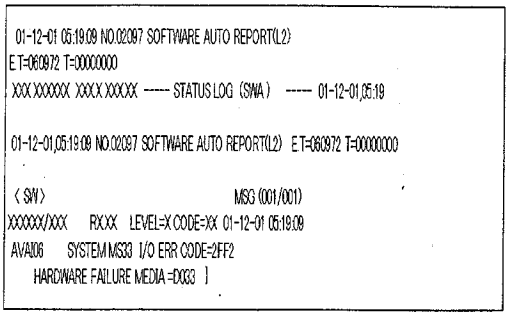


図 1: 障害ログの例

そこで、DEISUM-Bでは以下の機能を提供する。

- 検索文字列をログから指定し検索
- 個々でログから要約に含める部分の指定・変更

## 3　DEISUM-Bの概要

### 3.1　要約方法の指定

DEISUM-Bでログを開くと、要約方法定義画面（図2）の左半分にログの内容が表示される。要約に含めたい部分の文字列 $S_1$ と，要約に含めたい部分の位置を特定するための部分の文字列 $C$ を選択し">"ボタンを押すと、その部分が、右上の要約表示領域に表示される。この際、システム内部では次の項目が記録される。(1) ログの先頭1バイト目から $C$ までの文字列長 $d_1$ (2)$C$ の文字列 (3)$C$ と $S_1$ との間の文字列長 $d_2$ (4)$S_1$ の文字列長 $d_3$

### 3.2　要約方法の適用による要約作成

このように作成された要約方法は、次の手順でログに適用され、要約が生成される。

① 要約対象のログの、先頭から $d_1$ 文字目の近傍で $C$ を検索する。

② $C$ が見つかった場合は、その位置から $d_2$ 文字後の位置から $d_3$ だけの文字列を抽出し要約とする。

An Interactively Customizable System-Log Browser
Susuki Nishida, Ken Nakayama, Norio Fueki,
Yoshitake Kobayashi, Mamoru Maekawa
Graduate School of Information Systems, University of Electro-Communications 1-5-1 Chofugaoka, Chofu-shi, Tokyo 182-8585, Japan

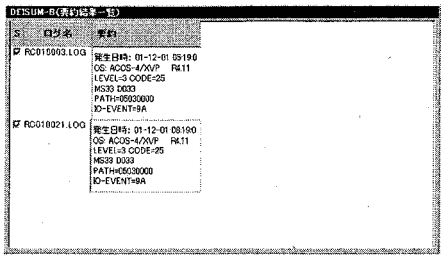


図 2: 要約方法定義画面

もし、$C$ が見つからなかった場合は、要約失敗とする。

### 3.3 要約方法の組み合わせ

要約方法をログに適用すると、要約結果一覧画面(図 3) に要約が表示される。表示された要約のログに対し要約方法を再度指定することにより、同一のログから異なる要約を得ることができる。尚、要約の内容を基にログを選択する場合は、要約から検索したい部分の文字列 $S_2$ を指定する。この際、システム内部では、要約の先頭 1 バイト目から $S_2$ までの文字列長 $d_4$ 文字後に $S_2$ が記述されているログを要約方法の対象とする。

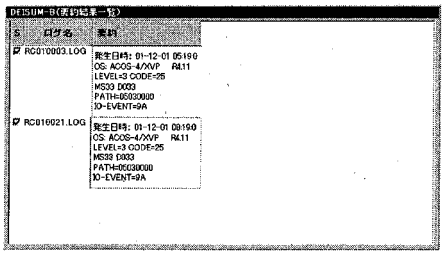


図 3: 要約結果一覧画面

### 3.4 ログの検索

#### 共通部分によるログの判別と検索

ログを構成する文字列を比較し、ログ全体の文字列に対して共通部分が占める割合から同一内容のログであるか判断を行う。尚、判断する割合は任意である。任意のディレクトリ配下にあるログに対して共通部分によるログの判別を行った場合、共通部分が指定された割合を満たすログをグループ単位に管理する。また、任意のログを基に共通部分によるログの検索を行った場合、指定されたログと比較して共通部分が指定された割合を満たすログを検索する。

#### 文字列によるログの検索

ログの内容から検索対象とする文字列を指定し、指定された条件を満たすログを検索する。尚、下記の検索内容とオプションを組み合わせることが可能である。

- 検索内容
  - 指定された文字列を含むログを検索
  - 指定された位置に指定された文字列を含むログを検索
- オプション
  - 大文字／小文字の区別指定
  - 16 進数変換の区別指定

#### 文字属性によるログの検索

ログの内容から検索対象とする文字列を指定し、指定された条件を満たすログを検索する。その際、検索対象の文字列及びログの各文字列をアルファベットなら a, 数字なら 9, それ以外の文字列はそのままの文字に置き換え検索を行う。尚、下記の検索内容と文字列によるログの検索で指定したオプションを組み合せることが可能である。

- 検索内容
  - 指定された文字属性を含むログを検索
  - 指定された位置に指定された文字属性を含むログを検索

## 4 まとめ

本研究では、システム管理者がログの内容を見ながらインタラクティブに要約方法を指定・変更ができるシステム DEISUM-B を開発した。システム管理者は、特別な知識がなくても熟練度, 好み, 目的に応じて要約方法を指定・変更することができる。また要約方法を複数組み合わせることにより、様々な角度から要約方法の評価ができる。今後は、複数のログもしくは 1 つのログに複数のメッセージが記述されているログに対し要約方法を指定できる機能を実装し、更なる機能拡張を行うとともにシステムの有用性評価を行う。

## 参考文献

[1] 高田 哲司, 小池 英樹. 見えログ:情報視覚化とテキストマイニングを用いたログ情報ブラウザ, 情報処理学会論文誌, Vol.41, No.12, 2000.