Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.27, NO.3, Jun. 2017 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2017.27.3.705

실효적인 정보보호관리 통제를 위한 맞춤형 보안정책 연구

손 영 환,† 김 인 석‡
고려대학교 정보보호대학원

A Study on the Customized Security Policy for Effective Information Protection System

Young-hwan Son,† In-seok Kim‡
Korea University, Graudate School of Inforamtion Security

요 약

오늘 날 세계는 과학기술과 정보통신의 비약적인 발전으로 정보화 기반 아래 실시간 정보 공유와 의사소통이 가능한 거대한 하나의 공동체로 발전하고 있다. 이러한 정보화의 이면에는 해킹, 바이러스 등에 의한 정보자산의 침해, 사이버 테러, 개인정보 및 중요정보 자산의 무단 유출과 같은 역기능은 지속적으로 증가하여 심각한 사회문제로 대두되고 있다. 침해사고 및 개인정보 유출 시 마다 정부 주도의 개인정보 보호를 위한 관련 법규 강화와 종합대책 수립 등 많은 규제정책이 발표되었고, 기업들 역시 정보보안의 중요성에 관한 인식이 점차 증가하면서 다양한 노력들을 기울이고 있다. 그럼에도 불구하고 개인정보 유출 및 산업기밀 유출과 같은 정보보안 사고는 계속적으로 발생하고 있으며 그 빈도 또한 줄어들고 있지 않는 것이 현실이다. 이에 본 논문에서는 획일적이고 기술 중심의 보안정책이 아닌 사용자 중심의 보안정책 수립을 통하여 다양한 업무환경 및 서비스 지원과 동시에 보안위협 대응 시 보다 신뢰성 있고 효과적으로 대처할 수 있는 사용자 맞춤형 보안정책 방법론을 제시하였다.

ABSTRACT

Today, the world is evolving into a huge community that can communicate with real-time information sharing and communication based on the rapid advancement of scientific technology and information. Behind this information, the adverse effects of information assets, such as hacking, viruses, information assets, and unauthorized disclosure of information assets, are continually increasing as a serious social problem. Each time an infringement of the invasion and personal information leaks occur, many regulatory policies have been announced, including stricter regulations for protecting the privacy of the government and establishing comprehensive countermeasures. Also, companies are making various efforts to increase awareness of the importance of information security. Nevertheless, information security accidents like the leaks of industrial secrets are continuously occurring and the frequency is not lessening. In this thesis, I proposed a customized security policy methodology that supports users with various business circumstances and service and also enables them to respond to the security threats more confidently and effectively through not a monotonous and technical but user-centered security policy

Keywords: Security Threat, Information Security, Security Policy, Operation Sympton

I. 서 론

1.1 연구 배경 및 필요성

오늘 날 세계는 과학기술과 정보통신의 비약적인 발전으로 정보화 기반 아래 실시간 정보 공유와 의사소통이 가능한 거대한 하나의 공동체로 발전하고 있다. 이를 통해 제4차 산업혁명은 로봇공학, 인공지능, 나노기술, 생명공학, 사물의 인터넷, 3D 인쇄 및 자율차량을 포함한 여러 분야에서 초연결과 초지

Received(05.11.2017), Modified(1st: 05. 30. 2017, 2nd: 06. 12. 2017), Accepted(06. 12. 2017)

† 주저자, ambitions21@naver.com
‡ 교신저자, iskim11@korea.ac.kr(Corresponding author)

능과 같은 새로운 기술혁신이 나타나고 있다[1]. 그러나 이러한 정보화의 이면에는 해킹, 바이러스 등에 의한 정보자산의 침해, 사이버 테러, 개인정보 및 중요정보 자산의 무단유출과 같은 역기능은 지속적으로 증가하여 심각한 사회문제로 대두되고 있으며, 이에 대한 사회적 관심과 정보보안을 위한 다양한 노력이 요구되고 있다[2].

침해사고 및 개인정보 유출 시 마다 정부 주도의 개인정보보호를 위한 관련 법규 강화와 종합대책 수립 등 많은 규제정책이 발표되었고, 기업들 역시 정보보안의 중요성에 관한 인식이 점차 증가하면서 다양한 노력들을 기울이고 있다. 그럼에도 불구하고 정보보안 사고는 계속적으로 발생하고 있으며 그 빈도 또한 줄어들고 있지 않은 것이 현실이다[3].

또한 보안관리를 위한 구조적이고 제도적인 대책과 보안의 주체인 기업 내 사용자에 대한 인식 및 이해 수준 향상에 대한 노력은 상당 부분 부족한 것으로 판단되며, 특히 내부 사용자에 의한 보안위협은 치명적인 결과를 초래하므로 중요한 보안관리 과제로 대두되고 있다[4].

최근의 침해사고 및 개인정보 유출 사고 사례를 보면 해당 기업은 이미 상당 수준의 보안 솔루션이 구축되어 있었음에도 불구하고 외부 해커 또는 악의적인 내부 사용자에 의한 정보유출 행위를 탐지/차단하는데 실패하였다. 이에 반복되는 보안사고의 원인을 살펴보고 효과적으로 침해 및 개인정보 유출 사고를 사전에 탐지/예방할 수 있는 해결방안을 찾기 위한 이론적인 연구가 필요하다고 판단된다.

1.2 연구 목적

개인정보 관련 규제강화에 따른 보안통제 및 점검대상의 증가와 지능화되어 가는 보안위협 대응을 위한 보안 솔루션 증가 등 기업/기관의 보안정책 수립에 많은 어려움이 발생하고 있다. 또한 다양한 업무환경 및 서비스 지원을 위한 비즈니스 차원의 보안정책 예외와 같은 요구사항도 증가하고 있다. 이에 본 연구에서는 최근의 개인정보 사고사례 분석 및 기술적 대응방안의 개선을 위한 추가 보안대책을 수립하였다. 또한 사용자 중심의 위협평가를 통해 보안등급을 산출하고 사용자 맞춤형 보안정책 방법론을 제시하였다. 이를 통해 다양한 업무환경과 서비스를 지원함과 동시에 기업의 보안사고 대응 역량도 한층 강화하였다.

본 논문의 구성은 다음과 같다. 제2장에서는 개인정보 유출사고 사례 분석 및 최근 보안위협의 기술적 보안대응 방안을 살펴보고, 정보보호 대책수립을 위한 위험평가 방법론에 대한 선행연구를 하였다. 제3장에서는 현재의 정보보호 정책현황 파악 및 준수를 위하여 개인정보보호 관련 법규 및 정보보호관리체계(ISMS) 인증제도에 대해 살펴보았고, 현재의 보안정책 개선을 위해 문제점을 조사하였다. 제4장에서는 사용자 관점의 보안정책 수립을 위한 사용자 맞춤형 보안정책 방법론을 제시하였다. 제5장에서는 사용자 맞춤형 보안정책 방법론에 대한 A사 기준의 사례검증과 사용자 보안등급별 보안대책의 실효성을 검증하였다. 마지막 제6장에서는 결론과 향후 발전방향에 대하여 논하였다.

II. 관련 연구

2.1 개인정보 유출사고 사례분석

최근에 발생한 개인정보 유출사고들을 살펴보면 공격유형과 과정이 유사한 형태로 반복되어 발생하고 있다. Fig. 1. 같이 천만 건이 넘는 개인정보 유출 사례를 살펴보면, 외부 공격자가 인터넷/웹메일을 이용한 APT공격 및 공개용 홈페이지 취약점을 이용한 외부 침해행위와 내부 악의적인 사용자가 보조기억장치를 이용한 개인정보를 유출사고로 분류할 수 있다[5].

외부 침행행위로 주로 사용되는 APT 공격은 온라인망을 통해 기업 내 정보시스템 서버와 DBMS, 업무용 PC 등이 해킹을 당하거나 악성코드에 감염되어 보안 피해가 발생하는 유형이다. 이 같은 경우

Company	Day	Number (Ten Thousand)	Attack Tool	Attack Course
인터파크	'16.05	1,030	APT	Mail, Server(file sharing), PC, DBMS
KT	'14.03	1,200	Web Proxy Tool	Web Server (Web Vulnerabilities)
KCB (신용정보회사)	'14.01	10,400	USB	PC,USB
넥슨	'11.11	1,320	APT	Mail, PC, Server(backup server)
네이트	'11.07	3,500	APT	Internet(update), PC, DBMS
옥션	'08.02	1,081	WebShell	Web Server (Web Vulnerabilities)

Fig. 1. Stories of massive personal information leaks

기업 내부자의 도움 없이도 해커의 개인적인 능력에 의해 보안 피해가 발생할 수 있다는 특징이 있다. 기업 내의 시스템이나 업무용 PC가 온라인으로 외부와 연결되어 있기만 하다면 해커는 유출하고자 하는 정보에 무리 없이 접근이 가능했다[3].

내부 악의적 행위에 의한 보안사고는 현재 가장 광범위하게 발생하고 있는 보안사고의 유형인데, 기업 내부에 있는 직원 혹은 외부 협력업체의 직원이 고의로 업무용 PC에서 보조기억장치(USB, 외장하드 등)로의 자료를 이동시키거나 인쇄, 복사 그리고 촬영 등의 행동으로 외부로 반출하는 행위가 모두 포함된다. 과학 기술의 발달로 인해 조그만 장치에 엄청난 용량의 파일을 저장할 수 있는 보조기억장치는 보안성에 끊임없는 문제에도 불구하고 가장 광범위하게 사용되고 있는 저장장치이다[3].

이에 본 연구에서는 천만 건이 넘는 개인정보 유출사례를 중심으로 살펴보고 공통된 문제점과 이에 대한 외부 공격자의 APT공격과 내부 악의적인 행위에 의한 개인정보 유출사고 시 사용된 접근매체(인터넷,웹메일,PC,서버,DBMS)를 중심으로 보안대책을 수립하고자 하였다.

2.2 최근 보안위협의 기술적 대응방안

2.2.1 APT 공격방식의 특징 및 대응

APT는 해킹을 시도하는 개인이나 그룹이 명확한 목적을 가지고 특정 대상을 겨냥하여 지능적이고 복합적인 방법을 동원하여 지속적으로 공격하는 위협형태를 말한다[6]. APT는 악성코드의 생존율을 높이기 위해 사전조사, 제로데이 취약점 공격, 사회공학기법 적용, 은닉, 적응, 지속 등의 공격기법을 조합하여 장기적으로 원하는 목적이 달성될 때까지 공격한다[7].

APT 공격 대응을 위하여 업무 외 웹사이트 접속금지, 의심스러운 웹메일 열람금지, 시그니처 기반의 APT 솔루션을 통한 대응을 하고 있다. 그러나 우리를 위협하는 공격은 점점 더 지능화되고 있기 때문에 방어하기에는 많은 한계점들이 존재하고 있다. APT 공격은 다양한 보안장비와 정보보호관리 체계를 구축·운영하고 있더라도 조기 식별 및 대응이 어려운 측면이 있다[8].

이에 본 연구에서는 사용자에게 부여된 접근매체(인터넷,웹메일,PC,서버,DBMS)별 접근권한를 통합분석하여, 고위험군 사용자의 접근권한 축소 및 추가 보안대책 수립을 통해 APT 공격과 같은 지능화된 보안위협을 최소화하고자 하였다.

2.2.2 이상징후 탐지를 위한 통합 보안관제 시스템

최근의 보안시스템 로그 관리 분야의 동향은 통합관리(ESM)에서 위험관리시스템(RMS), 보안 정보 및 이벤트 관리(SIEM)에 이르기까지 지속적으로 진화하고 있다. 이 가운데 로그 통합관리를 위해 등장한 SIEM은 이기종 환경의 인프라 및 보안로그를 효율적으로 통합 운영하고 리스크를 낮추기 위한 해결책으로 받아들여지고 있다[9].

이런 기술적 발전을 통해 기업 내부적으로 운영되는 보안관리, 네트워크 관리, 부대설비 관리, 서버 관리 등 모든 보안 시스템에서 발생되는 로그를 통합 수집 및 상관분석을 통해 외부침입 및 내부 악의적인 행위 등 이상징후 탐지 및 분석를 위한 통합 보안관제 시스템으로 발전하고 있다. [10]

이에 본 연구에서는 외부 공격자 및 내부 악의적인 행위를 파악하기 위해 통합 보안관제 시스템을 통해 수집된 이상징후 정보와 사용자 보안정책(접근권한,보안준수 충성도 등) 정보를 통합분석함으로써 오탐은 최대한 줄이고 정탐비율을 높임으로써 신속·정확한 보안위협 대응체계를 구축하고자 하였다.

2.3 위험평가 방법론

위험이란 원하지 않는 사건이 발생하여 손실 또는 부정적인 영향을 미칠 가능성을 정의할 수 있다.

손실 및 위험의 수준을 표현하는 방법에 따르 크게 정량적인 방법과 정성적인 방법으로 구분될 수 있으며, 평가된 위험의 규모에 따라 수용할 위험과 수용할 수 없는 위험을 분류하고 수용할 수 없는 위험에 대해서는 위험 규모에 따라 우선순위에 따른 적절한 대응책을 마련해야 한다.

위험의 유형과 규모를 확인하기 위해서는 위험에 관련된 모든 요소들과 그들이 어떻게 위험의 규모에 영향을 미치는 지를 분석해야 한다. 일반적으로 IT 환경에서의 위험은 자산, 위협, 취약성의 함수로 정의될 수 있다. [11]

지금까지의 위험평가 기준은 IT자산 중심의 개별적 통제항목 중심으로 평가되었으나, 본 연구에서는 사용자 중심의 보안정책(접근권한, 보안준수 충성도

보안정책 예외 등) 정보를 통한 사용자별 위험평가 및 그에 대한 보안대책을 수립하고자 하였다.

2.4 선행연구와의 차이점

본 연구는 첫째, 최근의 침해사고 및 개인정보 유출 사고 시 사용된 공격방식과 접근매체(인터넷,웹메일,PC,서버,DBMS)를 중심으로 보안정책을 수립하고자 하였다, 둘째, APT공격과 같은 지능화된 보안위협을 최소화하고자 사용자 접근권한를 최소화하고 통합 보안관제 시스템의 정탐비율을 높이기 위하여 이상징후 정보와 사용자별 보안등급 정보를 활용하고자 하였다. 셋째, IT자산 중심의 위험평가가 아닌 사용자 중심의 보안정책(접근권한,보안준수 충성도 보안정책 예외 등) 정보를 반영한 위험평가 및 사용자 맞춤형 보안정책을 수립하고자 하였다.

III. 현재의 정보보호정책 현황 및 고려사항

3.1 개인정보 관련 법규의 강화

사이버 공격이 지능화되고 각종 보안사고가 발생하면서 정보보호 관련 규제도 지속적으로 늘어나고 있다. 정부와 관련 부처는 중복규제를 없애고 규제간 상충되는 항목을 개선하려는 노력을 지속하고 있지만, 기업/기관에서는 규제준수에 어려움을 겪는 것이 현실이다. 최근 개정된 개인(신용)정보보호를 위한 관련 법규 및 종합대책을 살펴보면, 금융위원회의 금융전산 망분리 가이드라인('13.09) 및 개인정보 유출 재발방지 종합대책('14.03), 신용정보 이용 및 보호법의 징벌적 과징금·손해('15.02), 금융감독규정의 보안점검 강화('15.04), 개인정보보호법의 주민등록번호 암호화('16.01), 정보통신망법의 ISMS 인증의무기관 확대('16.06) 등을 통해 개인정보보호를 위한 관련 법규 및 규정을 강화하고 있다.

3.2 정보보호관리체계(ISMS) 인증 기업의 확대

정보보호관리체계(ISMS) 인증은 정보보호에 대한 인식을 제고하여, 보호되어야 할 정보통신망 및 정보자산의 안전 신뢰성을 강화하고 국제적 신뢰도를 향상시키기 위한 목적으로 제정되었다. 어떤 조직이 정보자산의 기밀성, 무결성, 가용성을 실현하기 위한 관리체계를 수립하여, 운영하고 있을 때, 그 관리체계가 방송통신위원회가 고시한 정보보호관리체계 인증심사 기준에 적합한지를 방송통신위원회가 지정한 기관, 한국인터넷진흥원에서 적합성 여부를 보증해 주는 것이다[12].

조직의 중요한 정보자산을 보호하기 위해 조직별로 부분적, 일회성 활동을 통해 단편적 대응을 하였다면 ISMS 구축을 통해 중요한 자산보호를 위해 조직 전체에 걸쳐 서로 협력관계를 유지하여 지속적 체계적 대응을 통하여 정보보안 사고의 발생가능성을 줄이고 사고가 발생했을 경우에도 손실경감으로 기업가치 향상과 비즈니스 연속성을 보장하고자 정보보호관리체계 인증 의무대상 기업을 확대하고 있다.

3.3 고려 사항

3.3.1 위반사항 지속발생

침해사고 및 개인정보 유출사고 시 마다 감독기관은 규제정책을 모든 기업에 강제화함으로써 많은 기업들이 한정된 자원으로 모든 보안요건 충족의 어려움을 호소하고 있다.

이를 입증하듯 금융위원회에서 발표한 금융기관 IT부문 점검 결과 조치위반 사항이 Fig. 2. 에서 보는 바와 같이 다수 발생하였고 도메인별 조치위반사례를 살펴보면 인적관리, 운영관리, 접근관리, IT도입개발 부분에서 많은 조치 위반사례가 발생하였다[13].

반대로 기업/기관이 IT부분 모든 점검항목을 준수하였다고 보안사고가 발생하지 않는다고 어느 누구도 장담하지 못 할 것이다. 체크리스트 방식의 측정항목 개발 및 점수 환산 방식, 근본적인 재검토가 필요하다. 유연성과 즉시적인 변경을 반영할 수 있는 구조로 전환해야 되어야 할 것이다[14].

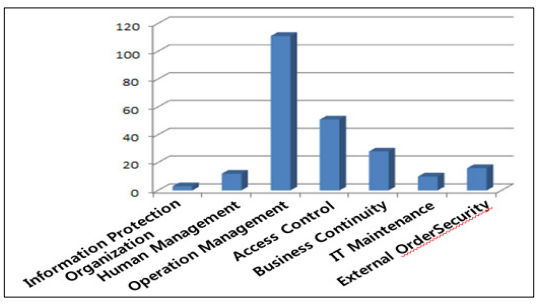

Fig. 2. Security Policy Violation Number of Financial Institutions

3.3.2 인적보안의 어려움

피터 드러커가 "조직에서 가장 민감하고 다루기 어려운 문제가 사람 다루는 것이다"라고 언급 하였듯이 결국 인적보안 관리도 사람을 다루는 문제로 인간의 내면을 관리하는 것이기 때문에 어려운 것이다. 환경의 지배를 받는 사람의 의식구조와 내면을 관리해야 하는 인원보안은 태생적으로 적용수단과 기술에 한계를 느낄 수 밖에 없다. 첫째, 인원보안은 관리주체와 객체가 사람이며 보호대상인 동시에 경계대상이 되는 양면성을 가지고 있어 사람은 가장 위험한 침해요소이며 위협의 대상이다. 둘째, 인간의 내면성 접근에 한계가 있어 예방조치가 어렵다. 셋째, 인간은 환경의 지배를 받으므로 정신적, 심리적 변화 가능성이 상존한다. 넷째, 보안관리는 인간의 행위규제를 수단으로 하고 있어 저항이 따른다. 다섯째, 제도권을 벗어난 자(퇴직,전직자 등)에 대한 보안관리는 사실상 어렵다[15].

이러한 한계를 조금이라도 극복하고 인간의 내면을 고려한 보안대책을 수립하기는 쉽지 않은 것이 현실이다. 따라서 역할과 접근의 정의를 통해 기준점을 마련하고 그에 따른 제약을 둔다면 다소나마 기업 내 사용자의 반발이 줄어들 것이다.

3.3.3 보안통제 및 관리의 어려움

개인정보 보호를 위한 관련 법규 및 컴플라이언스 준수를 위하여 많은 보안 솔루션과 보안정책이 적용됨으로써 업무 효율성 저하 및 보안관리 측면의 업무 부담이 가중되고 있고, 다양한 업무 환경 및 서비스 지원을 위해 불가피한 보안정책 예외처리를 적용 함으로써 보안정책 수립 및 관리를 위한 이중의 어려움이 발생하고 있다.

2011년 4월 농협 전산망 마비 사태 이후 금융 정보기술(IT) 보안강화를 위해 도입한 '557규정'은 전체 인력 5%는 IT인력, IT인력 5%는 정보보호 인력, 전체 IT예산 가운데 7%는 정보보호 예산으로 배정하라는 규정이다[16].

이마저도 규제개혁 철폐차원에서 완화한다는 발표가 있었다. 이를 기업들이 악용한다면 보안대책 수립 및 운영을 위한 최소한의 보안자원 확보도 어려워 질 것이다.

IV. 사용자 맞춤형 보안정책 방법론

본 연구에서 제시한 사용자 맞춤형 보안정책 방법론은 최근 침해행위 및 개인정보 유출 시 사용된 접근매체를 기준으로 기술적 보안대책과 사용자 보안정책 정보를 융합하여 현재의 보안정책 문제점 및 취약점을 개선하고자 하였다.

제2장의 관련연구를 통해 첫째, 침해사고 및 개인정보 유출사고 시 외부침해 공격은 지능화된 APT 공격기법을 주로 사용하여 외부에서 인터넷, 웹메일, 업무PC, 서버, DBMS 의 접근매체를 경유하여 공격에 성공하였고, 내부 악의적인 행위자는 보조기억장치를 이용하여 업무PC, 서버, DBMS의 접근매체를 이용하여 정보유출에 성공하였다. 둘째, 지능화되어가는 공격대응을 위하여 APT공격대응, 통합 보안관제 시스템을 이용한 기술적 보안대책을 수립하고 있으나, 전체 사용자 대상의 동일 기준의 시나리오와 룰 등으로 과탐 및 오탐으로 신속한 분석 및 대응에 어려움이 발생하고 있고, IT자산 중심의 위험평가외 인적보안 측면의 보안위험이 평가도 필요하였다. 제3장에서는 사이버 공격의 지능화 및 각종 보안사고가 발생하면서 정보보호 관련 규제 강화 및 보안위협 증가에 따른 보안통제 및 관리의 어려움이 가중되고 있다.

Fig. 3.는 사용자 관점의 맞춤형 보안정책 수립을 위하여 첫째, 침해사고 및 개인정보 유출 시 사용된 5개의 접근매체(인터넷, 웹메일, 업무PC, 서버, DBMS)를 정의하였다. 둘째, 접근매체 사용을 위한 사용자의 접근권한을 정의하였고 셋째, 사용자의 보안정책 준수여부와 보안위협 행위 등을 통한 보안준수 충성도를 정의하였다. 넷째, 이상징후는 접근매체별 시나리오 및 룰(rule) 기준으로 추출되는 사용자의 보안로그을 바탕으로 정의하였다. 마지막으로 사

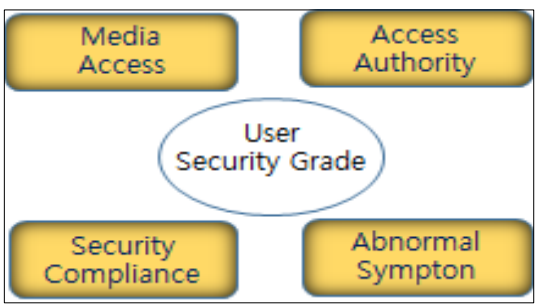

Fig. 3. Four element for user security grade

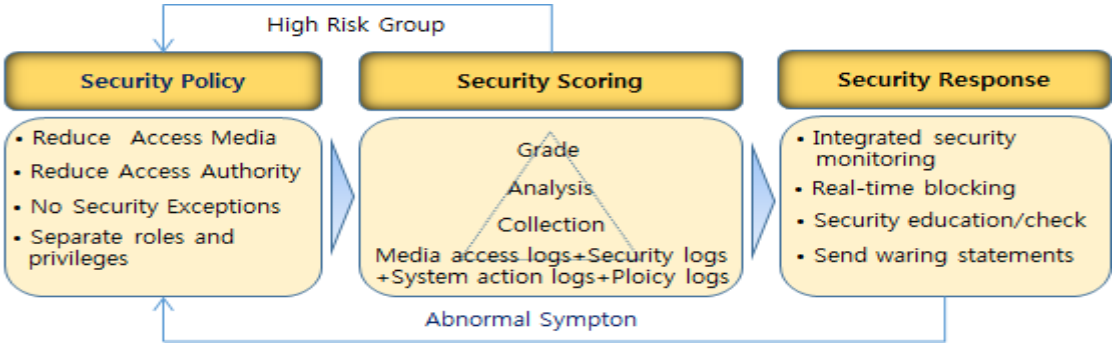

Fig. 4. The whole Concept for customized security policies

용자 보안등급은 4가지 요소를 합산하여 산출하였다.

Fig. 4.는 사용자 맞춤형 보안정책 방법론의 전체 구성도를 그림으로 도식화하였다.

첫째, 사용자의 역할 및 권한을 바탕으로 접근매체, 접근권한, 보안정책 예외자 최소화 등 1차 보안 위협 방지를 위한 보안정책을 정의하였다.

둘째, 보안 점수화는 접근매체의 접속로그, 보안 준수 충성도 및 이상징후 로그와 사용자 보안정책 정보를 융합한 사용자 보안등급을 점수화하였고, 고위험군의 사용자에 대해서는 보안등급 하향조정을 위한 보안정책 검증과정을 재수행하도록 하였다. 셋째, 사용자의 보안등급 상승 및 고위험군 사용자에 대한 보안통제 및 점검을 위한 보안대응 방안을 정의하였다. 본 연구의 사용자 맞춤형 보안정책 방법론을 통해 정확한 보안정책 수립과 신속한 보안위협 대응을 위한 실효적 정보보호관리 체계를 구축하였다.

4.1 사용자 및 접근매체 정의

다중 사용자, 다중 환경을 위한 사용자의 역할에 기반한 접근통제 모델을 통해 권한과 역할을 연관시키고, 사용자들이 적절한 역할을 할당받게 되면 역할에 대한 권한관리가 용이해 질 것이다. 역할은 작업 기능들을 바탕으로 정의되고, 사용자들은 직무에 의한 책임에 따라 역할을 할당받는 것이다.

역할기반 접근제어의 중심적인 개념은 사용자가 기업이나 조직의 정보 자원을 임의로 접근할 수 없도록 하는 것이다. 대신에 접근권한이 역할에 부여되고 사용자는 적절한 역할에 소속됨으로써 역할의 수행에 필요한 최소 자원만을 접근할 수 있도록 한다. 이러한 아이디어는 권한관리를 매우 단순화 시켜주고 기업의 특정한 보안정책을 구현하는데 있어서 유연성을 제공하는 장점이 있다. 사용자는 그들의 업무적 권한과 책임에 따라 특정 역할의 구성원이 되며 접근 구조의 변경이 없어도 역할의 변경을 쉽게 할 수 있다[17].

Table 1.은 사용자별 역할 및 권한 정의를 위해 직원을 내부직원과 외부직원으로 분류하였고, 정보처리시스템의 직접 접속 여부와 업무상 보안 예외정책이 필요한 직무로 구분하여 분류하였다.

Table 2.는 기업에서 APT공격 또는 내부 사용자에 의해 대량의 개인정보 유출 시 사용되어진 접근매체를 5가지(인터넷,웹메일,PC,서버,DB)로 구분하였고, 사용자별 업무처리를 위한 필요성에 따라 접근매체 직무권한을 분류하였다.

▶ 접근매체에 대한 직무권한 분류
1 : 업무처리를 위해 반드시 필요
2 : 업무처리를 위해 선별적 필요
3 : 불필요

Table 1. User classification table

No	Staff	Role
1	Internal	IT
2		Head office
3		Branch office
4	External	IT(System Management)
5		IT(System Intergration)
6		Head/Branch office

Table 2. Classification of job permissions for access media

Staff (No)	WEB	EMAIL	PC	SEVER	DBMS
1	2	2	1	1	1
2	2	2	1	3	3
3	2	2	1	3	3
4	3	3	1	2	2
5	3	3	1	3	3
6	3	3	1	3	3

4.2 접근매체의 접근권한 정의

Table 3.은 접근매체를 사용하고자 하는 경우 접근매체에 대한 접근권한을 4가지로 구분하여 분류하였다.

▶ 접근매체의 접근권한 분류
0 : 접근매체의 접근권한 미허용
1 : 접근매체의 최소 접근권한 허용
2 : 접근매체의 일부 접근권한 허용
3 : 접근매체의 최대 접근권한 허용

Table 3. Access authority of access media

Access Media	Wei-ght	Contents
Web/ Email	3	Able the use of the Web / Email
	2	Blacklists Policies
	1	Whitelists Policies
	0	Disable the use of the Web / Email
PC	3	Not Install all PC Security programs
	2	Install some PC Security programs
	1	Install Core PC Security programs
	0	Install All PC Security programs
Server/ DBMS	3	Direct connection to Root Account
	2	Direct connection to Business account
	1	Direct connection to User account
	0	No Direct connection to ALL account

4.3 보안준수 충성도 정의

Table 4.는 사용자별 보안정책 준수여부 또는 보안위협 행위를 기준으로 단순실수, 관리소홀, 고의적 행위 등으로 구분하여 가중치를 정의하였다. 사용자에 의한 보안위협 가중치는 전자금융감독규정 제37조의 5(정보보호최고 책임자의 의무)의 금융감독원장이 정한 34개 정보보안 점검항목, 개인정보 위험도 분석기준, 보안준수 여부를 바탕으로 정의하였다.

Table 4. Security compliance loyalty table

Weight	Contents
Strong (3.0)	- Security threat behavior
Middle (2.0)	- Security Carelessness
Weak (1.5)	- Simple Mistake

4.4 이상징후 정의

Table 5.는 접근매체별 시나리오 및 룰(rule) 기준으로 이상징후를 정의하였고, 각 이상징후의 가중치는 보안준수 충성도 가중치를 준용하였다.

Table 5. Abnormal symptom definition table

Access Media	Scenario
Web/ Email	Excessive network traffic occurrs
	Network traffic occurs, not working hours.
Server/DB MS	Attempt to connect unauthorized IP
	More than 3 Passwords failed
	Using risk commands for servers
Office PC	Retrieve files containing customer information
	Force Shutdown Security Program
	Boot safe mode from PC
	Illegal software installation on the PC
	Reinstall the OS on the PC

4.5 사용자 보안등급 정의

기존 기술적, 관리적 측면에서 획일적, 단편적으로 관리되고 있는 보안정책을 사용자 관점에서 3개의 보안정책(접근권한, 보안준수충성도, 이상징후)과 5개의 접근매체(인터넷,웹메일, 업무PC, AP Server, DBMS)를 상호연계하여 Fig. 5.과 같이 통합 계산함으로써 사용자별 보안등급을 분류하였다. 이를 통해 과도한 권한 소유자, 보안 미준수자, 보안정책 예외자, 이상행위 사용자 등을 상호연계 및 통합분석하여 고위험군을 분류하고, 이를 통해 사용자별 신속하고 정확한 보안정책(보안교육, 보안점검, 권한조정 등) 수립 및 보안조치를 수행하였다.

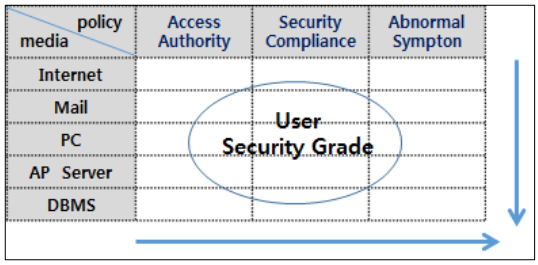

Fig. 5. Matrix table for user security grade calculation

▶ 사용자 보안등급 계산공식

$$\text{User Security Grade} = \Sigma\,(\text{Media}*\text{Policy}*\text{Weight})$$

V. 사용자 맞춤형 보안정책의 사례검증

감독기관의 법규 준수 및 정보보호관리체계(ISMS) 인증을 획득한 A사를 기준으로 사용자 관점에서 3개의 보안정책(접근권한, 보안준수 충성도, 이상징후)과 5개의 접근매체(인터넷, 웹메일, 업무PC, Server, DBMS)에 대한 3개월간의 단일로그를 수집하여 통합분석을 하였다.

- 전체 대상자 : 3,823명
  (내부직원:1,491명, 외부직원:2,332명)
- 조사기간 : 2017.1 ~ 2017.3

5.1 전체 사용자 검증결과

제5장에서 사용자 맞춤형 보안정책 방법론에서 언급하였던 5개 접근매체와 3개 보안정책을 상호 연계하여 통합분석한 결과, Fig. 6. 과 같은 결과를 도출하였다. 상위의 보안등급 소유자는 내부IT 〉 내부본부 〉 외주IT(SM) 〉 내부영업점 〉 외주IT(SI) 순으로 조사되었다.

Table 6.은 전체 사용자를 대상으로 3개의 보안정책 분석결과, 보안준수 충성도 〉 접근권한 〉 이상행위 순으로 파악되었다. 인터넷 악성코드 감염 및 웹메일 모의훈련 시 악성메일 열람 등 단순 실수가 가장 많았고, PC 내 고객정보 파일저장과 같은 관리소홀 등이 뒤를 이었다.

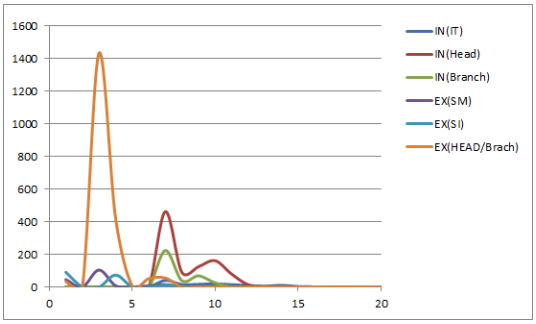

Fig. 6. User security grade distribution(Refer to Table 1. for user classification classification)

Table 6. Security policy violation status

Policy	Sortation	Num-ber	%
Security Compliance	Malicious code infection	316	8.2
	Keep customer information within PC	78	2.0
Access Media	Excessive authority	101	2.6
Abnormal Sympton	Using risk commands for servers	32	0.8

5.2 고위험군 사용자 검증결과

Table 7.은 사용자 보안등급별 보안정책 관리를 위해서 개인정보 유출사고 사례와 보안위협 등을 고려하여 11등급 이상을 위험(danger), 8~10등급은 주의(care),5~7 등급은 관심(attention), 1~4등급은 정상(normal) 단계로 구분하였다.

고위험군(danger) 사용자에 대한 분석결과, 접근매체의 접근권한이 높은 상태에서 Table 6.에서의 조사된 내용과 비슷한 사유로 보안등급이 높아졌다.

Table 7. Security risk step table

Risk Step	Security Grade	Number	%
danger	11 or more	159	4
care	8~10	570	15
attention	5~7	883	23
normal	1~4	2,211	58
Total		3,823	100

5.3 사용자 맞춤형 보안정책 적용

5.3.1 사용자 맞춤형 보안정책 수행

3개월간 수집된 사용자 관점의 통합로그를 기준으로 사용자 보안등급 분류(위험,주의,관심,정상) 후 고위험군 사용자에 대하여 맞춤형 보안대책을 Table 8. 와 같이 수행하였으며, 기존과 달리 고위험군에 속한 사용자들의 접근매체, 접근권한 축소가 용이했으며 또한 보안준수 충성도가 높아지는 결과를 얻을 수 있었다.

Table 8. Perform custom security policies

Risk Step	Security Response
Danger	- Security education and check Reduce access media and access authority - Reinforce third-party verification for security exceptions - Monitoring after blacklist entries
Care	- Send warning statements
Attention	- not applicable
Normal	- not applicable

5.3.2 사용자 보안등급의 평균 하향화

Fig. 7. 은 사용자 맞춤형 보안정책 수행 후 전반적인 보안인식 제고 효과를 얻었으며, 이를 통해 접근매체 및 접근권한 축소, 보안준수 충성도 향상 등 사용자 보안등급이 전체적으로 평균 하향화되었다.

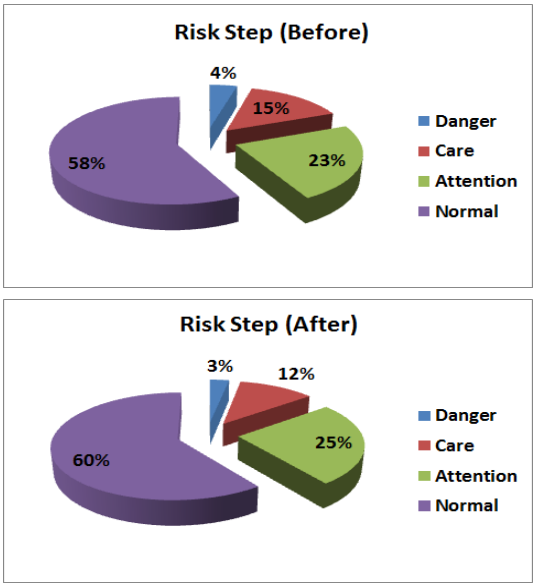

Fig. 7. Comparison of risk step after performing user security policies

5.3.3 실효적 보안점검 및 신속한 보안대응

기존의 보안정책은 사용자(내부/외부)의 업무특성을 고려하지 않은 획일적인 보안통제 및 점검으로 업무효율성 저하 및 보안관리 측면의 어려움이 가중되었다. 그러나 사용자 보안등급에 따른 맞춤형 보안정책을 통해 샘플링 위주의 보안점검이 아닌 우선순위를 통한 실효적 보안점검이 가능했으며, 이상징후 발생 시 오탐, 과탐이 아닌 정탐 위주의 보안대응이 가능했다.

VI. 결론 및 향후 발전방향

6.1 결론

본 논문은 침해사고 및 개인정보 유출 방지를 위

하여 개인정보보호 관련 법규 강화와 기업들의 다양한 노력에도 불구하고 보안사고는 지속적으로 발생하고 있으며 그 빈도 또한 줄어들고 있지 않고 있다. 이에 최근의 보안사고 사례 분석 및 기술적 보안대책과 정보보호대책 수립을 위한 위험평가 방법론을 살펴보았다. 첫째, 과도한 접근권한을 소유한 사용자의 접근매체를 통해 APT 공격 대상이 되었고 둘째, 보안정책 예외자 및 보안위협 행위자에 대한 지속적인 모니터링 및 관리 미흡으로 내부 악의적인 행위자에 의한 개인정보 유출이 발생하였다.

셋째, IT자산 및 보안 솔루션 중심의 보안대책과 모니터링으로 사용자의 업무적 목적 사용여부와 이에 따른 보안위협 판단이 어려워 신속·정확한 보안대응이 쉽지 않았다. 이에 대한 보안대책의 개선방안을 찾고자 사용자 중심의 보안정책 방법론을 제안하였다.

제안한 방법론은 사용자의 직무별 접근매체(인터넷,웹메일,PC,서버, DBMS)에 대한 상세 접근권한과 보안준수 충성도(보안정책 준수여부, 보안위협 행위) 및 이상징후 정보를 이용한 사용자 기준의 위험평가를 통해 보안등급을 산출하였다. 보안등급이 높은 고위험군 사용자는 보안통제 및 점검을 강화하고, 저위험군 사용자는 다양한 업무특성과 서비스 지원을 위하여 보안통제 및 점검을 완화함으로써 업무 효율성 증대와 동시에 전체 사용자의 보안등급을 하향 평준화하였다. 또한 기업 내 사용자는 자신의 보안등급을 직접 확인함으로써 보안의식 고취 및 보안준수 충성도도 자연스럽게 상승하였다. 사용자를 관리감독하는 제3자(상위 결재자,보안 담당자) 역시 사용자별 보안등급을 고려한 합리적, 객관적 관리감독 및 보안정책 수립을 위한 사실적 근거를 마련하였고, 고위험군 사용자의 이상징후 발생 시 신속·정확한 분석 및 대응이 우선적으로 가능하게 되었다.

기업의 보안사고는 경제적 피해와 더불어 기업 이미지 및 신뢰도 하락, 소비자 소송 등 유.무형의 손실을 초래한다. 따라서 보안사고가 발생하면 신속하게 대응하여 피해를 최소화 할 수 있는 관리체계를 갖추어야 하고 보다 중요한 것은 사고를 미연에 방지할 수 있도록 예방 활동에 더 많은 투자와 노력을 해야 한다. 사용자 맞춤형 보안정책은 다양한 업무환경과 서비스를 지원함과 동시에 기업의 보안사고 대응 역량을 한층 강화시켜 줄 것이다.

6.2 향후 발전방향

본 연구의 사례검증을 위해 3개월 간 수집된 접근매체의 보안로그와 사용자 보안정책 정보는 사용자 보안등급 산정을 위한 귀중한 자료가 되었다. 향후 더 방대한 보안로그의 실시간 수집과 사용자 보안정책의 상세정보가 융합된다면 사용자 보안등급 산정의 신뢰성과 정확성이 한층 더 발전 될 것이다. 이를 바탕으로 고위험군 사용자에 대해서는 접근매체별 보안솔루션과 실시간 연동을 통해 보안위협 탐지와 동시에 접근권한을 차단함으로써 선제적 보안사고 대응을 위한 초석이 될 것이다.

References

〔1〕 Wikipedia, “Fourth Industrial Revolution,” May. 2017.

〔2〕 Jun-Taek Lee, ″Overview of Information Protection,″ Dec. 2016.

〔3〕 Hu-Eul Kim and Dong-Hyun Baek, ″A Study on Categorization of Accident Pattern for Organization’s Information Security Strategy Establish,″ Annual Report of Industrial Management Systems in Korea, 38(4), pp. 193-201, Dec. 2015

〔4〕 In-Hwan Cha, ″(An)Empirical Research on Developing Personnel Security Management Indicators in Information Security,″ Thesis for the Degree of Dotor, Gwangun University, Aug. 2009.

〔5〕 Security News, “http://www.boannews.com/media/ view.asp?idx=51343,” 2016. 7.27.

〔6〕 GARTNER,“Strategies for Dealing With Advanced Targeted,” Aug. 2011.

〔7〕 Seong-Back Han and Sung-Kwon Hong,″Countermeasures against APT Attacks,″ Journal of the Korea Institute of Information Security & Cryptology, 23(1), pp. 44-53, Feb. 2013

〔8〕 Seol-Hwa Im,Jong-Su Kim,″ APT status and new malicious code counter-measures,″ Journal of the Korea Institute

of Information Security & Cryptology,24(2), pp.64-70, Apr. 2014
〔9〕 Song-young Kim, "A study on the security policy improvement using the big data," Journal of the Korea Institute of Information Security & Cryptology, 23(5), pp.969-976, Oct. 2013.
〔10〕 Financial Security Sources,"Status and prospect of using behavioral detection system(FDS)," Jul. 2015.
〔11〕 Hye-Won Sin, "Methodology to analyze insider risk for the prevention of corporate data leakage," Korea Information Science Society, Jul. 2012.
〔12〕 KISA, "Research on the Development of Information Security Management System (ISMS)," 2009.
〔13〕 Financial Security Sources,"Training for Human Resource Surveillance Training Personnel Training(Financial IT Compliance)," Mar. 2017.
〔14〕 Security news, ″ measured but unprotected information protection management system ″, 2016.06.02.
〔15〕 Byeong-Seol Min, ″ Limits and Challenges of Human Security Management,″ Korea Occupational Technology Protection Association, 2011.
〔16〕 Financial Supervisory Service,″ Electronic Financial Supervisory Regulations," 2017.
〔17〕 Chang-Woo Byun and Seog Park, ″A Role-Based Access Control Model ensuring Confidentiality and Integrity,″ ournal of the Korea Institute of Information Security & Cryptology, 15(3), pp.13-29, Jun. 2005.

〈저자소개〉

손 영 환 (Young-Hwan Son) 정회원
1999년 2월: 국민대학교 정보관리학과 졸업
2000년 5월~현재: KB국민카드 근무
2015년 8월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 침해사고대응, 위험관리, 정보보호 및 개인정보보호정책

김 인 석 (In-Seok Kim) 정회원
1973년 2월: 홍익대학교 전자계산학과 졸업(학사)
2003년 2월: 동국대학교 정보보호학과 졸업(석사)
2008년 2월: 고려대학교 정보경영공학과 졸업(박사)
2009년~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 전자금융보안, IT감사, 전자금융법규