

## 表計算ソフトウェアを GUI とするログ解析システム logeeasy

麓 泰丈\*、千種 康民\*、Hector Sandoval\*、濱 正章\*\*、石丸 雅彦\*\*

\*東京工科大学 \*\*日立ソフトウェアエンジニアリング

### 1. はじめに

本研究グループでは、Linux マシン遠隔管理システムの構築を目的とし、ネットワーク資源の有効活用、遠隔管理、複数 PC の一括管理、データベース化、自動化、自律化、等の実現を目指し研究を行っている。

本稿では、クライアント側によるログ解析システムによる可能な限りの自律診断、保守管理者への負担の軽減を目的とし、linux 遠隔管理におけるログ監視サブシステム logeeasy を実現するものである。  
(図 1)

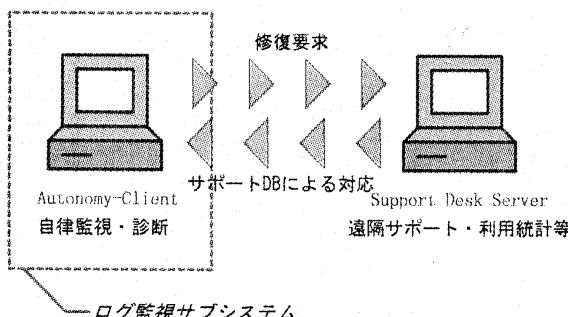


図 1 : システム全体の概要

### 2. システムの構築の方針

クライアントとなる Autonomy-Client が、ログを元にシステムを自律的に監視、エラーなどを自動検出。直接ネットワークに繋がっていない、外部管理者にあたる Support Desk Server へ、電子メールという形で修復要求を送信する。

本研究では基本的に、同じ LAN に繋がっていない、または、セキュリティ上リモートログインの許さ

れない、外部のワークグループの保守管理者へ注意喚起する事を目的としているため、メールで送信という手法を採用している。メールで送信という方法でログ情報を伝達する場合のセキュリティについては、使用するメールの機能に依存している。

### 3. 実現方法

#### 3.1 カスタマイズ及び保守性の容易さ

実現においては、既存の linux 用代表的ログ解析ツールである swatch、logsurfer を踏まえ、より複雑な抽出条件を分かりやすく絞り込める物を目指した。

本プログラムでは、設定ファイルを CSV 形式のファイル一つに集約させる事で、既存の表計算ソフトとの親和性を高め、編集を容易にした。これにより、よりグラフィカル、スピーディーにログ抽出条件を設定する事が可能となった。また、表計算ソフトに依存したサポート機能等も活用する事ができる。

以下に logsurfer との機能の比較を表 1 にまとめた。

	Logsurfer	Logeasy
正規表現を利用した抽出	利用可能	利用可能
複数行に跨る条件	利用可能	利用可能
時間情報の利用	テキストデータの一つとして認識	時間幅による設定が可能
アプリケーションとの連携	特に無し	抽出情報からのグラフ化など
保守性	テキストデータによる直接編集	既存の CSV 対応ソフトを利用した編集

表 1 : logsurfer との機能の比較

#### 3.2 ログ抽出機能の充実

ファイルをタイマーを使って定期的に監視・自動解析、抽出したログをメール送信できる事は勿論、外部プログラムに与えて自動実行させる等の機能を

持つ。また、ログ情報内の複雑な前後関係を解析、ファイル中の前後関係が一定条件を満たす時にアクションさせる等、ファイルを前後する条件を認識する機能を持つ。

図2の画面はWindows・Excelで使用したケースの一例である。既存の表計算ソフトを利用する事で、「オートフィル」や「色分け表示」等、表計算ソフト上の機能を利用でき、また「バルーン機能によるヘルプ」や「リストボックス」等で入力し易くなっている。Linux用表計算ソフトでもこうした機能の幾つかは利用可能である。

	A	B	C	D	E	F	G
1	PING	10.10.10.10	10.10.10.10	10.10.10.10	10.10.10.10	10.10.10.10	10.10.10.10
2	ADDRESS	10.10.10.10	10.10.10.10	10.10.10.10	10.10.10.10	10.10.10.10	10.10.10.10
3	JUNK_MAILER	/var/lib/sendmail					
4	SNMP	netmstat -an  P					
5	LOGGED-IN	root@10.10.10.10					
6	LOGGED-IN	root@10.10.10.10					
7	LOGGED-IN	root@10.10.10.10					
8	LOGGED-IN	root@10.10.10.10					
9	LOGGED-IN	root@10.10.10.10					
10	LOGGED-IN	root@10.10.10.10					
11	LOGGED-IN	root@10.10.10.10					
12	LOGGED-IN	root@10.10.10.10					
13	LOGGED-IN	root@10.10.10.10					
14	LOGGED-IN	root@10.10.10.10					
15	LOGGED-IN	root@10.10.10.10					
16	LOGGED-IN	root@10.10.10.10					
17	LOGGED-IN	root@10.10.10.10					
18	LOGGED-IN	root@10.10.10.10					
19	LOGGED-IN	root@10.10.10.10					
20	LOGGED-IN	root@10.10.10.10					
21	LOGGED-IN	root@10.10.10.10					
22	LOGGED-IN	root@10.10.10.10					
23	LOGGED-IN	root@10.10.10.10					
24	LOGGED-IN	root@10.10.10.10					
25	LOGGED-IN	root@10.10.10.10					
26	LOGGED-IN	root@10.10.10.10					
27	LOGGED-IN	root@10.10.10.10					
28	LOGGED-IN	root@10.10.10.10					
29	LOGGED-IN	root@10.10.10.10					
30	LOGGED-IN	root@10.10.10.10					
31	LOGGED-IN	root@10.10.10.10					
32	LOGGED-IN	root@10.10.10.10					
33	LOGGED-IN	root@10.10.10.10					
34	LOGGED-IN	root@10.10.10.10					
35	LOGGED-IN	root@10.10.10.10					
36	LOGGED-IN	root@10.10.10.10					
37	LOGGED-IN	root@10.10.10.10					
38	LOGGED-IN	root@10.10.10.10					
39	LOGGED-IN	root@10.10.10.10					
40	LOGGED-IN	root@10.10.10.10					
41	LOGGED-IN	root@10.10.10.10					
42	LOGGED-IN	root@10.10.10.10					
43	LOGGED-IN	root@10.10.10.10					
44	LOGGED-IN	root@10.10.10.10					
45	LOGGED-IN	root@10.10.10.10					
46	LOGGED-IN	root@10.10.10.10					
47	LOGGED-IN	root@10.10.10.10					
48	LOGGED-IN	root@10.10.10.10					
49	LOGGED-IN	root@10.10.10.10					
50	LOGGED-IN	root@10.10.10.10					
51	LOGGED-IN	root@10.10.10.10					
52	LOGGED-IN	root@10.10.10.10					
53	LOGGED-IN	root@10.10.10.10					
54	LOGGED-IN	root@10.10.10.10					
55	LOGGED-IN	root@10.10.10.10					
56	LOGGED-IN	root@10.10.10.10					
57	LOGGED-IN	root@10.10.10.10					
58	LOGGED-IN	root@10.10.10.10					
59	LOGGED-IN	root@10.10.10.10					
60	LOGGED-IN	root@10.10.10.10					
61	LOGGED-IN	root@10.10.10.10					
62	LOGGED-IN	root@10.10.10.10					
63	LOGGED-IN	root@10.10.10.10					
64	LOGGED-IN	root@10.10.10.10					
65	LOGGED-IN	root@10.10.10.10					
66	LOGGED-IN	root@10.10.10.10					
67	LOGGED-IN	root@10.10.10.10					
68	LOGGED-IN	root@10.10.10.10					
69	LOGGED-IN	root@10.10.10.10					
70	LOGGED-IN	root@10.10.10.10					
71	LOGGED-IN	root@10.10.10.10					
72	LOGGED-IN	root@10.10.10.10					
73	LOGGED-IN	root@10.10.10.10					
74	LOGGED-IN	root@10.10.10.10					
75	LOGGED-IN	root@10.10.10.10					
76	LOGGED-IN	root@10.10.10.10					
77	LOGGED-IN	root@10.10.10.10					
78	LOGGED-IN	root@10.10.10.10					
79	LOGGED-IN	root@10.10.10.10					
80	LOGGED-IN	root@10.10.10.10					
81	LOGGED-IN	root@10.10.10.10					
82	LOGGED-IN	root@10.10.10.10					
83	LOGGED-IN	root@10.10.10.10					
84	LOGGED-IN	root@10.10.10.10					
85	LOGGED-IN	root@10.10.10.10					
86	LOGGED-IN	root@10.10.10.10					
87	LOGGED-IN	root@10.10.10.10					
88	LOGGED-IN	root@10.10.10.10					
89	LOGGED-IN	root@10.10.10.10					
90	LOGGED-IN	root@10.10.10.10					
91	LOGGED-IN	root@10.10.10.10					
92	LOGGED-IN	root@10.10.10.10					
93	LOGGED-IN	root@10.10.10.10					
94	LOGGED-IN	root@10.10.10.10					
95	LOGGED-IN	root@10.10.10.10					
96	LOGGED-IN	root@10.10.10.10					
97	LOGGED-IN	root@10.10.10.10					
98	LOGGED-IN	root@10.10.10.10					
99	LOGGED-IN	root@10.10.10.10					
100	LOGGED-IN	root@10.10.10.10					
101	LOGGED-IN	root@10.10.10.10					
102	LOGGED-IN	root@10.10.10.10					
103	LOGGED-IN	root@10.10.10.10					
104	LOGGED-IN	root@10.10.10.10					
105	LOGGED-IN	root@10.10.10.10					
106	LOGGED-IN	root@10.10.10.10					
107	LOGGED-IN	root@10.10.10.10					
108	LOGGED-IN	root@10.10.10.10					
109	LOGGED-IN	root@10.10.10.10					
110	LOGGED-IN	root@10.10.10.10					
111	LOGGED-IN	root@10.10.10.10					
112	LOGGED-IN	root@10.10.10.10					
113	LOGGED-IN	root@10.10.10.10					
114	LOGGED-IN	root@10.10.10.10					
115	LOGGED-IN	root@10.10.10.10					
116	LOGGED-IN	root@10.10.10.10					
117	LOGGED-IN	root@10.10.10.10					
118	LOGGED-IN	root@10.10.10.10					
119	LOGGED-IN	root@10.10.10.10					
120	LOGGED-IN	root@10.10.10.10					
121	LOGGED-IN	root@10.10.10.10					
122	LOGGED-IN	root@10.10.10.10					
123	LOGGED-IN	root@10.10.10.10					
124	LOGGED-IN	root@10.10.10.10					
125	LOGGED-IN	root@10.10.10.10					
126	LOGGED-IN	root@10.10.10.10					
127	LOGGED-IN	root@10.10.10.10					
128	LOGGED-IN	root@10.10.10.10					
129	LOGGED-IN	root@10.10.10.10					
130	LOGGED-IN	root@10.10.10.10					
131	LOGGED-IN	root@10.10.10.10					
132	LOGGED-IN	root@10.10.10.10					
133	LOGGED-IN	root@10.10.10.10					
134	LOGGED-IN	root@10.10.10.10					
135	LOGGED-IN	root@10.10.10.10					
136	LOGGED-IN	root@10.10.10.10					
137	LOGGED-IN	root@10.10.10.10					
138	LOGGED-IN	root@10.10.10.10					
139	LOGGED-IN	root@10.10.10.10					
140	LOGGED-IN	root@10.10.10.10					
141	LOGGED-IN	root@10.10.10.10					
142	LOGGED-IN	root@10.10.10.10					
143	LOGGED-IN	root@10.10.10.10					
144	LOGGED-IN	root@10.10.10.10					
145	LOGGED-IN	root@10.10.10.10					
146	LOGGED-IN	root@10.10.10.10					
147	LOGGED-IN	root@10.10.10.10					
148	LOGGED-IN	root@10.10.10.10					
149	LOGGED-IN	root@10.10.10.10					
150	LOGGED-IN	root@10.10.10.10					
151	LOGGED-IN	root@10.10.10.10					
152	LOGGED-IN	root@10.10.10.10					
153	LOGGED-IN	root@10.10.10.10					
154	LOGGED-IN	root@10.10.10.10					
155	LOGGED-IN	root@10.10.10.10					
156	LOGGED-IN	root@10.10.10.10					
157	LOGGED-IN	root@10.10.10.10					
158	LOGGED-IN	root@10.10.10.10					
159	LOGGED-IN	root@10.10.10.10					
160	LOGGED-IN	root@10.10.10.10					
161	LOGGED-IN	root@10.10.10.10					
162	LOGGED-IN	root@10.10.10.10					
163	LOGGED-IN	root@10.10.10.10					
164	LOGGED-IN	root@10.10.10.10					
165	LOGGED-IN	root@10.10.10.10					
166	LOGGED-IN	root@10.10.10.10					
167	LOGGED-IN	root@10.10.10.10					
168	LOGGED-IN	root@10.10.10.10					
169	LOGGED-IN	root@10.10.10.10					
170	LOGGED-IN	root@10.10.10.10					
171	LOGGED-IN	root@10.10.10.10					
172	LOGGED-IN	root@10.10.10.10					
173	LOGGED-IN	root@10.10.10.10					
174	LOGGED-IN	root@10.10.10.10					
175	LOGGED-IN	root@10.10.10.10					
176	LOGGED-IN	root@10.10.10.10					
177	LOGGED-IN	root@10.10.10.10					
178	LOGGED-IN	root@10.10.10.10					
179	LOGGED-IN	root@10.10.10.10					
180	LOGGED-IN	root@10.10.10.10					
181	LOGGED-IN	root@10.10.10.10					
182	LOGGED-IN	root@10.10.10.10					
183	LOGGED-IN	root@10.10.10.10					
184	LOGGED-IN						