



**(19) 대한민국특허청(KR)**  
**(12) 등록특허공보(B1)**

(45) 공고일자 2008년07월16일  
 (11) 등록번호 10-0846835  
 (24) 등록일자 2008년07월10일

(51) Int. Cl.  
 G06F 15/00 (2006.01) H04L 12/22 (2006.01)  
 G06F 17/00 (2006.01)  
 (21) 출원번호 10-2006-0117746  
 (22) 출원일자 2006년11월27일  
 심사청구일자 2006년11월27일  
 (65) 공개번호 10-2008-0047826  
 (43) 공개일자 2008년05월30일  
 (56) 선행기술조사문헌  
 KR100559474 B1  
 KR1020040048468 A  
 KR100506851 B1

(73) 특허권자  
**(주)타임네트웍스**  
 경기 성남시 분당구 야탑동 145 분당테크노파크  
 제시동 제4층 제406호  
**한국전력공사**  
 서울특별시 강남구 삼성동 167번지  
 (72) 발명자  
**신동휘**  
 경기 성남시 분당구 이매동 아름마을두산아파트  
 422동 1904호  
**김종관**  
 경기 남양주시 호평동 현대아이파크아파트 1109동  
 1701호  
 (뒷면에 계속)  
 (74) 대리인  
**이범일, 이세진**

전체 청구항 수 : 총 9 항

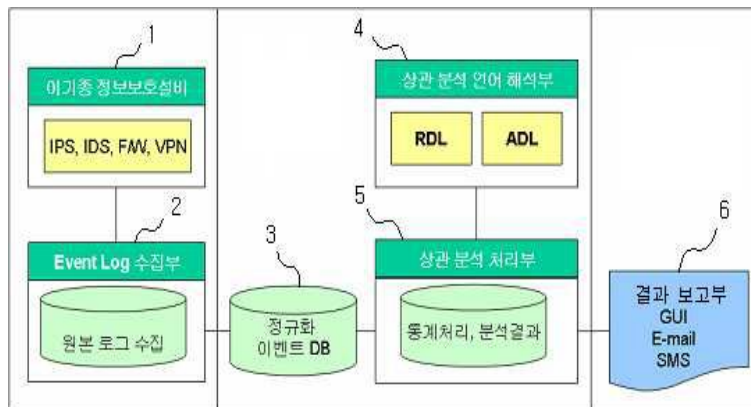
심사관 : 김상우

**(54) 문맥 언어 기반의 보안이벤트 상관분석 장치 및 방법**

**(57) 요약**

본 발명은 문맥 언어 기반의 보안 이벤트 상관분석 장치 및 방법에 관한 것으로, 각종 정보 보호설비(방화벽, 가상사설망, 침입탐지시스템, 침입방지시스템 등)로부터 다양한 방식으로 전송되는 보안 이벤트를 다양한 형식의 전송프로토콜을 통하여 수집하고, 수집된 이벤트를 설비군 별 공통된 형식으로 정규화하여 데이터베이스에 저장하고, 정규화된 이벤트의 주요 정보를 이용하여 이벤트의 발생 시간, 설비 및 네트워크의 위치에 기반을 두어 시/공간적 이벤트 상관분석을 기반으로 네트워크 공격 및 침해에 대한 신속한 탐지 및 그 결과를 휴대전화 단문메시지, 지유아이 팝업(GUI Popup) 및 이메일(E-mail)로 보안 운용자에게 알릴 수 있는 것을 특징으로 하는 것이다.

**대표도** - 도1



(72) 발명자

**최효열**

대전 유성구 송강동 한마을아파트 102동 103호

**송문호**

경기 성남시 분당구 서현2동 301번지 효자삼환아파트 507동 603호

**신준섭**

경기 용인시 기흥구 동백동 호수마을써미트빌 1701동 604호

**채문창**

경기 군포시 궁내동 1148번지 롯데묘향아파트 932동 203호

**배병오**

경기 광주시 오포읍 양벌리 대주1차아파트 111동 302호

## 특허청구의 범위

### 청구항 1

이벤트 로그가 발생하는 이기종 정보 보호설비(1); 상기 이기종 정보 보호설비(1)에서 발생한 이벤트 로그를 다양한 형식의 로그 전송프로토콜을 통하여 수집하는 이벤트 로그 수집부(2); 상기 이벤트 로그 수집부(2)에서 수집한 이벤트 로그를 정규화한 후에 표준화된 이벤트로 변환하여 DB에 저장하는 정규화 이벤트 DB(3); 사용자가 입력한 상관 분석 규칙을 RDL과 ADL로 나뉘어 해석하고 해석된 규칙을 상관 분석 처리부에 전달하는 상관분석 언어 해석부(4); 상기 상관분석 언어 해석부(4)로부터 해석된 규칙을 전달받아 상기 정규화 이벤트 DB에서 저장된 이벤트의 주요 값들을 참조하여 분석 및 통계를 수행하는 상관분석 처리부(5); 및 상기 상관분석 처리부(5)에서 분석된 결과를 사용자에게 알리는 결과보고부(6)로 이루어진 것을 특징으로 하는 문맥 언어 기반의 보안이벤트 상관분석 장치.

### 청구항 2

제 1 항에 있어서,

상기 상관분석 처리부(5)는 상관분석 규칙 스크립트를 통하여 정규화 이벤트를 불러들여 분석을 수행하고, 분석을 통하여 사용자에게 통지하기 위한 모든 과정이 상관분석 규칙 스크립트를 통하여 이루어지는 것을 특징으로 하는 문맥 언어 기반의 보안이벤트 상관분석 장치.

### 청구항 3

사용자에 의해 상관분석 규칙 스크립트가 입력되는 제 1 단계(ST1); 상기 제 1 단계(ST1) 후 이벤트 상관 분석 처리를 위한 RDL과 분석결과를 처리하기 위한 규칙인 Action 규칙처리를 위한 ADL로 구성된 상관분석 규칙 스크립트를 읽어서 문장 분석하는 제 2 단계(ST2); 상기 제 2 단계(ST2) 후 Syntax Grammer와 Syntax Diagram을 참조하여 해당 상관분석 규칙 스크립트를 해석하는 제 3 단계(ST3); 상기 제 3 단계(ST3) 후 사용자가 입력한 상관분석 규칙 스크립트에 오류가 있는지 없는지 판별하는 제 4 단계(ST4); 상기 제 4 단계(ST4) 후 사용자가 입력한 상관분석 규칙 스크립트에 오류가 있다면 이를 보고하는 제 5 단계(ST5); 상기 제 4 단계(ST4) 후 사용자가 입력한 상관분석 규칙 스크립트에 오류가 없다면 RDL과 ADL로 구분하는 제 6 단계(ST6); 상기 제 6 단계(ST6) 후 RDL로 구분된 상관분석 규칙 스크립트를 이벤트 상관분석 처리하는 제 7 단계(ST7); 상기 제 7 단계(ST7) 후 상관분석 처리한 결과가 다음 규칙의 새로운 조건인지 판별하여 새로운 조건이 아닐 경우 그 결과와 상기 제 6 단계(ST6) 후 ADL로 구분된 상관분석 규칙 스크립트를 Action 규칙 처리한 후 그 결과를 사용자에게 알려주고 다시 문장분석을 위해 상기 제 2 단계(ST2)로 재전송하는 제 8 단계(ST8); 상기 제 7 단계(ST7) 후 상관분석 처리한 결과가 상기 제 8 단계에서 다음 규칙의 새로운 조건으로 판별될 경우, 새로운 문맥을 생성하여 다음 규칙에서 이를 조건으로 새로운 규칙을 적용할 수 있도록 하는, 즉, 하나의 RDL을 처리한 결과가 다음 규칙의 RDL에서 새로운 조건(Context)으로 처리될 수 있도록 하는 제 9 단계(ST9); 및 상기 8 단계(ST8) 후 사용자에게 휴대전화 단문메시지, GUI Popup 및 E-mail을 통하여 보고하는 제 10 단계(ST10)를 포함하여 수행하는 것을 특징으로 하는 문맥 언어 기반의 보안이벤트 상관분석 방법.

### 청구항 4

제 3 항에 있어서,

상기 RDL의 Syntax Diagram은, 상관분석언어를 통하여, 규칙을 생성하거나, 생성된 규칙을 갱신할 수 있으며, 생성된 규칙에 대한 규칙의 명칭 및 생성된 상관분석규칙이 속하는 대분류의 Class를 지정하고, 정규화된 이벤트를 정규화이벤트 DB로부터 참조하여 시간, 디바이스 ID, 네트워크 ID, 이벤트, 방화벽 규칙 ID, 침입탐지/침입차단 시스템의 Signature ID의 정보보호설비가 제공한 정보를 일반적인 AND, OR, 괄호, 비교연산자(==, !=, <, >, =, =>)를 통한 조합으로 Context(문맥/조건)을 생성하는 것을 특징으로 하는 문맥 언어 기반의 보안이벤트 상관분석 방법.

### 청구항 5

제 3 항에 있어서,

상기 RDL의 Syntax Diagram은, 정의된 상관분석 규칙 스크립트에 의해 생성된 문맥/조건(Context)을 참조하여

다수개의 문맥/조건을 그룹으로 하여 새로운 문맥/조건을 생성할 수 있는 것을 특징으로 하는 문맥 언어 기반의 보안이벤트 상관분석 방법.

**청구항 6**

제 3 항에 있어서,

상기 ADL의 Syntax Diagram은, RDL에 의해 출력된 상관분석의 결과에 따라 새로운 문맥/조건(Context)를 생성할 수 있으며, 이때 생성된 문맥명칭(Context Name)은 RDL에 의해 재사용이 가능한 것을 특징으로 하는 문맥 언어 기반의 보안 이벤트 상관분석 방법.

**청구항 7**

제 3 항에 있어서,

상기 ADL의 Syntax Diagram은, RDL에 의해 출력된 상관분석의 결과에 따라 RDL에 의해 출력된 상관분석의 결과를 사용자에게 알림에 있어서, 그 결과의 중요도를 지정할 수 있는 것을 특징으로 하는 문맥 언어 기반의 보안 이벤트 상관분석 방법.

**청구항 8**

제 7 항에 있어서,

상기 RDL의 결과를 사용자에게 알림에 있어서, 관리자를 지정할 수 있으며, 결과를 알려 주는 수단으로 휴대전화 단문메시지, GUI Popup 및 E-mail을 통한 전달 방법을 언어로 정의할 수 있는 것을 특징으로 하는 문맥 언어 기반의 보안 이벤트 상관분석 방법.

**청구항 9**

제 3 항에 있어서,

상기 상관분석 규칙 스크립트를 통한 문맥/조건(Context)의 생성 기능과 생성된 문맥/조건(Context)를 이용한 상세한 조건 검색 및 이벤트 추적 기능을 제공할 수 있는 것을 특징으로 하는 문맥 언어 기반의 보안이벤트 상관분석 방법.

**명세서**

**발명의 상세한 설명**

**발명의 목적**

**발명이 속하는 기술 및 그 분야의 종래기술**

- <9> 정보산업화가 급속히 성장한 근래에 있어서, 정보의 진산화 및 업무의 네트워크화로 인하여 정보의 중요성과 함께 정보에 대한 외부로부터의 공격 및 침해사고가 빈번히 발생함에 있어서 정보보호침해 사고를 방지하기 위한 각종 보안 설비들이 소개되어 운영되고 있었다.
- <10> 다양한 제품들이 다양한 제조사들로부터 소개되고 있으며, 네트워크 정보보호설비들은 동일 또는 유사 이벤트에 대한 표현형식에 있어서 제각각의 형식으로 운영자에게 정보를 제공함으로써 단일 네트워크의 다수 정보보호설비를 동시에 운영하고 있는 관리자에게 정보보호설비 및 정보보호 이벤트에 대한 대응에 있어서 많은 어려움이 있었다.
- <11> 또한, 정보보호설비로부터 발생하는 보안이벤트는 그 발생빈도가 상당히 높고, 운영자가 개별 이벤트에 대한 추적 및 관리가 어려운 상태이며, 더욱이, 정보보호설비의 보안이벤트가 오탐(False Positive 및 False Negative)의 경우가 많아 이벤트의 신뢰성이 떨어지는 상황이 종종 발생하는 문제점이 생겼다.
- <12> 이러한 환경에서 정보보호설비의 보안 이벤트에 대한 분석의 의무가 국내외 주요기관의 지침 및 사내 지침에 의해 강조되고 있다.
- <13> 이로 인하여, 국내 로그분석 시스템이 소개되어 다양한 형식의 이벤트 형식을 정규화 하여 하나의 형식으로 통

일하여 출력하고, 빈번히 발생하는 이벤트 등에 대한 통계 정보를 제공함에 있어서 보안 관리자에게 관리의 편의를 제공하고 업무의 간소화에 기여한바가 있었다.

<14> 하지만, 다소 규모가 있는 시스템의 경우 업무의 성격에 따라 네트워크를 세분화 하여 운영하고 있으며, 정보보호설비 또한 각 네트워크에 설치 운영되고 있다. 즉, 네트워크가 세분화됨에 따라 단일 설비에서 발생한 이벤트가 제공하는 정보만으로는 침해사고 및 공격 추적에 상당히 미흡한 문제점이 있었다.

<15> 또한, 하나의 네트워크에서 다수의 정보보호설비의 이벤트의 상관관계를 추적하고, 또, 다수의 네트워크 간에 발생한 이벤트를 상관분석 함으로써 보다 확장된 개념의 공격 침해 상황을 판단하여 침해에 조기에 대응할 수 있는 환경을 제공하기 위해 정보보호설비 이벤트 상관분석 (Event Correlation)기법을 필요로 하게 되었다.

<16> 그러나, 기존의 국내 로그분석 시스템의 구현방법은 이벤트 간 상관분석을 위하여 '분석규칙'이 필요할 때마다 분석엔진 자체가 빈번히 수정되어야 하는 구조를 가지고 있다. 즉, 기존의 분석프로그램은 새로운 규칙의 적용에 있어서 매우 제한적일 수 밖에 없으며, 지원하지 않는 규칙의 적용을 위한 프로그램 수정에 있어서 많은 시간과 비용 및 유지보수 인력이 요구되는 문제가 있다.

<17> 또한, 상기의 고정된 규칙을 가지는 분석엔진의 문제점을 해결함에 있어서, 분석 대상인 정보보호설비의 이벤트를 정규화하여 DB에 저장하고, 정보보호 이벤트 상관분석에 특화된 '문맥 기반 상관분석 언어' 및 '상관분석 엔진'을 개발함으로써 새로운 상관분석의 규칙적용이 상당히 유연한 상관분석 기반기술을 제공할 필요가 생겼으며, 이러한 프레임워크 구현을 위하여 상관분석 방법을 조합하여 기본 로그분석 기능뿐만 아니라, 프레임워크를 위한 RDL 기반으로 분석규칙 및 대응규칙에 대한 유연성과 확장성을 요구하게 되었다.

<18> 하기의 [표 1]은 본 발명과 국내외 유사·경쟁 기술과의 특징을 비교분석한 것이다.

<19> [ 표 1 ]

국내외 유사·경쟁기술과의 특징비교(정성적 비교)			
항 목 (적용기술)	본 발명	국내 유사·경쟁기술 (기술명:로그분석기 )	선진국 유사·경쟁기술 (선진사 도입 설비)
공격분석기법 (Network Attack Context-based attack Analysis)	있 음	없 음	없 음
분석 Rule 정의 유연성 (Rule Description Language based)	있 음	없 음 (단순 Filter)	없 음 (Hard Coded)
분석 Rule 정의 확장성 ( Rule 정의 언어를 통한 확장성 )	있 음	없 음	없 음
이벤트 정규화 (국제표준기반)	있 음	없 음	있 음

<20>

**발명이 이루고자 하는 기술적 과제**

<21> 이에 본 발명은 상기와 같은 종래 문제점을 해결하기 위해 발명된 것으로, 다양한 형식의 동종 또는 이기종 정보보호설비의 이벤트로부터 '이벤트 발생 시간' 및 정보보호설비가 위치한 네트워크의 위치 정보를 반영한 시공간(Spatiotemporal)적 상관분석기법을 유연하고 확장성 있게 기술할 수 있도록 문맥 언어 기반의 보안이벤트 상관분석 장치 및 방법을 제공함에 그 목적이 있다.

**발명의 구성 및 작용**

<22> 상기한 목적을 달성하기 위한 본 발명은, 이벤트 로그가 발생하는 이기종 정보보호설비(1); 상기 이기종 정보보호설비(1)에서 발생한 이벤트 로그를 다양한 형식의 로그 전송 프로토콜을 통하여 수집하는 이벤트 로그 수집부(2); 상기 이벤트 로그 수집부(2)에서 수집한 이벤트로그를 정규화한 후에 표준화된 이벤트로 변환하여 DB에 저장하는 정규화 이벤트 DB(3); 사용자가 입력한 상관 분석 규칙을 RDL과 ADL로 나누어 해석하고 해석된 규칙을

상관 분석 처리부(5)에 전달하는 상관분석 언어 해석부(4); 상기 상관분석 언어 해석부(4)로부터 해석된 규칙을 전달받아 상기 정규화 이벤트 DB(3)에 저장된 이벤트의 주요 값들을 참조하여 분석 및 통계를 수행하는 상관 분석 처리부(5); 및 상기 상관분석 처리부(5)에서 분석된 결과를 사용자에게 알리는 결과 보고부(6)로 이루어진 것을 특징으로 한다.

- <23> 또한, 본 발명의 동작은 사용자에 의해 상관분석 규칙 스크립트가 입력되는 제 1 단계; 상기 제 1 단계 후 이벤트 상관 분석 처리를 위한 RDL과 분석결과를 처리하기 위한 규칙인 Action 규칙처리를 위한 ADL로 구성된 상관 분석 규칙 스크립트를 읽어서 문장 분석하는 제 2 단계; 상기 제 2 단계 후 Syntax Grammer와 Syntax Diagram을 참조하여 해당 상관분석 규칙 스크립트를 해석하는 제 3 단계; 상기 제 3 단계 후 사용자가 입력한 상관분석 규칙 스크립트에 오류가 있는지 없는지 판별하는 제 4 단계; 상기 제 4 단계 후 사용자가 입력한 상관분석 규칙 스크립트에 오류가 있다면 이를 보고하는 제 5 단계; 상기 제 4 단계 후 사용자가 입력한 상관분석 규칙 스크립트에 오류가 없다면 RDL과 ADL로 구분하는 제 6 단계; 상기 제 6 단계 후 RDL로 구분된 상관분석 규칙 스크립트를 이벤트 상관분석 처리하는 제 7 단계(ST7); 상기 제 7 단계 후 상관분석 처리한 결과가 다음 규칙의 새로운 조건인지 판별하여 새로운 조건이 아닐 경우 그 결과와 상기 제 6 단계 후 ADL로 구분된 상관분석 규칙 스크립트를 Action 규칙 처리한 후 그 결과를 사용자에게 알려주고 다시 문장분석을 위해 상기 제 2 단계로 재전송하는 제 8 단계; 상기 제 7 단계 후 상관분석 처리한 결과가 상기 제 8 단계에서 다음 규칙의 새로운 조건으로 판별될 경우, 새로운 Context를 생성하여 다음 규칙에서 이를 조건으로 새로운 규칙을 적용할 수 있도록 하는, 즉, 하나의 RDL을 처리한 결과가 다음 규칙의 RDL에서 새로운 조건(Context)으로 처리될 수 있도록 하는 제 9 단계; 및 상기 8 단계 후 사용자에게 휴대전화 단문메시지, GUI Popup 및 E-mail을 통하여 보고하는 제 10 단계를 포함하여 수행하는 것을 특징으로 한다.
- <24> 이하 본 발명의 실시예를 첨부된 도면에 의하여 상세히 설명하면 다음과 같다.
- <25> 도 1은 본 발명의 일 실시예에 의한 문맥 언어 기반의 보안이벤트 상관분석 장치의 개념도이다.
- <26> 도시된 바와 같이, 이기종 정보보호설비(1)에서 발생한 이벤트 로그를 이벤트 로그 수집부(2)는 다양한 형식의 로그 전송 프로토콜을 통하여 수집하고, 이를 IDMEF 국제 표준에 기반하여 정규화(Normalization)한 후에 표준화된 이벤트로 변환하여 DB(3)에 저장한다. 이때 DB의 데이터 저장 형식은 하드디스크에 저장될 수도 있으며, 때에 따라 고속처리를 위한 메모리 DB 형식을 존재 할 수 있다.
- <27> 또한, 상관분석 언어 해석부(4)는 사용자가 입력한 상관분석규칙을 RDL과 ADL로 나누어 해석하고 해석된 규칙은 상관분석 처리부(5)에 전달한다. 규칙을 전달 받은 상관분석 처리부는 정규화이벤트 DB에서 저장된 이벤트의 주요 값들을 참조하여 분석 및 통계처리를 수행하며, 결과 보고부(6)에서 분석된 결과를 사용자 환경에서의 휴대전화 단문메시지, GUI Popup 및 E-mail을 통하여 사용자에게 전달하도록 구성된다.
- <28> 특히, 상관분석 규칙 스크립트를 통하여 정규화 이벤트를 불러들여 분석을 수행하고, 분석을 통하여 사용자에게 알리는 모든 과정이 상관분석 규칙 스크립트를 통하여 가능한 것을 가장 큰 특징으로 한다.
- <29> 도 2는 도 1의 동작을 나타내는 스크립트 처리를 나타낸 흐름도이다.
- <30> 이에 도시된 바와 같이, 사용자에 의해 상관분석 규칙 스크립트가 입력되는 제 1 단계(ST1); 상기 제 1 단계(ST1) 후 이벤트 상관 분석 처리를 위한 RDL과 분석결과를 처리하기 위한 규칙인 Action 규칙처리를 위한 ADL로 구성된 상관분석 규칙 스크립트를 읽어서 문장 분석하는 제 2 단계(ST2); 상기 제 2 단계(ST2) 후 Syntax Grammer와 Syntax Diagram을 참조하여 해당 상관분석 규칙 스크립트를 해석하는 제 3 단계(ST3); 상기 제 3 단계(ST3) 후 사용자가 입력한 상관분석 규칙 스크립트에 오류가 있는지 없는지 판별하는 제 4 단계(ST4); 상기 제 4 단계(ST4) 후 사용자가 입력한 상관분석 규칙 스크립트에 오류가 있다면 이를 보고하는 제 5 단계(ST5); 상기 제 4 단계(ST4) 후 사용자가 입력한 상관분석 규칙 스크립트에 오류가 없다면 RDL과 ADL로 구분하는 제 6 단계(ST6); 상기 제 6 단계(ST6) 후 RDL로 구분된 상관분석 규칙 스크립트를 이벤트 상관분석 처리하는 제 7 단계(ST7); 상기 제 7 단계(ST7) 후 상관분석 처리한 결과가 다음 규칙의 새로운 조건인지 판별하여 새로운 조건이 아닐 경우 그 결과와 상기 제 6 단계(ST6) 후 ADL로 구분된 상관분석 규칙 스크립트를 Action 규칙 처리한 후 그 결과를 사용자에게 알려주고 다시 문장분석을 위해 상기 제 2 단계(ST2)로 재전송하는 제 8 단계(ST8); 상기 제 7 단계(ST7) 후 상관분석 처리한 결과가 상기 제 8 단계에서 다음 규칙의 새로운 조건으로 판별될 경우, 새로운 문맥을 생성하여 다음 규칙에서 이를 조건으로 새로운 규칙을 적용할 수 있도록 하는, 즉, 하나의 RDL을 처리한 결과가 다음 규칙의 RDL에서 새로운 조건(Context)으로 처리될 수 있도록 하는 제 9 단계(ST9); 및 상기 8 단계(ST8) 후 사용자에게 휴대전화 단문메시지, GUI Popup 및 E-mail을 통하여 보고하는 제 10 단계

(ST10)를 포함하여 수행한다.

- <31> 도 3은 본 발명의 일실시예에 의한 RDL의 구성도이며, 도 4는 본 발명의 일실시예에 의한 ADL의 구성도이다.
- <32> 도 3은 RDL의 Syntax Diagram으로 이벤트 또는 이벤트간의 이벤트 상관분석을 위한 규칙을 정의한 상관분석 규칙 스크립트의 언어 형식에 대한 자세한 내용을 담고 있다. 상관분석 언어를 통하여, 규칙을 생성하거나, 생성된 규칙을 갱신할 수 있으며, 생성된 규칙에 대한 규칙의 명칭 및 생성된 상관분석규칙이 속하는 대분류의 클래스(Class)를 지정하고, 정규화된 이벤트를 정규화이벤트 DB로부터 참조하여 보안이벤트의 시간, 디바이스 ID, 네트워크 ID, 이벤트, 방화벽 규칙 ID, 침입탐지/침입차단 시스템의 Signature ID 등과 같이 후술하는 [표 2]에 기재된 정규화이벤트 파라미터 정보를 일반적인 AND, OR, 괄호, 비교연산자(== , != , < , > , =< , =>)를 통한 조합으로 문맥/조건(Context)을 생성하고, 또, 기 정의된 상관분석규칙에 의해 생성된 문맥/조건(Context)을 참조하여 다수개의 문맥/조건을 그룹으로 하여 새로운 문맥/조건을 생성할 수 있음을 나타낸다. 이때, 문맥/조건(Context)을 만족하는 이벤트의 주요 출발지 IP 및 목적지 IP는 도 4의 ADL의 경고 메시지(Alert-Message)에서 사용될 수 있으며, 이는 문제의 IP를 사용자에게 알려 줄 수 있는 기능을 가능하게 한다.
- <33> 상관분석 규칙 스크립트에 의해 생성된 문맥/조건을 만족하는 이벤트의 조합이 발생할 경우, 특정시간 동안에 사용자가 지정한 시간에서 그 발생횟수가 사용자가 지정한 횟수를 넘어설 경우 상관분석결과를 출력하고, 또, 특정시간 동안 상관분석결과가 사용자가 지정한 시간 내에 중복 발생할 경우 중복경고를 억제할 수 있다.
- <34> 도4는 ADL의 Syntax Diagram으로 RDL에 기반한 이벤트상관분석의 결과를 처리하는 언어 형식에 대한 자세한 내용을 담고 있다. RDL에 의해 출력된 상관분석의 결과에 따라 첫 번째로, 새로운 문맥/조건(Context)을 생성할 수 있으며, 이때 생성된 문맥명칭(Context Name)은 RDL에 의해 재사용이 가능하다. 두 번째로, RDL에 의해 출력된 상관분석의 결과를 사용자에게 알림에 있어서, 그 결과의 중요도를 지정할 수 있다. 또한, 사용자에게 RDL의 결과를 알림에 있어서, 관리자를 지정할 수 있으며, 결과를 알려 주는 수단으로 휴대전화 단문메시지, GUI Popup 및 E-mail을 통한 전달 방법을 언어로 정의할 수 있다.
- <35> 따라서, 상기의 상관분석 언어를 활용하여, 정보 보호설비로부터 하기에 [표 2]나타낸 정규화 이벤트 파라미터를 바탕으로 이벤트 간, 정보 보호설비 간, 네트워크 간 이벤트의 상관분석이 가능하다.

<36> [ 표 2 ]

정보보호 설비군	로그 파라미터	상 세 설 명
정보 보호 설비 공통	Device ID	정보보호설비의 고유 ID
	Network ID	정보보호설비가 속한 네트워크 ID
	Date_Time	이벤트 발생 시간
	TYPE	로그 타입(Alert, Warn, Info, System)
	LogType	발생 이벤트의 성격
	Version	Log 버전
	OriginIP	로그 생성 설비의 IP (정보보호설비)
	HostName	정보보호설비 명
	Interface	이벤트 발생 인터페이스
	Protocol	UDP, TCP, ICMP 등
	ServiceName	알려진 서비스 또는 운용자에 의해 정의된 서비스 명칭
	Source_IP	출발지 주소
	Source_Port	출발지 포트
	Destination_IP	목적지 주소
	Destination_Port	목적지 포트
Severity	이벤트 중요도 'Critical, Major, Info, Minor'	
RuleID	방화벽 Rule ID	
Action	세션 허용, 거부 (permit, deny)	
Sequence	로그 이벤트의 순번	
F/W	NAT_Source_IP	NAT 주소 변경 후 출발지 주소
	NAT_Source_Port	NAT 주소 변경 후 출발지 포트
	NAT_Destination_IP	NAT 주소 변경 후 목적지 주소
	NAT_Destination_Port	NAT 주소 변경 후 목적지 포트
	NAT_Rule	NAT 변경 룰 ID
IPS/IDS	StartTime	NAT 변경 후 목적지 포트
	EndTime	Protocol (TCP/UDP/ICMP)
	Duration	사용 포트에 정의된 서비스 명
	EventCount	Duration' 동안 발생한 동일 이벤트 횟수
	RuleGroup	Rule 그룹명
	RuleName	Rule 명칭
VPN	SignatureName	Signature 명칭
	Code	이벤트 중요도
	Authentication	인증 성공 여부
	Encryption	Encryption 성공 여부
	Decryption	Decryption 성공 여부
	IKE	IKE Event
	L2TP_Create	L2TP Tunnel 생성
L2TP_Close	L2TP Tunnel 닫기	
기타	Note	이벤트에 대한 별도의 상세 정보

<37> [ 정규화 이벤트 파라미터 ]

<38> 상기의 정보 보호설비의 정규화된 이벤트 정보로부터 간단하게는 하기와 같은 단일 이벤트를 기반으로 상관분석 규칙을 지정하고 그 결과를 확인 할 수 있다.

<39> 상관분석의 첫 번째 예로, 하기의 [표 3]은 방화벽의 단일 이벤트로부터 이벤트 상관분석을 통하여, 그 결과를 사용자에게 알려주는 상관분석 규칙 스크립트이다.

<40> [ 표 3 ]

<41> 

출발지IP=any, 출발지포트=1356, 목적지IP=any, 목적지포트=2101, action=any
--

<42> 출발지 포트가 1356이고, 목적지 포트가 2101을 사용하는 공격을 'Buffer Overflow 공격시도'라고 할 때, 해당 분석의 결과에 대한 중요도와 위의 방화벽 정보로부터 공격을 시도한 출발지 IP 및 목적지 IP를 사용자에게 휴대전화 단문메시지, GUI Popup 및 E-mail을 통하여 동시에 알려주기 위한 상관분석 규칙 스크립트의 표현은 하기의 [표 4]와 같다.

<43> [ 표 4 ]

상관분석언어 규칙 (단일 이벤트)	설 명
CREATE rule 'ncsc-09' class 2	규칙명과 규칙이 속하는 Class 지정
FROM IDMEF	IDMEF로 명명된 정보보호설비 이벤트의 위치
WHERE s_port==1356 && d_port==2101	출발지포트가 1356 이고, 목적지포트가 2101 인 이벤트에 대해
ACT CONTEXT CREATE "cxt-09"	'cxt-09'라는 문맥/조건(Context) 생성
ACT ALERT WARNING	'cxt-09'라는 문맥/조건(Context) 발생시, cxt-09를 발생시킨 공격 수준이 WARNING 으로 경고를 발생시키고,
'Buffer Overflow공격 시도 의심: [\$cxt-09.s_ip] -> [\$cxt-09.d_ip]'	공격의 내용(Buffer Overflow 공격 시도 의심)과 출발지 IP(공격자 IP)와 목적지 IP(공격대상IP)를 표기하여,
to all by GUI,email,sms	사용자에게 GUI, E-mail, 휴대전화 문자메시지로 경고메시지를 전달한다.

<44>

<45> 또한, 상관분석의 두 번째 예로, 위의 첫 번째 예에서 이벤트분석을 통한 문맥/조건(Context)가 발생한 경우에 한하여, 아래의 보안 이벤트가 발생할 경우, 그 결과를 사용자에게 알려주는 것으로, 상관분석 언어가 문맥/조건(Context)을 활용할 수 있음으로 하여, 그 규칙적용의 유연성을 확인 할 수 있다.

<46> [ 표 5 ]

출발지IP=any, 출발지포트=1356, 목적지IP=any, 목적지포트=2101, action=any 출발지IP=any, 출발지포트=20, 목적지IP=any, 목적지포트=34568
---

<48> 상기의 [표 5]와 같이 첫 번째 예의 이벤트가 발생하고, 이를 발생시킨 출발지 IP 및 목적지 IP를 가지고, 출발지 포트 20, 목적지 포트 34568을 가진 이벤트가 발생하였을 경우에 한하여 경고메시지로 사용자에게 알려주기 위한 상관분석 언어의 표현은 하기의 [표 6]과 같다.

<49> [ 표 6 ]

상관분석언어 규칙 (단일 이벤트)	설 명
CREATE rule 'ncsc-09-01' class 2	규칙명과 규칙이 속하는 Class 지정
FROM IDMEF	IDMEF로 명명된 정보보호설비 이벤트의 위치
WHERE s_ip==\$cxt-9.d_ip && d_ip==\$cxt-9.s_ip && s_port==20 && d_port==34568	첫 번째 예에서 발생한 상관분석결과에의 출발지IP와 목적지 IP로 출발지 포트 20과 목적지 포트가 34568인 이벤트 발생시,
CONTEXT "cxt-09"	첫 번째 예에서 생성한 'cxt-09'라는 문맥/조건 (Context)이 발생한 경우에 한하여,
ACT ALERT WARNING	공격 수준이 WARNING 으로 경고를 발생시키고,
'원격 접속관리 취약점 공격: [\$cxt-09.s_ip] -> [\$cxt-09.d_ip]'	공격의 내용(원격접속관리 취약점 공격)과 출발지 IP(공격자 IP)와 목적지 IP(공격대상IP)를 표기하여,
to all by GUI,email,sms	사용자에게 GUI, E-mail, 휴대전화 문자메시지로 경고메시지를 전달한다.

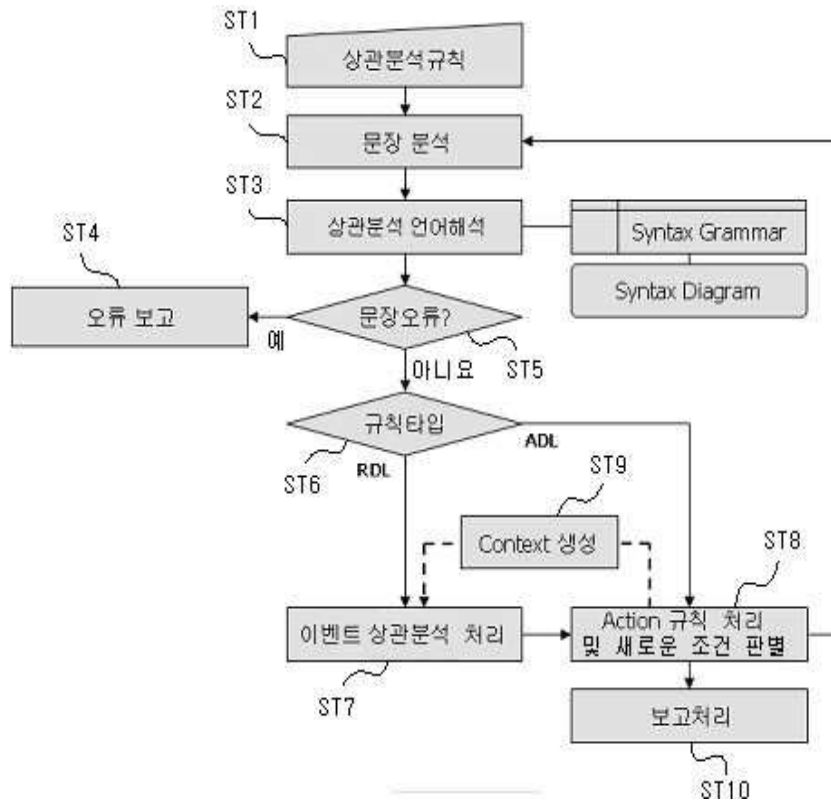
<50>

<51> 즉, 이 상관분석 규칙 스크립트의 가장 큰 특징 중 하나인, 문맥/조건(Context) 기반의 유연한 규칙표현이 가능함을 확인 할 수 있다.

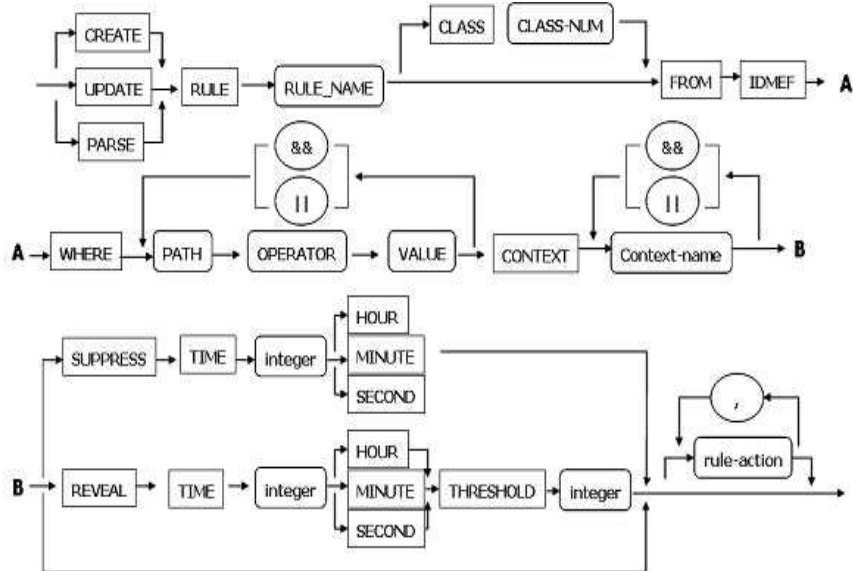
<52> 또한, 상위의 상관분석언어를 통한 상관분석 기능을 활용함에 있어서, 사용자가 보안이벤트를 추적함에 있어서



도면2



도면3



도면4

