2005년도 대한전기학회 하계학술대회 논문집 2005. 7. 18 - 20

상관관계분석 기반 통합망 장애감시

조동권 KT 운용시스템연구소

An Integrated Network Monitoring Based on Event Correlation Analysis

D. K. Cho KT OSSL

Abstract - 본 논문에서 상관관계분석 기술을 이용하여 IP망과 전송망에서 발생되는 장애유형을 패턴화하였으며, 이를 Rule로써 자동처리가 가능하도록 시스템화하였다. 정의된 Rule로 인하여 이벤트 자동분석 및 장애근원 도출이 가능해졌으며, 도출된 근원 이벤트는 운용자에게 이벤트 분류를 위한 수고를 덜어주고, 궁극적으로 신속한 대처가 가능하게 하였다. 알고리듬의 효율성을 보이기 위하여 IP망과 전송망을 대상으로 10여개의 장애유형 표준을 패턴화하고 Rule로서 정의하여 적용한다.

1. 서론

현재 대형고장에 대한 판단이 운용자의 노하우에 주로 의존하여 이루어지고 있는 형편이다. 이런 조치방법은 운용자의 기량에 따라 대형고장 여부를 판단하여 장애대처를 해야 하기 때문에 고장조치 시간의 단축이 어려워 종합적이고 자동화된 장애관리 체계의 구현 및 수립을 어렵게 하는 요인이다. 또한 특정 도메인 상의 장애가 다른 도메인 장애로 인해 영향을 받은 경우, 도메인 통합 장애 상황관리 화면이 현장에 적용되지 못해서 고장원인의 추적이 어렵고, 도메인별 중복 트러블 티켓 발행 가능성이 크다. 이런 체계 하에서는 서비스 영향영역(관련 서비스 상품, 고객, 위치)의 신속한 도출 어렵다.

최근, 선진국에서는 도메인별/서비스별 장애관리에서 통합 망장애관리 형태로 관리방법이 진화하고 있으며 망장애에 대한 판단 및 문제해결을 위해 통합망 이벤트 정보로부터 그 장애근원을 찾으려 노력하고 있다. 시스템 통합 연동 여건이 보다 성숙하였으며, 통합 망장애정보 상관관계 분석 알고리즘을 비롯하여 H/W, S/W, 네트워킹 등 컴퓨터 성능 및 기술이 급속하게 발전하여 통합망 장애관리를 위한 환경이 무르익었다. 통합망관리 구축 사례를 살펴보면 제품 Lucent Navis NFM를 이용하여 실시간 Cross-Domain 장애감시(미국 AT&T NOC) 사례가 있고, HP OpenView TeMIP을 이용하여 ORB 미들웨어 기반의 상관관계분석 패키지를 개발한 경우 (호주 Telstra DSL-FAS Solution)도 있다. 또 국내에서는 Micromuse Netcool를 이용하여 장애영향 분석 기능을 구현한 경우도 있다. 본 논문에서는 장애관리를 위한 상관관계분석 기술을 소개하고 네트워크 통합장애관리에 적용가능함을 보이고자 한다.

네트워크 통합 장애관리시스템이란 다양한(시설별/서비스별) 도메인으로부터 장애정보를 수집하여 대형 고장유무를 판단하고, 신속한 상황전파 및 피해규모를 분석 조치하는 시스템이라 정의할 수 있다. 본 시스템은 장애원인을 규명하고 장애원인에 근거한 상황제어를 함으로써 신속하고 정확한 장애처리를 가능하게 한다. 그림1은 장애원인에 근거한 상황제어 도입 전후에 대해 운용자 관점에서 비교하여 나타낸 것이다.

기존 장애관리는 네트워크 도메인 단위로 별도로 운용되고 있어 타 도메인에 장애원인이 있는 경우 운용자들이 장애상황을 파악하고 처리하는 것이 대단히 어렵다. 운용자들은 장애해결을 경험에 의존하거나 타 도메인 운용자와의 대화를 통해 문제를 해결하는 등 비효율적인 장애처리가 지속되고 있다. 도입 후 시스템은 장애원인 분석을 통하여 장애 이벤트의 건수를 감소시킬 수 있어 장애 근원 이벤트만 경보로서 발생되도록 할 수 있다. 이러한 장점은 통합 도메인으로부터 장애정보를 수집하여 장애원인을 분석하고 분석된 장애원인에 대해서만 장애상황판에 보여지게 구성하였기에 가능한 것이다. 운용자들은 발생된 경보에 대한 처리만 수행하게 되며 이때 제공되는 장애원인에 대한 정확한 정보와 처리지침에 따라 신속하게 상황을 제어하면 된다. 또한 장애원인으로 인한 영향 고객 및 피해시설을 실시간으로 분석하여 제공함으로써 경영자에게 운용현황을 한눈에 파악할 수 있도록 하며 분석된 정보를 고객에게 제공하여 고객 만족도를 향상시킬 수 있게 된다.

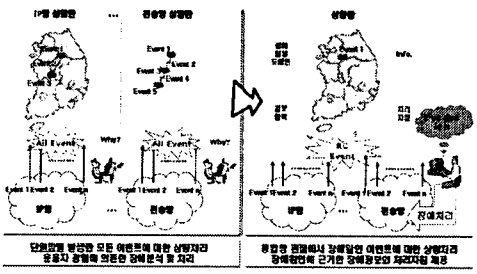

그림 1 장애원인에 근거한 상황제어

2. 상관관계 분석 기법

상관관계란 두 이벤트 간의 발생위치, 내용, 시간 등의 항목들을 비교하고 상호 관계를 정의함으로써 이벤트가 갖고 있는 특정 패턴을 검출하고 코드화하여 자동처리하기 위한 프로세스로 정의할 수 있다. 상관관계 적용이란 이벤트가 갖는 표준패턴에 대해 처리절차를 정의하고 이에 대해 각 이벤트마다 적합한 패턴을 적용하는 것이다. 이때 장치가 발생시키는 이벤트에 대해 고유의 패턴이 존재하고 이를 시스템화하는 것이 일반적인 적용방법이지만 실제로는 운용자의 이벤트 운용 방식에 따라 각 패턴의 수용방법에 차이를 갖게 된다. 즉, 장치 상으로는 별로 중요하지 않은 이벤트라고 정의되어 있어도 운용자에 의해 심각한 이벤트로 정의될 경우가 존재하게 된다. 상관관계 기술을 개발하여 적용하려는 가장 중요한 목적은 운용자 및 고객에게 네트워크 자원에 대해 최적화된 운용 및 서비스를 제공하기 위한 것이다. 상관관계 기술은 네트웍 서비스 장애 또는 그에 준하는 사유로 인해 발생되는 수많은 이벤트의 개수를 줄여주고 이벤트 처리로직의 최대한 자동화함으로써 운용자에 의해 처리되는 영역을 최소화하는 등이 가능해 진다.

가. 용어 및 분석 패턴 정의

용어 및 상관관계 분석을 위한 기본적인 정의는 다음과 같다.

Event : 상태가 변화하는 과정을 기록한 것으로 장치나 서버로부터 수신된 이벤트와 새로 생성한 이벤트를 의미

Message : 이벤트를 시간 정보와 함께 구체화한 것 (정보 제공이 목적)

Fault : 비정상적인 매개변수를 갖는 상태

Alarm : Fault에 대한 외부적 표현

Alert : 주의를 요구하는 표현 (Fault일 가능성이 있음)

Sequential: 순차적으로 발생되는 이벤트들의 관계분석

Temporal: 시간적인 조건을 통한 이벤트들의 관계분석

Causal: 원인과 결과의 관계를 따르는 이벤트 집합에 대한 규정

Content: 이벤트에 내포된 의미를 분석하여 관계를 규정

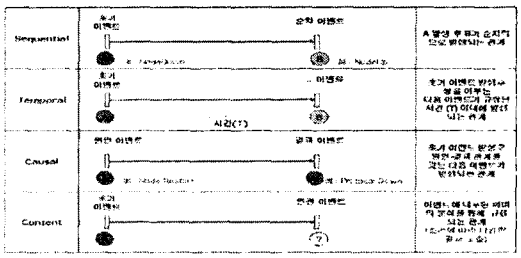

그림 2 상관관계 분석 패턴

나. 상관관계 분석 메커니즘

상관관계의 적용은 발생된 이벤트에 대한 상관관계의 분석, 상관관계에 대한 Rule 코드화, 생성된 Rule의 시험 및 현업 적용 등의 흐름으로 진행된다. 수신된 표준화된 이벤트(AllRawEvent)는 상관관계 기능 영역에서 4개 Rule 기능군을 지나게 되며 만일 중간에 처리되어 은폐되는 경우 모든 Rule의 적용을 받지 않을 수도 있다. 이벤트가 최종 단계에까지 이르는 장애근원 이벤트라고 가정할 경우 4단계를 통해 처리될 것이다. 장애정보를 처리하기 위한 상관관계 Rule은 장애 자체에 대한 상관관계(즉, De-Duplication) 정의로부터 단일망 (IP망, 전송망 등)내의 적용을 위한 것과 통합망(IP망-전송망)의 적용을 위한 것으로 해당 범위를 확대하면서 도출한다. 이벤트의 상관관계 처리 단계는 "이벤트 자체(단일 이벤트) 상관관계 적용" "단일망 상관관계 적용" "통합망 상관관계 적용"의 단계를 통해 정의된다. 이벤트의 표준화 단계로부터 산출된 표준 이벤트는 수신된 전체 이벤트를 수용하고 있으므로 운용자의 관점에서 그리고 시스템 관점에서 불필요한 이벤트들을 걸러주어야 한다. 또한 이벤트에 대한 기본적인 포맷 표준화 단계만을 거쳤기 때문에 운용자 수준의 이벤트 뷰를 제공하기 위해서는 이벤트의 필드 단위 가공이 필요하게 된다. 최종적으로는 이벤트 감소 기능을 사용하여 불필요한 이벤트를 억제하고 더 유용한 새 이벤트를 추가함으로써 이벤트 스톰을 관리하고 이벤트의 정보 내용을 개선하도록 한다. 이런 기능적인 요소들은 이벤트 자체에 대한 처리 과정을 통해 수행되고 이런 수행 과정을 통해 단일망 및 통합망과 같은 복합적인 이벤트 상관관계를 수행할 수 있는 기반이 마련된다. 장애 이벤트에 대한 영향분석을 위해 단일망 내에서의 상관관계 분석이 선행되어야 한다. 전송망과 IP망의 물리적 자원에 대한 장애 이벤트 분석에 대한 상관관계를 도출한다.

(1) 전송망 이벤트 상관관계 분석

전송망에서 발생되는 이벤트의 양은 수용되는 장치의 개수와 이벤트를 중계하는 중계시스템의 적용 규정에 따라 많은 차이가 있을 수 있다.

종속관계 : "전송망1-Pair"

A 이벤트가 수신되면 B 이벤트가 반드시 순차적으로 생성되는 경우에 대해 종속관계 패턴으로 정의한다. 이런 패턴에서는 장애의 근원에 대한 정보를 A 이벤트가 갖고 있다고 판단하며 따라서 A 이벤트의 수신 이후에 B 이벤트를 기다려서 B 이벤트가 수신되면 B를 은폐(화면에서 삭제)하고 A 이벤트를 근원정보로서 처리하는 로직을 고려할 수 있다.

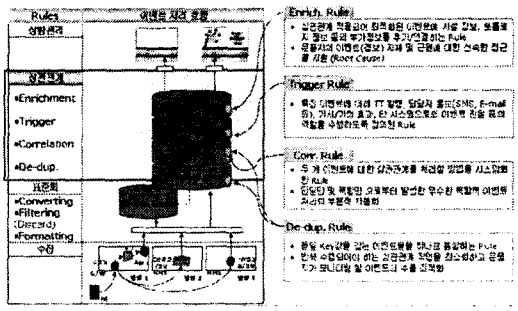

그림 3 상관관계 이벤트 처리 흐름

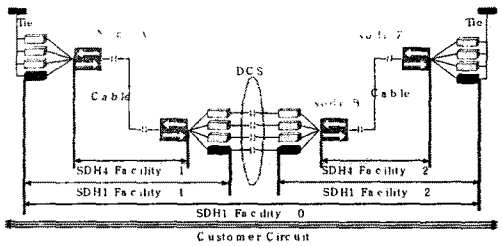

그림 4 전송망 구조

조건

A 이벤트 수신 후 T 시간 후 B 이벤트가 수신되면 수신된 B 이벤트를 제거하고 A 이벤트의 특정 필드에 대해 정보를 부가하거나 장애등급 (경보등급)을 상향(Escalation) 조정한다.

검색 조건은 Unique Key인 "국소명+시스템명+발생개소+경보항목" (전송망 필드 기준)을 기준으로 관련 이벤트를 검출하며 이벤트 수신 시까지의 적정시간 규정을 추가할 수 있다.

Rule 정의

표1 종속관계 : 전송망 Pair에 대한 Rule 1

[illegible] Rule		Value & Result
TPMS-RS_전송망_종속관계_전송망1-Pair	[Condition]	[Condition] ▸ 수신된 신규 이벤트가 다른 이벤트에 종속되는 관계를 갖을 경우 입력 발생한 주이벤트를 이벤트 DB에서 검출 (국소명+시스템명+발생개소+경보항목) ▸ 검출된 결과 이벤트가 존재하는지 판별
	[Action]	[Action : Delete Event] ▸ 신규 이벤트를 삭제

삼성25G-BLSR 경보 분석 - 6개 HSRU LOS-MSRDI 패턴1,2

삼성 2.5G BLSR 광단국 장치의 경우 발생되는 경보의 패턴을 몇가지 도출할 수 있다. 광단국 장치의 장애시 실제로는 여러 장치들간에 다양한 장애 경보가 발생될 수 있으나 여기에서는 기본적인 정보로서 삼성 2.5G 장치 자체에 대한 경보만을 고려 대상으로 삼았다.

조건

ADCU 경로 (MAP) 설정내역 : [A국-B국 : AUG1-1,2,3]

A국 HSTU(E) Tx 절체, B국 HSRU(W) Rx 절체시

그림 5에서와 같이 A국 2.5G BLSR 장치와 B국 2.5G BLSR

장치가 서로 연결되어 있고 A국 HSTU(Tx)와 B국 HSRU(Rx) 사이의 연결이 종단되는 것을 가정하였다. 이 경우 송신단인 A국 HSTU(Tx)에서는 경보가 발생되지 않는데 이것은 보내는 영역에서는 보내기까지의 과정에 문제가 없으면 수신단에서 해당 신호를 받고 못받는 상황을 전혀 고려하지 않도록 장치가 구성되어 있기 때문이다. 그러나 B국의 HSRU(Rx) 장치의 경우는 수신이 제대로 되지 않을 경우 경보가 발생되고 본 구성상에서 제일 앞서 발생되는 장애경보가 B국 HSRU(Rx) 단에서 발생되는 LOS 경보이다. LOS 경보가 발생된 이후 쌍(Pair)에 해당되는 B국의 HSTU(Tx)로부터 A국 HSRU(Rx)까지의 경로를 통해 A국의 HSRU(Rx) 단에서 장애가 있었음을 알려주는 경보를 발생하게 된다. 이들 경보가 발생된 후에 두 장치의 다른 유니트에서도 통신상에 문제가 있음을 감지하여 서로 경보를 발생시키게 되는데, 발생된 모든 경보는 결국 A국과 B국 간의 통신 불량으로 인해 발생된 것이고 근원 경보는 LOS로 규정된다.

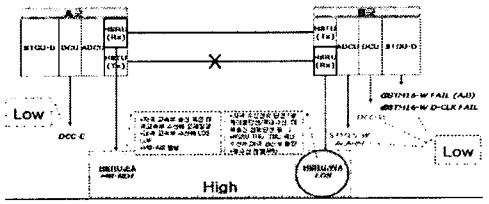

그림 5 삼성 2.5G BLSR 광단국 발생 경보

Rule 정의

관리대상 장치 및 시스템간 시간 동기화가 보장된다고 가정하며, Rule 정의시 시설정보를 참조하여야 하나 현재 NeOSS-FM의 시설정보가 완전치 않으므로 사례로서 동해중-강릉중 간 2.5G 장치의 연결정보를 수신하는 것으로 가정한다.

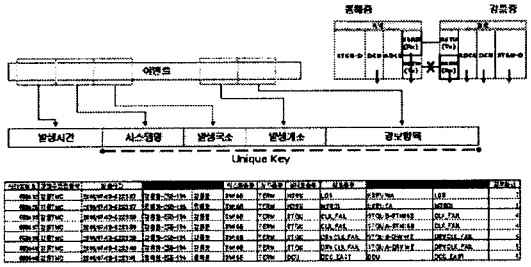

그림 6 삼성 2.5G BLSR 광단국 Rule 적용대상 이벤트

Rule 적용을 위한 이벤트 비교는 Unique Key로서 기본적인 비교를 수행하고 추가적으로 요구되는 비교 영역에 대해서는 다른 필드 정보를 추가로 적용함으로써 보다 상세한 비교 및 관련 영역의 이벤트들을 그룹으로 묶는 작업을 수행할 수 있다. 삼성 2.5G BLSR 광단국 Rule에서는 두 국소에 설치되어 있는 장치들 간에 LOS, MSRDI, CLK_FAIL, DRV CLK_FAIL, DCC_EAST, DCC_WEST 등의 경보가 발생하는 것으로 샘플링하였다.

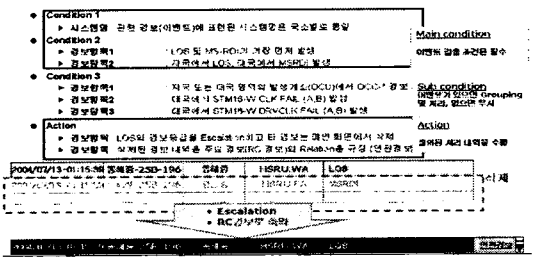

그림 7 삼성 2.5G BLSR 광단국 Rule 정의

Condition 1 :시스템명은 두 개로 구분되며, 발생된 이벤트는 두 개의 시스템명으로만 구성된다.

Condition 2 : LOS 및 MSRDI가 각각 자국 및 대국에서 가장 먼저 발생되며 관련된 이벤트 들이 이후에 발생된다.

Condition 3 : Condition 3는 발생될 수도 있고 발생되지 않을 수도 있는데, 발생되는 경우를 Rule 1으로 발생되지 않는 경우를 Rule 2로 정의한다. 발생되는 경우를 예로 들어, 발생되는 경보는 DCC-EAST, DCC-WEST, STM16-W CLK FAIL A, B 및STM16-W DRVCLK FAIL A,B 가 발생된다.

Action : LOS가 장애근원지의 정보로서 판단되므로, LOS 이후 T 시간 동안 경보의 발생을 기다린 후에 LOS와 관련된 경보들을 그룹으로 묶어서 LOS를 제외한 나머지 모든 이벤트들을 은폐(화면에서 삭제)한다. 은폐된 이벤트들은 연관경보 아이콘을 통해 보여질 수 있도록 구성한다. 최종적으로, LOS 경보는 장애근원 경보로서 경보등급을 상향 조정(Escalation)하여 상황관리 화면 상에 나타내 준다.

표 2 삼성 2.5G BLSR 광단국 Rule

항목 [Item] Rules		Value & Result
TFMS-RS_ 청송향_2-5G_ HSRU_LOS-MSRDI_ 패턴1	[Condition1] & [Condition2]	[Condition 1] ①HSRU.WA : LOS ②HSRU.EA : MSRDI [Condition 2] ①A국 DCU : DCC-E ②B국 DCU : DCC-W ③B국 STGU-D : (A,B) - STM16-W FAIL STM16-W D-CLK FAIL
	[Action]	[Action : Delete events] ▸ 관련 이벤트를 삭제: Condition 1-③ Condition 2-①②③ [Result] ▸ HSRU.WA : LOS
TFMS-RS_ 청송향_2-5G_ HSRU_LOS- MSRDI_패턴2	[Condition1] & Not [Condition2]	[Condition 1] ①HSRU.WA : LOS ②HSRU.EA : MSRDI
	[Action]	[Action : Delete events] ▸ 관련 이벤트를 삭제: Condition 1-③ [Result] ▸ HSRU.WA : LOS

표 2에서 삼성 2.5G BLSR 광단국 장치에서 도출될 수 있는 Rule의 영역을 2개로 분할하여 전체 규정된 이벤트가 모두 발생되는 경우의 Rule과 발생 대상 경보 중 주요 경보만이 발생되는 경우의 Rule을 정의하였다.

(2) IP망 이벤트 상관관계 분석

종속관계 : "IP망1-Pair"

A 이벤트가 발생된 뒤 B 이벤트가 반드시 발생되는 종속관계의 Pair인 경우라면 장애근원에 해당되는 A 이벤트를 남겨두고 B 이벤트를 삭제하여야 한다.

조건

A 이벤트와 B 이벤트의 종속관계 규정은 Rule에 정의되어 있다. 신규 이벤트가 수신되면 이 이벤트가 A-B 종속관계에 해당되는 이벤트인지 확인한다. 확인 결과 종속관계에 해당된다면 A,B 이벤트가 모두 발생되었는지 확인한다.

Rule 정의

발생사실이 확인되면 해당 이벤트 들 중 B 이벤트를 삭제하고 A 이벤트의 경보 등급을 상향 조치 하거나 (운용자 정의에 의해) 별도 조치 없이 남겨두는 등의 작업을 수행한다. 만일 종속관계의 이벤트 중 하나만 발생되었을 경우 DB 상에 남겨두어 향후 다른 이벤트가 발생되면 처리한다.

표 3 종속관계 : IP망 Pair 관련 Rule

항목 [Item] Rules		Value & Result
TFMS-RS_ IP망_ 종속관계_ IP망1-Pair	[Condition]	[Condition] ▸ 수신된 신규 이벤트가 다른 이벤트에 종속되는 관계를 갖을 경우 검사 발생된 주-이벤트를 이벤트 DB에서 검출 (국소명+시스템명+발생개소+경보항목) ▸ 검출된 결과 이벤트가 존재하는지 판정
	[Action]	[Action : Delete Event] ▸ 신규 이벤트를 삭제

대등관계 : "대등처리1-Pair"

Down/Up과 같이 Pair로 구성된 이벤트의 경우 두 이벤트가 모두 발생되면 모두 삭제하도록 정의할 수 있다.

조건

Pair로 구성된 이벤트에 대한 정의는 Rule에 정의되어 있어야 한다. 신규 이벤트가 수신되고 해당 이벤트가 Pair 중 한 쪽이며 다른 한 이벤트의 존재가 확인될 경우 두 이벤트를 묶어서 삭제한다. Pair의 분류는 일반적으로 경보등급을 통해 처리하도록 한다.

Rule 정의

표 4 대등관계 : 대등처리 Pair 관련 Rule

[Condition]	[Condition]
TMS RS_IP망_대등관계_대등처리1-Pair	▸ 수신된 신규 이벤트가 다른 이벤트와 Pair에 해당되는 관계정보 상 두 이벤트가 모두 존재하는 경우 (국소명+시스템명+망명+경보원인+경보등급
[Action]	[Action : Delete Event]
	▸ Pair 이벤트를 삭제

(3) 통합망 상관관계 분석

통합망의 상관관계 정의를 위해서는 단일망에 대한 상관관계 정의 및 적용이 일정 수준 이상 운용되어 그 운용 상의 안정성 및 정보관계가 어느 정도 인증된 후에 적용되어야 한다. 통합망의 상관관계 Rule에 포함되어야 할 정보가 기본적으로 단일망의 Rule 정보를 기반으로 구성되기 때문에 통합망의 상관관계는 단일망의 기반 위에서 구성되는 것이 타당하다. 단일망에서 이벤트의 처리가 장애근원 이벤트를 도출하는 과정이고 단일망 관점의 시설정보나 토폴로지 정보가 필요하다면 통합망에서는 이를 통합망 관점까지 확장하여야 하기 때문에 통합망에 대한 시설정보, 토폴로지 정보 등이 필요하게 된다.

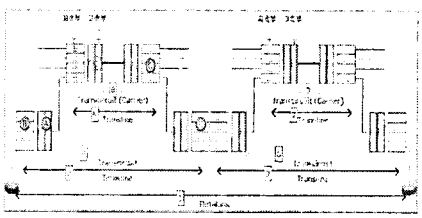

그림 8 통합망 토폴로지 예시

다. Sample 시뮬레이션 수행

여러 Ruleset을 이용하여 이벤트를 필터링하거나, 중복방지하는 등의 기능을 정의하고, 상관관계 Ruleset은 근원장애를 분석하거나, 영향 서비스 또는 영향 고객을 분석하는 업무를 정의한다. 하나의 Ruleset은 여러 Rule Group으로 세분화되고, 여기서 Rule Group이란 구체화된 작업 그룹으로써, 정의하는 업무의 세분화 정도에 따라 다양한 계층 구조로 구성된다. 도메인을 나타내는 IP, 전송망, Common등으로 최상위 Rule Group을 구성하고, IP Rule Group은 다시 CheckFrequency Rule Group으로 세분화하고 있다. 또한전송망 Rule Group도 EquipSpecifi과 General Rule Group으로 세분화된다. 각 Rule Group은 향후 적용되는 Rule들에 의해 하위 Rule Group으로 세분화 될 수 있다. 본 고에서 상용패키지로 Ilog Jrules를 이용하여 이벤트 상관관계 처리를 위한 서버를 구성하였고 Rule을 생성하여 적용하였다

3. 결론

상관관계를 적용함으로써 운영자가 감시해야 하는 이벤트 개수를 현격하게 감소시킬 수 있었으며, 근원 장애를 빠르게 분석할 수 있었다. Prototype에서는 기본적인 상관관계분석 시스템의 기능 구현을 통해 10개 Rule을 적용함으로써, 부분적인 근원 장애를 분석할 수 있었다. 향후 통신망에서의 장애 발생에 대한 지속적인 분석 및 패턴의 도출을 통해 Rule을 생성하고 Rule-Base를 갱신함으로써, 보다 정확한 근원 장애 분석 및 영향 분석이 가능하여 운영자의 감시대상 이벤트에 대한 노력을 절감시킬 수 있을 것으로 기대된다.

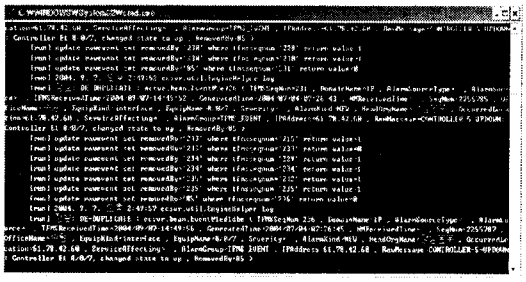

그림 9 데이터 처리 Console 화면

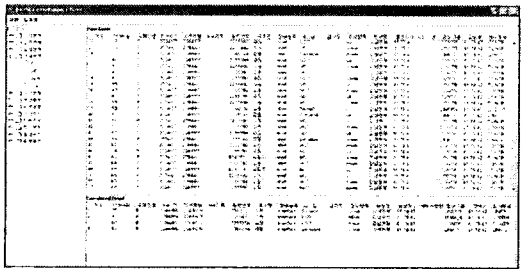

그림 10 운영자 화면

참고문헌

[1] Anthony V. Edwards and Robert J. Whitaker, Ph.D., Fault Management: A Functional View of Root Cause Analysis and Correlation, Tavve, 2000

[2] Jeff Caruso, Mgmt. tools will blanket N+I, Network World, May 10, 1999

[3] Cisco Network Monitoring and EventGuidelines, Cisco Press, 2002

[4] Creating the Environment for Root Cause Analysis (RCA) to Succeed: The Reliability Performance Process (TRPP), Reliability Center, Inc.