The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 15, No. 1, pp.15-23, Feb. 28, 2015. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2015.15.1.15
JIIBC 2015-1-2

통합보안관리시스템 보안 분석 및 개선

Security Analysis and Improvement of Integrated Security Management System

김경신*

Kyung-Shin Kim*

요 약 본 논문은 지난 2012년 이후 떠오른 개념인 '빅 데이터'의 등장으로 정보보안 환경이 어떻게 변화되고 있는지, 빅 데이터와 관련된 분석 기술을 바탕으로 보안위협으로부터 어떤 통합보안시스템을 구축해야 하는지 제안하고자 한다. 빅 데이터 분야에 대해서는 최근 활용 분야에 대한 연구가 활발히 진행 중이며 APT(Advanced Persistent Threats)와 같은 보안 위협으로부터 보호하기 위해 빅 데이터 기반 통합보안관리시스템에서는 어떤 요구사항이 필요한 지 살펴보고자 한다. 또한, 기존 통합보안관리시스템과 현재 빅 데이터 기반 통합보안관리시스템을 비교 분석하며 한계점은 무엇이며 보완되어야 할 점을 제안하여 개선된 통합보안관리시스템을 제안하고자 한다.

Abstract This thesis proposes how data security has changed since the emergence of 'Big Data' in 2012 and the type of Integrated Security Management System that needs to be built against security threats, based on an analysis of Big Data. Much research has been conducted in Big Data. I need to think about what an Integrated Security Management System requires in order to safeguard against security threats such as APT. I would like to draw a comparison between the current Integrated Security Management System and one that is based on Big Data, including its limitations and improvements, so that I can suggest a much improved version of Integrated Security Management System.

Key Words : Big Data, IDS, IPS, Integrated Security Management System

Ⅰ. 서 론

최근 IT 환경은 디지털 데이터 빅뱅 시대로 진입하고 있다. 기업의 IT 활용단계는 제 1의 벽인 전자화, 정보화 단계를 넘어 제 2의 벽인 데이터 활용 단계로 넘어가고 있으며 전자화, 정보화 단계는 기업의 비용 절감을 강조하는 반면, 데이터 활용 단계는 새로운 이익의 창출에 초점을 맞추게 됨에 따라 대량의 데이터를 활용하여 분석한 데이터를 바탕으로 새로운 이익을 창출하려는 빅 데이터 분석 기술이 부각되고 있다.

한편 컴퓨터와 인터넷의 확산으로 실현된 정보화는 데이터 생산을 가속하여 2011년 한 해에만 1.8ZB(제타바이트)를 생산하는 데이터 폭증 현상에 직면하고 있으며, 향후에도 데이터는 기하급수적으로 증가하여 2020년에 이르면 현재 대비 50배로 폭증할 것으로 예상된다.[1]

이와 같이 데이터 홍수와 폭증으로 대표되는 "빅 데이

*정회원, 인덕대학교 방송영상미디어과
접수일자 : 2015년 1월 20일, 수정완료 : 2015년 2월 10일
게재확정일자 : 2015년 2월 13일

Received: 20 Jan., 2015 / Revised: 10 Feb., 2015
Accepted: 13 Feb., 2015
*Corresponding Author: kskim@induk.ac.kr
Dept. of Broadcasting & Media Engineering, Induk College, Korea

터"가 최근 특정 분야에 국한되지 않는 화두로 등장하였으며 빅 데이터 처리 및 분석 능력을 미래 경쟁력으로 인식하게 되었다. 세계경제포럼은 2012년 가장 주목할 기술로 빅 데이터를 지목하였으며 데이터 과잉 문제를 해결하고 데이터를 자산화하여 활용하는 것을 최우선 현안으로 선정하였다.[2]

본 논문에서는 보안 환경에 있어서 중요한 변수로 작용할 빅 데이터의 특성을 먼저 이해하고, 그에 따른 보안 위협을 살펴본 후, 그에 따른 통합보안관리시스템을 제안하고자 한다. 통합보안관리시스템에 대해서는 빅 데이터 이전과 빅 데이터 이후 현재 적용되고 있는 시스템이 무엇인지 살펴본 후 보안성이 강화된 통합보안관리시스템을 제안하고자 한다. 또한 현재 사용하고 있는 통합보안관리시스템과 그에 따른 한계점을 분석하고 향후 통합보안관리시스템이 필요로 하는 요건과 보완점을 제시하고자 한다.

II. 관련 연구

1. 단일 보안 시스템

1) 침입탐지시스템

침입탐지시스템(IDS: Intrusion Detection System)은 대상 시스템에 대한 인가되지 않은 행위와 비정상적인 행동을 탐지하고, 탐지된 불법 행위를 구별하여 실시간으로 침입을 차단하는 기능을 가진 보안시스템이다. 침입탐지시스템은 일반적인 보안시스템 구현 절차의 관점에서 침입차단시스템(IPS)과 더불어 가장 우선적으로 구축되었으며, 해킹 등의 불법 행위에 대한 실시간 탐지 및 차단과 침입차단시스템에서 허용한 패킷을 이용하는 해킹 공격의 방어 등의 목적으로 구축된다.

2) 침입방지시스템

침입방지시스템(IPS: Intrusion Prevention System)은 공격에 대한 탐지만을 하는 침입탐지 시스템의 한계성을 뛰어넘는 보안시스템이다. IPS는 공격 Signature를 찾아내 네트워크에 연결된 기기에서 발생하는 수상한 활동을 감시 및 중단시키는 보안 솔루션이다. 이것은 단순한 네트워크 단에서의 탐지가 제공하지 못하는 각종 서버를 위해 알려지지 않은 공격까지도 방어할 수 있는 실시간 침입방지 시스템으로 OS 레벨에서 실시간 방어와 탐지 기능을 제공한다.

IPS의 기존 보안제품에 대한 차별성은 사후 대응이 아닌 사전대응, 관리와 설치의 편이성, 설치와 동시에 사용 가능, Customizing 기능, Exceptions, Security Levels, Policies 설정 변경, 서버 보호를 제공하는 다단계 디자인, 위험한 공격을 막아내기 위한 한 가지 이상의 방법, 적용 및 관리의 편이성 등을 들 수 있겠다.[3,4,5]

2. 통합 보안 시스템

1) 통합보안관리시스템 동향

최근 몇 년간 보안 패러다임이 기술적 관점에서 관리, 서비스 중심으로 옮겨가고 있다. 과거에는 단일 보안 제품을 시장에 내놓아 기능적인 측면에서 보안을 유지하였으나 관리의 어려움으로 인해 보안에 필요한 각 기능을 하나로 통합한 보안 관리 시스템이 등장하기 시작했다.

표 1. 2000년대 통합보안관리시스템의 현황
Table 1. Current Status of Integrated Security Management System

시기	2000년대 이전	2000 ~ 2006년	2007년 이후
구분	SIM, SEM	ESM	SIEM
용도	IT단위시스템 로그통합 및 장애처리 모니터링용 활용	IT시스템과 보안시스템의 연계분석을 통한 보안관제용으로 활용	ESM기능을 포함. Application 연계를 통한 종합분석으로 활용
영역	IT시스템 위주의 통합 및 분석 중점	IT + 내부 보안영역 전체에 대한 알려진 보안위협 분석에 중점	알려지지 않은 보안위협 분석 포함
국내	로그세이버 등	이글루시큐리티, 인젠	윈스테크넷, 이글루시큐리티
해외	Cisco, Symantec 등	SIEM 기반 업체들이 대부분	HP, EMC, McAfee, IBM 등

방화벽, IDS, IPS, VPN, Anit-Virus 같은 각 보안 구성요소들이 전체 시스템의 일부로 제 기능을 하는 것뿐만 아니라 기존 구축된 보안시스템과도 완벽 연동 및 호환성을 유지하여 통합보안관리의 시너지 효과를 내고 있다. 현재 출시된 ESM제품의 경우 이 모든 요소를 고려한 통합보안관리시스템을 제공하고 있다.

SIEM은 기존에 SIM과 SEM에 ESM기능을 포함한 것이며,. SIM은 관리영역이 정보에 기반하고, SEM은 이벤트발생과 관련된다.[6] 따라서 어플리케이션 계층에 일어나는 보안 취약점과 위협을 상관관계 분석하여 구성한 것이 현재의 SIEM 시스템이라 할 수 있다.

2) ESM(Enterprise Security Management)

ESM은 국내 정보보호 업계에서 통용되는 용어이지만 학술 연구 단체 또는 산업 표준단체 등에 의해 정의되고 명세화 된 후 업계에서 통용된 것이 아니기 때문에, 그 의미 및 요구 기능에 있어서 정보보호 업체 및 소비자 또는 학계 및 산업계에서 다양한 관점으로 접근되고 있다.

ESM은 최근 통합관리 수준에서 벗어나 시스템자원관리(SMS), 네트워크자원관리(NMS) 등 전사적 자원 관리 시스템까지 포함하는 형태로 개발되는 추세여서 상용화된 제품이 거의 없을 정도로 아직 개발 단계에 불과하며 주요 보안솔루션 업체들이 최근 보안솔루션 상호연동을 위한 표준 프로토콜에 합의하면서 ESM 구현을 가속화하고 있어 국내에서도 데이터게이트, 이글루시큐리티, 인텐 등 보안업계들이 최근 ESM을 잇따라 출시하면서 제품 상용화에 주력하고 있다.

3) SIEM(Security Information & Event Management)

SIEM은 이전의 서로 다른 제품 카테고리인 SIM(Security Information Management)과 SEM (Security Event Manager)이 조합된 것으로 ESM의 해외 통합 솔루션을 뜻하는 명칭으로 사용되기도 한다. 이러한 기능은 기존 ESM을 빅 데이터 기술과 융합하면서 IT 시스템 전반에 걸쳐 생성되는 대량의 로그와 이벤트를 통합 관리하여 외부 위험을 사전에 예측하고, 내부 정보 유출을 방지할 수 있도록 하는 플랫폼을 제공한다. 의미 및 제품 기능에는 차이가 있지만 SEM, SIM과 SIEM은 상호 교환적으로 사용되었다. 보안 관리의 영역인 실시간 모니터링, 이벤트의 상관관계, 알림 및 콘솔 뷰는 일반적으로 Security Event Management(SEM)로 잘 알려져 있다. 두 번째 영역은 장기적 스토리지, 분석 및 로그 데이터의 보고를 제공하는 Security Information Management(SIM)이다.[7]

Ⅲ. 기존의 통합보안시스템 보안 분석

1. 기존 통합보안관리시스템 보안 현황

현재 SIEM을 활용하는 국내외 업체들의 솔루션 현황과 주요 특징들을 정리해 보았으며, 이처럼 SIEM은 대용량 데이터 분석을 위해 빅데이터 기술을 이용하며, 이를 통해 로그 데이터로부터 유의미한 보안 위협을 찾아낸다. 이러한 SIEM을 이용한 솔루션의 사례가 국내외에서 증가하고 있다.

국외의 경우 IBM과 McAfee와 같은 대형 해외 보안업체는 APT와 같은 고도의 사이버 공격에 대응하기 위해 기존의 SIEM기술을 서비스하고 있는 회사들과 전략적 인수 합병을 이루고 있으며, 국내의 경우, 기존 로그 및 데이터베이스를 이용한 솔루션을 제공하는 보안 업체에서의 분산시스템 및 빅 데이터 기술을 적용함으로서, IT 영역에서 발생하는 대용량 로그 데이터에 대한 처리의 효율성을 높여가는 형태로 SIEM 솔루션의 발전이 진행되고 있다. 기존의 보안기술에 새로운 IT기술을 접목시켜 나가는 형태로 발전 중인 국내의 솔루션과는 달리 국외에서는 이전에 개발되었거나 개발 중인 솔루션과의 통합을 통해 다양한 영역의 보안 솔루션 서비스를 제공하고 있다.

표 2. 국내외 통합보안관리솔루션 특징
Table 2. Features of Integrated Security Management System

구분	업체	솔루션	솔루션 주요 특징
국외	IBM	QRader	- 네트워크 상에서 전송되는 정보 실시간 관측 가능 - 모니터 소스로부터 로그 데이터와 함께 NetFlow 및 로그 이벤트 행동분석
	McAfee	ESM	- 위험 기반 활동 프로파일, 규칙 기반의 상관관계분석 강화 Advance Correlation Engine탑재
국내	넷크루즈	넷크루즈 SIEM	- 대용량 압축 아카이빙을 통한 대용량 로그데이터 처리 - 실시간 통합 로그 관리 보안 정보 및 이벤트 관리 모듈로 구성
	이글루 시큐리티	아이에스 로거	- 분산파일시스템(MDFS)을 통한 로그데이터처리 - 분산된 소형서버 및 메모리 디스크 활용한 로그저장 기능

2. 기존 통합보안관리시스템 보안 현황

빅 데이터의 개념이 부각된 이후 중요성 인식과 연구 및 마케팅 등에 이용하려는 노력은 매우 활발한데 비해 빅 데이터의 보안 및 개인정보 보호에 대한 노력은 상대적으로 낮은 수준을 보이고 있다. 개인정보보호법 강화에 따라 법적 제도적 제약사항도 많아지고 있는 실정이다. 이에 따라 기존 단위 보안시스템과 통합보안관리시스템에서 대량의 탐지 이벤트 발생 시 오탐(False Positive)이 다수 존재하므로 빅 데이터 시대의 위협을

분석하고 처리하는데 어려움이 있다.[8] 그러므로 기존 네트워크 중심의 시그너처 탐지가 아닌 어플리케이션 계층 중심의 이상행위 기반으로 빅 데이터를 처리해야 한다. 표 3.에서 볼 수 있듯이 현 보안 시스템의 한계는 APT 공격과 같은 지능화된 위협을 알아내기 어려운 점과 통합관리 측면에서 어플리케이션 계층에서의 내부유출을 고려하는 점, 빅 데이터를 이용한 지능화된 공격과 공격 간에 연관성 분석에서 개선점들이 보이고 있다.

표 3. 보안 시스템별 현행 분석 및 한계
Table 3. Limits and Analysis of Security Systems

구분	현행 분석	한계점
단위 보안 관리 시스템	- IP, 포트 중심의 네트워크 계층 탐지 - 알려진 공격 위주의 탐지 분석 - 보안이 취약한 특정 부분에 대해 특화되어 있음	- 알려지지 않은 공격 탐지 불가 - APT 위협을 탐지하기 어려움 - 단일 보안 시스템을 여러 개 사용할 경우 중첩되는 경우 발생 - 비용 중복 투자와 관리의 어려움 - 모든 보안 위협에 대처할 수 없다.
통합 보안 관리 시스템	- 네트워크와 단말 시스템 간 연관시 L3 계층 위주로 연계 - 단시간 내 데이터 분석가능 - 비용 절감 효과 - 운영 및 관리가 용이함 - 이기종 간 보안 시스템 간 연동을 지원함	- 사용자 및 어플리케이션 계층에서 단위 연관성을 분석하기 어려움 - 수개월 범위의 데이터 분석이 어려움 - 타 솔루션과의 연동이 어려운 경우 특정 IT 기업의 솔루션에만 의존해야 함

3. 현 통합보안관리시스템 세부 항목별 분석

본 절에서는 통합보안관리시스템 내 로그관리솔루션의 로그 수집 및 저장, 검색 및 분석 기능으로 구분하여 현재 사용되고 4개 사의 통합보안로그 솔루션의 특징과 취약점을 진단하며 보완해야 할 점을 도출하고자 한다.

(1) 로그 수집 및 저장

MapReduce기반의 분산처리 기술의 지원여부, 로그 솔루션 내에 자체 DBMS를 지원하는지, Agent, Syslog, SNMP 등 다양한 로그 수집 방식을 지원하는지, 신규로그 연동과 로그 압축 성능, 지원되는 비교적 안전한 로그 암호화 알고리즘을 지원하는 지 등을 세부 평가항목으로 정하였다.

표 4. 통합로그분석솔루션 평가기준과 평가항목
Table 4. Evaluation Items and Standards

기준	평가항목
로그 수집 및 저장	대량로그 수용기술 : MapReduce기반 분산처리 기술 지원
	로그 저장 DB : 자체 DB 지원 여부
	로그 수집 방식 : Agent, Syslog, SNMP 등
	신규 로그 연동 여부
	로그 파싱 및 필터링 기능
	로그 압축 성능 : 80% 이상
	고속검색을 위한 로그 인덱싱
	비정형 로그 인덱싱
	로그 암호화 알고리즘
	원본 무결성 검증 알고리즘
검색 및 분석 기능	원본 내 구문검색 기능
	드릴다운 상세분석 기능
	차등 상관분석 기능
	멀티레벨 상관분석 기능
	실시간 쿼리기반 이벤트 탐지
	사용자 지정 데이터 통계분석 기능

(2) 검색 및 분석 기능

로그 시스템 원본 내 구문 검색이 가능 여부, 드릴다운 상세 검색 기능 제공 여부, 차등 및 멀티레벨 상관분석 기능 제공 여부, 실시간 쿼리 이벤트 지원 기능, 데이터 통계분석 기능 지원 여부를 세부 평가항목으로 정하였다.

표 4. 의 기준을 바탕으로 국내외 4개 사의 통합보안관리 시스템 내 로그솔루션의 지원 여부를 평가하고 한계점을 살펴본 종합적 결과는 표 5. 와 같다.

평가항목에 추가하지 않았지만 통합보안관리시스템에서 다음 사항은 반드시 고려되어야 한다.

- 사용자별 특정 데이터에 따른 권한 분리 기능 제공
- 사용자 저작형 대시보드 지원으로 각종 통계 데이터 분석 용이성 제공
- 데이터 분석 결과와 쿼리 저장 기능으로 사용자 편의성 제공
- APT 공격 같은 각종 공격정보 룰 보유
- 수시로 업데이트 되는 보안취약점을 탐지하는 스캐너 연동에 대한 벤더사의 지속적 지원
- APT 공격 대응으로 네트워크 상에서 발생하는 행위를 프로파일링하여 비정상적 행위 및 패턴 이상징후 탐지

표 5. 4개사 통합보안관리시스템 평가표
(지원 : O, 미지원 : X, 일부지원 혹은 특정기준을 충족하지 못함 : △)
Table 5. Evaluation Results of Integrated Systems

기준	평가항목	A	B	C	D
로그 수집 및 저장	대용량로그 수용 기술	X	X	O	O
	자체 DB 지원 여부	X	X	O	O
	다양한 로그 수집 방식 지원 여부	O	O	O	O
	신규 로그 연동 여부	O	O	O	O
	로그 파싱 및 필터링 기능	O	X	O	O
	로그 압축 성능	O	O	O	O
	고속검색을 위한 로그 인덱싱	X	X	O	O
	비정형 로그 인덱싱	X	X	O	O
	로그 암호화 알고리즘	O	△	O	O
	원본 무결성 검증 알고리즘	O	O	O	O
검색 및 분석 기능	원본 내 구문검색 기능	X	X	X	O
	드릴다운 상세분석 기능	O	O	O	O
	차등 상관분석 기능	X	X	O	X
	멀티레벨 상관분석 기능	O	X	△	O
	실시간 쿼리 기반 이벤트 탐지	O	O	O	X
	사용자 지정 데이터 통계분석 기능	△	△	△	O

Ⅳ. 통합보안관리시스템 개선

1. 개선사항

위에서 분석한 4개의 통합보안관리시스템 제품을 비롯해 빅 데이터 환경의 관점에서 보완되어야 할 요건들을 제시한다첫째, 현재 많은 시스템에 SIEM 기능이 연동되지 않고 있는 상황이다. 위의 4개 사의 솔루션 분석 결과 C사를 제외하고는 SIEM과 관련된 로그 보안 기능이 제대로 구현되지 않았음을 살펴볼 수 있다. 둘째, 현재 SIEM 시스템 기능은 결국 IT 인프라에 관한 정보만 수집하므로 APT와 같은 공격에 대응하기 어려운 점도 존재한다. 이 점에 대해서는 기존 시스템 외에 조직의 보안 운영센터를 두어 빅 데이터 관련 분석가들이 다양한 데이터 유형에 대해 종합적인 분석이 요구된다. 또 기존 SIEM 기능은 실행 가능한 정보를 담고 있지 않기 때문에 많은 기관들이 SIEM 으로부터 원하는 일부 데이터만을 사용하고 있는 실정이다. 그러므로 기존 SIEM 기능은 APT와 같은 위협에 대해 통찰력, 가시성, 민첩성, 신속성을 갖춘 종합적인 분석 플랫폼으로서의 변화를 취해야 할 것이다.본 장에서는 기존 통합보안관리시스템을 강화할 두 가지 부분을 도입하여 해당 기능의 연동을 제안하고자 한다. 또 해당 기술을 적용했을 때 성능 비교와 기대효과를 제시한다.

가. CEP 아키텍처 도입

(1) CEP 아키텍처란

CEP(Complex Event Processing)란 여러 이벤트 소스로부터 발생한 스트림 데이터를 실시간으로 의미 있는 데이터를 추출하는 것을 의미한다. 여기서 스트림 데이터는 이벤트 데이터로 대량으로 입력되는 데이터, 시간 순서가 중요한 데이터를 의미한다. 이같은 스트림 데이터를 분석하기 위해서 기존 SQL 기반의 DBMS 분석으로는 어렵기 때문에 초당 수백에서 수십만 건의 이벤트 스트림을 처리하기 위한 아키텍처가 도입되었다. CEP 기술을 사용하면 데이터베이스 상에 저장할 필요 없이 메모리상에서 실시간으로 지연 없이 분석을 가능하게 한다.

(2) 기존 SQL기반 분석과의 비교

기존 SQL 기반 분석 방식과 CEP 기반 분석 방식을 비교한 내용은 아래 표와 같다.

표 6. SQL기반 로그분석과 CEP기반의 로그분석 비교
Table 6. Log Analysis Comparison of SQL with CEP

구분	SQL 기반 분석	CEP 기반 분석
쿼리 패러다임	Ad-Hoc 쿼리	연속된 스탠딩 쿼리
지연시간	데이터 규모 및 시스템에 따라 초, 시간, 일별, 월별로 다름	1000분의 1초 이하
데이터 발생 주기	초당 수백 이벤트 이하	초당 수만이벤트이상
처리 방식	선 저장 후 분석 방식	선 분석 후 저장 방식
매커니즘	쿼리 실행, 리포트 실행	결과에 따른 자동 모니터링
패턴	Ad-Hoc	시간주기지향 스탠딩쿼리
프로그램 처리 방법	SQL을 통해 분석	SQL에 스트림 데이터 처리 기능을 확장한 Query Language를 사용한다.

가장 주목해야 할 점은 지연시간과 처리 방식과 관련된 부분이다. CEP 기반 분석의 경우 메모리상에서 데이터를 로드하여 선 분석 후 저장하는 방식을 채택하고 있

기 때문에 데이터 발생 주기와 지연 시간에 있어서 상당한 차이가 발생할 수 있다. 특히 분석 대상 데이터의 크기가 크면 클수록 두 방식의 처리 속도 격차는 상당히 커진다는 것을 알 수 있다.

(3) 기대효과

첫째, 초당 수백 수십만 이상의 이벤트 스트림 분석이 가능하다. 기존 SQL기반의 AD-HOC processing은 데이터베이스에 저장해서 분석하기 때문에 많은 이벤트 발생 시 업데이트 지연현상이 발생하고 병목현상으로 이어진다.

그러나 CEP기반 엔진은 In-Memory 기반의 고성능 분석으로 선 처리 후 저장하는 메커니즘이므로 데이터 용량에 상관없이 지연시간을 대폭 줄여 빅 데이터 환경에서 빠른 대응을 가능하게 한다. 보통 500,000 TPS 수준의 강력한 성능을 가지고 있다.

둘째, 이미 지나간 데이터에 대해서 저장과 분석을 통해 보고서를 제공받고자 할 때 용이하다. Hadoop 및 NoSQL 데이터베이스의 다양한 저장소를 지원하는 기능을 갖추고 있다. 또 웹 표준을 준수하며, JAVA 기반의 플랫폼을 지원하는 데이터 스트림 분석 솔루션들이 현재 제공되고 있다.

나. 새 암호화 솔루션 연동

(1) 보안시스템 암호화에서 고려할 사항

기존 통합보안관리시스템에서 제공하는 암호화 방식은 AES, 3DES 등 비교적 강력한 알고리즘 기능을 지원하지만, 현재 컴플라이언스 이슈나 데이터 보호를 위한 기술적 요구를 충족하기에는 다소 부족하거나 일부 시스템의 경우 구성 시 원본 로그에 대한 무결성 및 암호화 기능이 포함하지 않는 경우도 있었다. 일부 외산 솔루션의 경우에는 일방향 알고리즘을 비롯해 SEED, SHA-256과 같은 검증된 알고리즘 계정단위 권한 관리 및 접근 통제 항목에 있어서 미흡한 점이 발견되었다.

이에 따라 주요 개인정보를 포함한 데이터에 대해 내외부 개인정보보호 감사에 대응 가능한 컴플라이언스를 준수하고 검증받은 암호 모듈을 이용한 암호화 기능을 제공해야 한다. 단순 DB 암호화를 넘어 다양한 시스템에서 적용 가능한 데이터 암호화 플랫폼 연동의 필요성을 제시하고자 한다. 그리고 다음과 같은 요소를 충족하는 새 DB암호화 방식을 제안하고 그에 따른 성능비교 및 기대효과를 제시하고자 한다. 우선 최근 사용되고 있는 DB 암호화 솔루션의 강점을 채택하여 통합보안관리시스템에서 채택해야 할 할 암호화 방식과 주요 기능들을 소개하고 암호문 조회 성능 비교, 암호화 복호화에 따른 DBMS의 부하율을 비교하여 새 암호화 방식에 대한 우수성을 입증하고자 한다.

표 7. 제안하는 암호화 방식에 관한 고려사항
Table 7. Considerations for proposed encryption method.

구분	기준	내용
인증	DB 암호제품의 필수 보안 기능 규정 준수 여부	국가정보원의 “DB암호제품 보안 요건” 및 “국가용 암호제품” 재검증 통과 여부
암호 모듈	인증된 암호화 알고리즘으로 최고의 보안성 보장	ARIA, SEED 등의 블록 알고리즘과 SHA-256 이상, HAS-160 등의 일방향 알고리즘 지원
키 기밀성	암호키 생성, 접근, 갱신, 파기 과정에서 안정성 확보	비인가자는 평문키에 접근 불가하여야 하며 제품 종료 시 메모리에 로딩된 키와 정책이 제로화 되어야 할 것
보안성	사용자와 기간에 따른 접근통제정책	사용자와 특정 시간대에 따라 비인가자의 접근 및 수정 차단 기능
감사	제품 관련 중요 이벤트에 대한 감사기록	암호화 데이터에 대한 접근 기록 저장, 제품 사용자 인증결과, 암호화 작업, 통제 정책 변경 기록 지원
가용성	고가용성 (High Availability) 보장	DB암호화 작업이 장시간 소요될 경우 서비스 중단이 없거나 최소일 것

(2) 새 암호화 시스템의 특징 및 성능검증

우선 기본 암호화 시스템의 방식으로는 API방식, Plug-In 방식 그리고 둘을 합친 하이브리드 방식이 있다.

기존 많이 활용되고 있는 Plug-In 방식은 운영안정성과 구축용이성이 높은 것이 특징이다. DB에서 제공하는 외부 함수를 사용하며, 별도 소스 수정은 없으나, 쿼리 최적화 시 소스 수정이 필요하다. 가장 큰 문제점은 DB 프로세스 종속에 따른 성능 저하이다. 또 DBMS에서 오브젝트 추가 및 변경에 따른 기존 DB Plan의 변경이 발생한다는 문제도 있다. 이 같은 문제에 대응하여 새 암호화 방식이 갖추어야 할 특성은 다음과 같다.

- 기존 DB의 Plan 변경 및 Object 추가 없이 성능 극대화 및 DB 무결성을 보장하여야 한다.

- 멀티스레딩 방식으로 암호화 복호화 시 다중 및 병렬 처리가 가능해야 한다.
- JAVA 기반으로 기본 DB서버의 OS와 하드웨어에 뛰어난 호환성을 제공해야 한다.
- 독립 프로세스 운영으로 부하분산처리에 매우 용이해야 한다. 즉, 다중화 부하 분산이 가능해야 한다.
- 암호화 되어 저장된 Index 기능을 제공하며 암호화 적용 후 Application의 성능이 보장되어야 한다.
- 3DES, AES, ARIA 등 강력한 암호 알고리즘의 채택

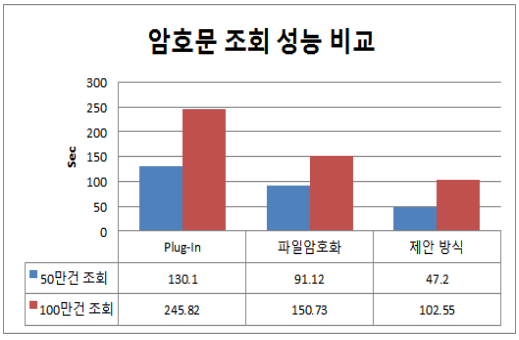

그림 1. 실시간 암호문 조회 성능비교 그래프
Fig. 1. Realtime Query performance comparison

그림 1.은 기존 Plug-In 방식과 파일 암호화 방식, 그리고 제안하는 방식의 실시간 암호문 처리에 따른 소요시간을 분석한 결과이다. 위에서 서술했듯 Plug-In 방식의 경우 DB 프로세스 종속에 따른 성능 저하가 발생하므로 경우에 따라서 필요 이상의 데이터 누적 시 사용하기 어려울 수 있음을 보여주고 있다. 그러나 제안하는 방식의 경우는 100만 건 조회 시 Plug-In 방식 대비 2.5배의 성능차이를 보여주고 있다.

그림 2.는 한 보험사의 3,000만 건의 Batch 일괄 정보를 업로드 시켰을 때 소요 시간을 각 방식 별로 비교한 것이다. Plug-In 방식의 경우 3,000만 건의 Batch 정보를 업로드 시키는 데 무려 5시간 가까운 시간이 소요되었다. Batch 업로드 기능을 비교적 효율적으로 사용하기 위해서는 1시간 이내로 마칠 수 있는 성능을 충족해야 하지만 필요 이상으로 시간이 소요되었기 때문에 대용량의 DB Batch 업로드 시 적합하지 않음을 입증했다.

그림 3.에서 쿼리 암호화 적용 전후의 CPU 점유율의 변화율을 측정하였다. SELECT 문 사용 시 성능에 영향을 주지 않았음을 확인할 수 있었다. UPDATE, INSERT 문의 경우에도 약 5~7% 정도의 리소스만 추가되었을 뿐 성능에는 거의 영향을 미치지 않았다.

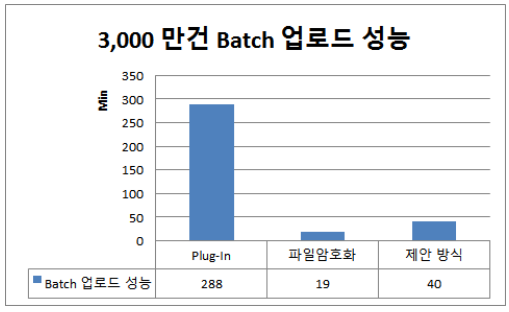

그림 2. 3,000만 건 DB Batch 업로드 성능 그래프
Fig. 2. DB Batch Upload Performance

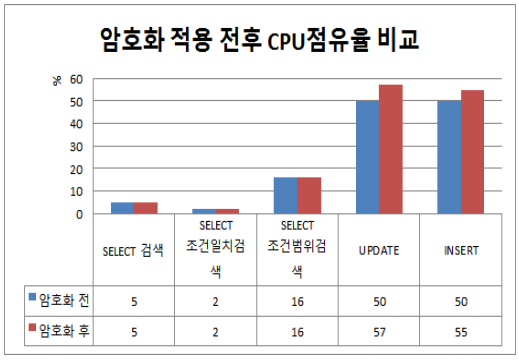

그림 3. 쿼리 암호화 적용에 따른 CPU 점유율의 변화
Fig. 3. CPU occupancy rates according to Query Encryption

(3) 기대효과

위에서 언급한 성능 비교 외에도 추가로 기대할 수 있는 항목들을 정리하였다.

- 암호화 이후에도 성능 저하가 거의 없다
- 사고 발생 또는 감사 요구 시 추적이 용이하다
- 중앙관리 서버의 고가용성이 보장된다
- 이기종의 OS와 DBMS 연동 가능하다
- 기밀 데이터 및 개인정보가 포함된 시스템 파일에 대한 완벽한 보호가 가능하다
- 운영 환경의 변화 없이 간단한 구축 과정으로 시스템의 무결성을 유지할 수 있다
- 사용자 행위 기반 접근제어 정책을 적용한 고객정보 보호가 가능하다
- 다양한 상용 DBMS에 모두 적용 가능하다.

2. 개선 요소를 적용한 통합보안관리시스템 기대효과

지금까지 통합보안관리시스템의 현황 및 보완 요소에 관한 부분을 살펴보았다. SIEM에 탑재 되어 있는 보안 요소의 부재, 보안 이벤트 수집의 어려움, APT 공격에 대해 장기적으로 대응하기 어려운 점을 확인할 수 있었다.

본 절에서는 표 8을 통해 제안한 CEP 아키텍처 도입과 새 암호화 솔루션 연동 의 두 항목에 대한 부분을 충족시킨 통합보안관리시스템과 기존에 사용되던 표 5. 와 비교하였다. 그리고 제안한 항목을 추가한 통합보안관리시스템이 보여줄 수 있는 기대효과를 제시하고자 한다.

표 8. 제안하는 기준을 반영한 통합보안시스템 평가표
Table 8. Proposed System Evaluation Result

기준	평가항목	A	B	C	D	제안
로그 수집 및 저장	대용량로그 수용 기술	X	X	O	O	O
	자체 DB 지원 여부	X	X	O	O	O
	다양한 로그 수집 방식 지원 여부	O	O	O	O	O
	신규 로그 연동 여부	O	O	O	O	O
	로그 파싱 및 필터링 기능	O	X	O	O	O
	로그 압축 성능	O	O	O	O	O
	고속검색을 위한 로그 인덱싱	X	X	O	O	O
	비정형 로그 인덱싱	X	X	O	O	O
	로그 암호화 알고리즘	O	△	O	O	O
	원본 무결성 검증 알고리즘	O	O	O	O	O
검색 및 분석 기능	원본 내 구문검색 기능	X	X	X	O	O
	드릴다운 상세분석 기능	O	O	O	O	O
	차등 상관분석 기능	X	X	O	X	O
	멀티레벨 상관분석 기능	O	X	△	O	O
	실시간 쿼리 기반 이벤트 탐지	O	O	O	X	O
	사용자 지정 데이터 통계분석 기능	△	△	△	O	△

제안한 시스템이 대부분의 평가항목을 충족시킬 수 있음을 확인할 수 있다. 먼저 제시한 4개사 솔루션의 경우 각 솔루션마다 우수한 기능이 탑재되어 경쟁력을 갖추고 있었지만, 우수한 평가를 받는 솔루션이라도 적어도 한두 가지 항목에 대해서는 필요한 기능이 제공되지 않아 다소 불편함이 따랐다. 그러나 제안된 시스템 내에서는 적어도 기능이 제공되지 않은 부분에 대한 불편함은 사라졌다고 볼 수 있다.

마지막으로 빅 데이터 이후의 통합보안관리시스템 항목과 비교하여 제안한 통합보안관리시스템의 대표적인 내용을 표 9. 에 비교하였으며, 정리하면 통합보안관리시스템은 분산 처리 기반 아키텍처로, 전송 계층부터 어플리케이션 계층에 이르기까지 상호 연관성 분석에 역점을 두고 있다. 빅 데이터의 분석용으로 활용되는 웹 마이닝 기반의 단위보안로그를 통합하여 보안 로그 데이터를 실시간으로 자동화, 시각화, 군집화 요소를 적용하여 동시에 대용량의 데이터를 수집하는 데 한계점이 없어야 한다.

표 9. 기존 통합보안관리시스템과 개선된 시스템 비교
Table 9. Comparison of proposed system with existing system

구분	기존 통합보안관리시스템	개선된 통합 보안관리시스템
특징	. 4~7계층 연관분석 . 보고서 및 예경보 가능 . 장기간 크로스 컨텍스트 분석	. 기존 단일보안시스템 및 네트워크 장비 간 확장성과 연동성 제공
단위보안로그	. 4~7계층 . IP, 프로토콜, 어플리케이션, 사용자 중심 . 콘텐츠, 컨텍스트 분석로그	. 콘텐츠, 컨텍스트 분석로그 . 웹 마이닝 기반
모니터링	. 데이터 중심 양방향 트래픽 분석	. 로그 데이터 중심 상호연관성 분석 . 외부에서 내부로 유입, 유입 트래픽 분석
분석 대상	. 사용자, 어플리케이션,서비스 . 보안 관제, 내부정보 및 개인정보 모니터링	. 사용자 및 데이터 행위 프로파일링 . 내부/개인정보
분석 방법	. 위험관리 중심 . 사용자 행위 중심 공격 탐지 . 내부정보 및 개인정보 유출탐지	. 각 시스템의 구성요소로부터 로그 수집하여 상호연관분석 . CEP 기술 사용
시스템 구조	. 무정지 결함 허용 구조	. 분산 처리 구조
로그 수집 대상	. Queues,WebService 등	. 동일

V. 결론

본 논문에서 현 통합보안관리시스템에 두 가지 제안 사항을 반영하여 성능 변화를 기록한 기대효과를 분석하였다. 본 논문의 제안 사항 외에도 현재 보안 사고를 예방하고 분석하기 위해서는 가장 이상적인 시스템에 가까운 모델을 연구하거나 지속적인 사이버 공격의 진화로 발생 가능한 다양한 상황에서 시스템 보완이 필요하다. 또 본 논문에 제안 사항을 통합보안관리시스템에 도입하는 과정에 있어서도 각 구성요소가 공통의 컴플라이언스

를 충족하는지, 해당 솔루션 도입에 따라 비용 측면에서 최소의 요건을 충족할 수 있는지도 고려해야 한다.

앞으로 SIEM은 빅 데이터 규모의 보안 정보를 수집하기 위한 분산 데이터 아키텍처를 제공함으로 네트워크 행위 프로파일링을 통한 이상 징후를 포착하여 위협 정보를 공유하는 등 다양한 개선 사항이 제시되고 있다.

또 통합보안관리시스템에서 중요한 부분은 차지하고 있는 통합로그분석시스템의 각 기준에 대해서 현 상황을 분석하고 보완해야 할 측면에 대해서 제시하였다. 또, 주된 내용으로 다루지는 않았지만 통합보안관리시스템은 운영적인 측면에 있어서 데이터 보안, 애플리케이션 보안, 엔드 포인트 보안과 시스템 전체를 관리하는 통합 솔루션을 어떻게 통합시킬 것인가에 관한 다양한 모델 연구도 과제로 남아있다.

APT와 같은 지능화된 공격이 날이 갈수록 강화되고 클라우드 컴퓨팅 환경의 도입으로 IT 환경이 빠르게 변화하고 있다. 이런 흐름에 대응하기 위해서는 본 논문에서 제시한 보완 기준을 반영하여 강화하는 것 뿐 아니라 관리 측면에서 발생할 수 있는 보안 위협 요소, 내부자에 의한 정보 유출과 같은 관리 측면의 위험을 방지하도록 노력해야 한다. 또한 다양하고 더 나은 평가 기준을 제공할 수 있도록 노력해야 하며 지속적으로 변하고 있는 네트워크 환경에서 유연하게 대처할 수 있는 방향으로 고민하고 발전해야 할 것이다.

References

[1] James Manyika etc, "Big data: The next frontier for innovation, competition, and productivity", McKinsey Global Institute, 2011
[2] Jyung Hyun Kim, "BigDataplatform-based socia-l net workdata analysis paractices", 2012
[3] John P. Wack, "Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls", NIST Special Publication, 1994
[4] KISA Internet Weekly, 2012.08.02
[5] Tyler Bell, "Big Data: An oppertunity in search of a metaphor", rader.oreilly.com/2011/02/big-data-meterphor.html
[6] NACS : Client/Server Security Assessment and Awareness, Accessed; 2009.04
[7] Ahn, C. W. and S. G. Hwang, "Big Data technologies and main issues", Journal of Korean Institute of Information Scientist and Engineers, Vol.30, No.6, pp.10-17, 2012
[8] Kyung-Bae Min, Jang-Mook Kang, "Rights to Control Information and Related Security Technologies on the CyberSpace", Journal of the institute of internet, broadcasting and communicaion, Vol.10, No.2, pp.136-142, 2010

저자 소개

김 경 신(정회원)

- 1983년 : 성균관대학교 전자공학과 학사
- 1985년 : 성균관대학교 전자공학과 석사
- 1997년 : 성균관대학교 정보공학과 공학박사
- 1995년 ~ 현재 : 인덕대학교 방송영상미디어과 교수

<관심분야 : 정보보안, 네트워크 보안, 콘텐츠 보안>

※ 본 연구는 인덕대학교 교내학술연구비 지원과제임