http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.23, No.4, November 2018, pp.153-169
https://doi.org/10.7838/jsebs.2018.23.4.153

내부자 보안위협 분석을 통한 전자금융 이상거래 탐지 및 대응방안 연구

Detecting Abnormalities in Fraud Detection System through the Analysis of Insider Security Threats

이재용(Jae-Yong Lee)*, 김인석(In-Seok Kim)**

초 록

기존의 전자금융 이상거래 분석 및 탐지기술은 전자금융 업무시스템으로부터 발생된 대량의 전자금융 거래로그를 빅데이터 기반의 저장 공간으로 수집하고, 기존 고객의 거래패턴 프로파일링 및 다양한 사고거래를 분석한 탐지룰을 이용하여 비정상적인 이상거래를 실시간 또는 준 실시간으로 탐지하고 있다. 하지만, 정작 피해금액 규모 및 사회적 파급효과가 큰 금융회사 내부자의 전자금융 부정접속 시도 및 내부 통제환경의 우회를 통한 전자금융 이용자의 중요정보 탈취와 같은 적극적인 분석은 제대로 이루어지지 못하고 있다. 이에 본 논문에서는 금융회사의 전자금융 보안프로그램에 대한 관리 실태를 분석하고, 관리상 취약점을 악용한 내부자의 보안통제 우회사고 가능성 도출한다. 또한, 이를 효율적으로 대응하기 위하여 기존 전자금융 이상거래탐지시스템에 더불어 내부자 위협모니터링과 연계한 포괄적인 전자금융 보안관리 환경을 제시하고자 한다.

ABSTRACT

Previous e-financial anomalies analysis and detection technology collects large amounts of electronic financial transaction logs generated from electronic financial business systems into big-data-based storage space. And it detects abnormal transactions in real time using detection rules that analyze transaction pattern profiling of existing customers and various accident transactions. However, deep analysis such as attempts to access e-finance by insiders of financial institutions with large scale of damages and social ripple effects and stealing important information from e-financial users through bypass of internal control environments is not conducted. This paper analyzes the management status of e-financial security programs of financial companies and draws the possibility that they are allies in security control of insiders who exploit vulnerability in management. In order to efficiently respond to this problem, it will present a comprehensive e-financial security management environment linked to insider threat monitoring as well as the existing e-financial transaction detection system.

키워드 : 내부자 보안위협, 위협모니터링, 무작위 대입공격, 전자금융 이상거래탐지시스템
Insider Security Threats, Threat Monitoring, Brute Forcing, FDS

* First Author, Graduate School of Information Security, Korea University(jaeyong.lee@kbfg.com)
** Corresponding Author, Graduate School of Information Security, Korea University(iskim11@korea.ac.kr)
Received: 2018-10-19, Review completed: 2018-11-23, Accepted: 2018-11-27

1. 서 론

최근 금융 감독당국의 전자금융 관련 규제가 법률을 기반으로 한 일률적인 규제에서 자율규제 형태로 전환됨에 따라 각 금융회사에서는 전자금융서비스 이용자의 편의성 제고를 목적으로 간편화된 다양한 전자금융서비스를 경쟁적으로 출시하고 있다. 간편한 전자금융서비스 이면에는 머신러닝, 딥러닝 등 최신 빅데이터 기술을 기반으로 이상거래 탐지시스템 고도화, 이용자의 생체정보 인식기술을 활용한 인증강화 등 전자금융 거래 안전성 확보방안에 역량을 집중하고 있으나, 정상적인 전자금융 거래패턴이 아닌 내부자에 의한 전자금융 이용자 중요정보 탈취를 통한 금융사고에 대한 적극적인 분석은 제대로 이루어지지 못하고 있는 실정이다.

내부자에 의한 전자금융 사고는 피싱, 파밍 등 일반적인 전자금융 이용자정보 탈취를 통한 금융사기 보다 피해금액이 크고, 동일 금융회사 내부자에 의한 사고라는 측면에서 금융회사에 미치는 사회적 파급효과 또한 심각하다고 할 수 있다.

본 논문에서는 내부자에 의한 전자금융 사고 사례를 기반으로 금융회사의 전자금융 보안과 관련된 내부자의 보안위협을 분석하고, 그 위협에 대응하고 있는 전자금융 보안 대응현황 점검을 통해 문제점을 도출하여 안전한 전자금융 보안환경이 운영될 수 있도록 방안을 제시하고자 한다.

2. 관련 연구

2.1 선행연구 결과분석

대부분의 금융회사는 비대면 금융서비스의 급증에 따라 전자금융서비스 이용자의 자산을 금융사기로부터 보호하기 위하여 이상거래 탐지시스템이 구축되어 있으며, 이상거래의 오탐율을 최소화하고 정탐율을 향상시키기 위해 머신러닝, 딥러닝 등 AI기반의 기술검토 및 실효성 검증을 위한 연구가 활발히 진행되고 있다.

선행연구에서는 비대면 금융서비스의 급증과 신기술에 등장에 따라 데이터마이닝을 기반으로 모바일 결제로그를 이용한 실증적인 연구를 통해 비대면 환경에 특화된 이상거래탐지시스템을 제시하는 연구가 진행되었으며[9, 12], 이상거래탐지시스템의 고도화를 위하여 이상거래와 정상거래 행태 간 분류기준을 정교화하는 규칙을 도출하여 모델링 방법론을 제시하는 연구도 진행되었다[2]. 또한, 이러한 이상거래탐지시스템의 연구가 지속되면서 내부자 위협으로부터 정보유출을 방지하기 위한 목적으로 활용하는 기업이 점차 증가하고 있다[14].

카네기멜론대학교의 CERT는 내부자 위협과 관련하여 내부 침입 연구를 위한 인공데이터를 제공하고 있으며, 로그인 정보, 디바이스 사용, 웹 사용, 이메일 사용 등의 60여 개의 변수를 추출하고, 이를 이용하여 4가지 추정방법을 통해 내부자 위협 스코어 측정에 어떠한 추정방법이 적합한지에 관한 연구를 하였다[13]. 이러한 이상치를 탐지하기 위하여 모두가 흔히 알고 있는 가우시안 밀도 추정, 파즌 윈도우 밀도 추정, 주성분 분석법 등을 이용하여 내부자 위협 스코어를 산출하였다[1, 4]. 해당 연구는 단일 이상치 탐지알고리즘과 더불어 두 개 이상의 이상치 탐지 알고리즘을 결합하는 앙상블 방식으로 한 결과가 가장 우수한 성능을 나타낸 결과를 연구한 의의가 있지만, 실제 데이터가 아닌 인공 데이터를 이용하여 실제 데이터로의

검증이 부족한 한계가 존재한다.

다른 내부자 위협 관련 연구에서는 위험분석 방법론 측면에서 현재 한국인터넷진흥원(KISA)이 주관하는 ISMS 인증에서 다루는 위험평가론의 문제점을 지적하고 대안을 제시했다[21]. 해당 연구에서는 국제표준 ISO/IEC TR 13335에 해당된 GMITS, 영국 표준협회에서 제정한 보안관리 평가기준인 BS7799에서 쓰이는 위험분석 방법론에 내부자 위험도를 반영하였다[10, 11]. 또한, 기존 ISMS의 위험평가 방법론의 한계점을 지적하고 내부자 위험평가를 첨가한 ISMS-AIR를 통한 연구 방향을 제안하고, 평균 출퇴근 시간, 일과시간 외 회사 출입시간 및 횟수, 연속되는 로그인 실패 등의 정보를 이용하여 내부자의 가치, 취약성의 수준, 대응책 존재여부 및 위협의 발생가능성을 변수로 위험도를 산출하는 방법을 제안하였다. 하지만, 실질적인 실효성을 증명하지 못하였고, 논문 내 수식위험도를 산출하는 수식에서 위협의 발생가능성을 0과 1만의 값으로 산정한 점과 이 해당 값이 곱의 변수로 들어감으로써 관리적 보안 관점에 있어 현실적인 적용에 어려움을 겪을 것으로 보인다. 이러한 내부자 위협의 심층적인 연구뿐만 아니라 이를 미연에 방지하기 위하여 내부자 위협을 방지하고자하는 교육 연구도 계속되고 있다[18].

2.2 선행연구와의 차이점

기존 선행연구들의 내부자 위협분석은 다양한 추정방법과 위험평가 방법론을 다루며 의미있는 연구의 시초가 되었지만, 관리적인 방법으로써의 실질적인 적용에는 한계점이 존재한다. 이에 기존 선행연구들에서 공통적으로 반영이 되었던 내부자 위협을 판단하는 요소들은 본 연구에서도 일부 활용하여 긍정적인 요소는 내부자 위협에는 적극적으로 활용하고, 금융회사 내부자에 의한 고객정보 유출사고 측면이 아닌 금융회사의 전자금융 보안프로그램의 관리취약점을 악용한 사고를 예방하기 위한 대응방안이 중점을 두고 연구하고자 한다.

유사한 선행연구로는 내부직원의 직무와 근무활동패턴을 이용하여 비정상적인 이상 징후 탐지패턴 도출 및 행위분석을 통해 금융회사 내 고객정보 유출방지 에 관한 연구가 수행되었으나, 본 논문에서 연구하고자 하는 실제 전자금융 보안사고의 핵심요소로 사용된 전자금융 보안프로그램 보호실태와 내부통제 강화방안을 분석하여 이용자의 중요정보를 보호하고 금융자산 탈취와 연결되는 사고를 예방하기 위한 연구는 부족하였다[19].

이용자로부터 수집된 비밀번호 등 전자금융거래에 필요한 중요정보는 전자금융 보안프로그램의 관리가 소홀하거나 보안통제 취약점을 악용하여 노출될 경우, 내부자에 의한 유사한 금융사고가 재발될 수 있으며, 전자상거래 및 외부 제휴 등 전자금융 업무영역이 점차 확대됨에 따라 다른 업무와 달리 그 중요도도 상대적으로 높아지고 있다.

이에 본 논문에서는 언론에 발표된 금융회사 내부자에 의한 전자금융 사고사례를 통해 전자금융 보안통제 환경의 문제점을 분석하고, 내부자의 이상행위 모니터링을 포함한 전자금융 이상거래 탐지시스템 연계 등 포괄적이고 안전한 전자금융 관리환경을 제시하여 연구를 발전시키고자 한다.

2.3 내부자 위협 탐지

정상 사용자의 실수, 불만을 가진 악의적인

사용자의 무단 접근 등 내부자의 모든 위협을 정확히 분류하여 네트워크에서 사전에 차단할 수 있는 방법은 쉽지 않으므로, 내부에서 이들의 활동을 효과적으로 탐지하기 위한 수단이 필요하다. 데이터 침해를 발견하는 데 소요되는 시간이 평균 191일, 이 침해를 진압하는 데 소요되는 시간이 평균 66일이며, 침해당 평균 비용이 362만 달러에 이른다는 점을 감안하면 의심스러운 사용자 활동을 조기에 탐지함으로써 얻는 효과는 막대할 것이다[20].

내부자의 이상행위를 분석하기 위하여 네이티브 윈도우 로깅과 상용화된 감사 솔루션 등을 통해 사용자의 매 동작(네트워크 로그인, 파일 열기 등)을 기록한 이벤트 정보 등 많은 의미있는 정보를 활용할 수 있다. 예를 들어, 8만 명의 사용자가 포함된 한 의료 업체는 최근 테스트에서 불과 한 달 만에 액티브 디렉토리(Active Directory), 인증, 파일 활동과 관련해 1억 9,300만 개에 이르는 감사 이벤트를 캡처를 했으며, 같은 기간 사용자 수 7,000명의 한 기술 업체는 3,000만 개의 이벤트를 캡처하여 데이터를 수집하였다. 이렇게 수집된 수많은 정보를 활용하여 비정상적인 행위만을 추출하기 위한 방안으로 크게 두 가지 접근 방법론을 제시하고 있다.

2.3.1 규칙 기반 탐지

가장 일반적인 방법은 특정 활동을 인식하고 이 활동이 발생할 경우 선제적으로 경보를 발령하는 규칙을 만드는 것이다. 도메인관리자(Domain Admins)와 같은 기본 관리자 그룹에 사용자가 추가되는 경우처럼 항상 정밀한 점검이 필요한 경우가 해당될 수 있으나 이 접근 방법에는 두 가지 큰 문제가 있다.

1. 특정 행동을 인식하는 규칙을 만들려면 사고를 유발하는 그 행동에 관한 과거의 경험 또는 지식이 필요하다. 시스템이나 환경에 변화가 생기면 기존 규칙이 정확하게 탐지하지 못하거나, 이전에 알지 못한 새로운 침입이 있을 경우 효율적으로 적용하기 어렵기 때문에 범용적으로 사용할 수 없다[16].
2. 항상 의심스러운 것으로 간주되는 행동은 소수이다. 규칙에 기반을 둔 탐지 방법은 규칙을 벗어난 침입에 대해서는 능동적으로 대응하기 힘든 단점이 있다[23].

첫 번째 제한을 조금 더 구체적으로 살펴보면 의심스러운 사용자 행동을 탐지하는 규칙 기반 접근 방법에서는 대부분 다음과 같은 행동에 대해 경보를 발령하는 규칙을 생성한다.

- 비 활성화 상태에서 최근 활성화된 사용자 계정
- 연속으로 여러 번 실패한 로그인
- 짧은 시간 동안 다수의 파일 수정

이러한 모든 규칙은 더 큰 맥락에서 벌어지는 일련의 의심스러운 행동 고리에 포함되는 하나의 행동을 캡처할 가능성이 있다. 그러나 규칙은 행동이 탐지될 때마다 경보를 발생한다. 예를 들면, 사용자 인증이 10회 연속 실패한 경우 95%는 무차별 대입 공격이 아니라 단순히 암호를 잊었거나 잘못 입력한 경우에 해당한다. 혹은 짧은 시간 내에 다수의 파일이 수정된 경우 사용자가 급여 애플리케이션을 실행해서 월별 재무 기록을 업데이트한 결과일 가능성이 높다.

따라서, 최근에는 내부 침입 행위를 규칙으로 분류하는 것 외에 침입 행위를 더욱 정교하

게 분석하기 위한 시도들이 있었으며, 내부자 위협을 기술적인 측면(IT aspects)과 사회적인 측면(social aspects), 두 가지 측면에서 정의하여 내부 침입자 유형을 제안하는 반면[17], 이와 반대로 분류 기준을 미리 정하지 않고 텍스트 마이닝 기법을 활용하여 내부침입자의 특성 사전을 구축하려는 시도도 있었다[15].

2.3.2 기계학습 기반 탐지

특정 패턴에 의한 규칙기반 탐지와 달리 기계 학습 기반으로 내부자 위협을 분류하는 연구도 등장하였다. 내부 침입자의 악의적 행동 시나리오, 비정상적인 행동, 통계 패턴, 시간적 순서 등을 근거로 이상 행위 탐지에 다양한 알고리즘을 적용하였다[22]. 내부자 위협의 이메일, 파일, 로그인 등과 관련된 행위를 변수로 생성하여 이 변수들을 RPAD, 가우시안 혼합모델(GMM) 등 기계학습 알고리즘에 적용하여 이상치 탐지에 가장 적합한 조합을 찾아내었다. 하지만 이 연구는 다양한 변수들을 사용했음에도 중요한 변수를 선택하는 과정이 부족했다. 일반적으로 변수가 많으면 기계 학습 모형의 성능이 저하될 수도 있기 때문에 중요 변수를 선택하는 과정이 필요하다[8]. 또한 같은 직군의 사람들은 비슷한 행위를 보이는 특성을 통해 자신이 속한 그룹과 다른 행동을 보이는 사용자를 내부 침입자로 정의하고 탐지한 연구가 있다[5].

규칙기반 탐지는 규칙을 보다 정교화 하는데 초점이 맞추어져 있는 반면, 최근의 연구에서는 이러한 규칙을 기계 학습을 통해 사람의 힘을 빌리지 않고 자동으로 추출하여 이상치 등을 더욱 정교하게 만들기보다는 내부자 침입에 적합한 프레임 워크를 찾는데 중점을 두고 있다.

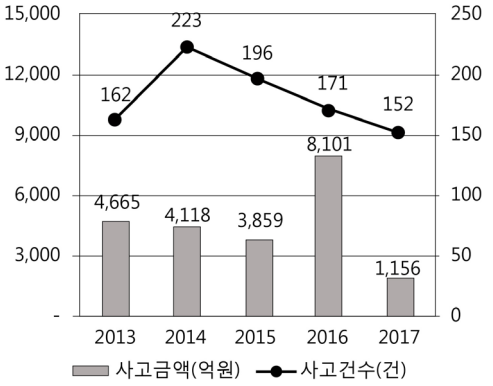
3. 내부자 보안위협 분석

사이버 공격의 대상과 목적이 경제적인 자금 탈취를 위한 영역으로 확대되고, 공격방식도 점차 정교화 됨에 따라 외부에서의 공격 못지 않게 악의적인 의도를 가진 내부자에 대한 대응도 중요한 요소라고 할 수 있다.

내부자에 의한 공격은 기존 전통적인 내부통제 및 관리적인 방어만으로는 수많은 위협에 효율적으로 대응하기에 한계가 존재하므로, 내부자에 의한 전자금융 사고의 핵심요소인 전자금융 보안프로그램 비인가 접근 등 사용자의 행위기반 분석을 통해 내부자의 보안위협을 탐지하여 예방하는 것이 무엇보다 중요하다고 할 수 있다.

3.1 최근 5년간 금융사고 발생현황

2017년 중 금융감독원에 보고된 금융사고는 총 152건, 1,156억 원으로 전년대비 사고 건수는 19건(11.1%↓), 금액은 6,945억 원(85.7%↓) 감소하였다.



〈Figure 1〉 Current Status of Financial Accident

사고 건수는 2014년 이후 지속적으로 감소하고 있지만, 사고금액의 경우는 과거 4개년 연속 발생한 초대형 금융사고가 2017년에는 발생하지 않아, 전년대비 크게 감소한 추세를 보이고 있다[6].

금융사고 피해금액 기준 발생규모와 사고 유형별 피해금액 현황은 다음과 같다.

〈Table 1〉 Status by Size of Financial Accident

Classify		2015	2016	2017
less than 100 million	Case	137	88	79
	Amount	28	27	22
100 million to 1 billion	Case	41	55	51
	Amount	150	199	211
1 billion to 10 billion	Case	13	18	19
	Amount	359	502	392
more than 10 billion	Case	5	10	3
	Amount	3,322	7,373	531
Sum	Case	196	171	152
	Amount	3,859	8,101	1,156

〈Table 2〉 Status by Type of Financial Accident

Classify		2015	2016	2017
Fraud	Case	29	48	48
	Amount	3,309	7,221	843
Dereliction of duty	Case	13	25	17
	Amount	90	755	135
Embezzlement	Case	150	95	84
	Amount	459	124	177
Robbery	Case	4	3	3
	Amount	1	1	1
Sum	Case	196	171	152
	Amount	3,859	8,101	1,156

3.2 내부자 관련 전자금융사고 사례

보안사고의 90%는 사람에 의해 발생하며 데이터 유출사고를 겪은 기업 중 약 40%는 내부자에 의한 보안사고이다[3, 7]. IT 보안 전문가의 75%는 외부자에 의한 리스크 보다 내부자의 위협이나 내부자 계정의 리스크를 더 심각하게 여기고 있다.

내부자 관련 사고사례는 크게 금전적 이득을 노리는 직원, 퇴직하거나 해고당한 직원, 악의적인 외부 계약자 등 3가지로 분류할 수 있다. 먼저 금전적 이득을 노린 내부자 위협사고 사례로는 한 카드사의 텔레마케팅 지원업무를 맡은 직원이 제휴사의 휴대전화 구매고객 개인정보 약 10만 건을 자신의 개인 이메일로 보내 외부로 유출하였고, 이 중 5만여 건을 분양 대행업자에게 전달하여 금전적 이득을 취하였다.

또한, 2014년 6월에는 한 기관 퇴직 직원인 A씨는 퇴직 이후에도 해당 기관 사업단에 출입하여 내부자 정보를 유출하였다. 이는 퇴직한 지 1년 반이 지나도록 신분증과 출입증을 회수하지 않은 것으로 밝혀져 퇴직하거나 해고된 직원의 악의적인 행동으로 사고가 발생하였다.

마지막으로는 악의적인 외부계약자 사례는 은행 IT센터 외주업체 직원이 대학선배의 부탁으로 고객정보 10만여 건을 USB에 저장하여 5차례에 걸쳐 유출한 사건을 들 수 있다.

이용자의 개인정보 유출사고는 사고가 발생할 때마다 발표되는 종합대책으로 인터넷 망분리, 문서암호화, 문서유출방지, 보조기억매체 통제 등 재발 방지를 위한 다양한 보안통제 기능들이 적용되고 있으나, 고객의 금융자산 횡령사고는 전자금융 보안프로그램을 대상으로 무작위 대입공격 등 비정상적인 행위를 시도할

경우, 정상거래와 이상거래를 판단하기가 쉽지가 않으므로, 전자금융 보안프로그램에 대한 상시 모니터링 강화는 내부자에 의한 전자금융 사고를 예방하고 안전한 전자금융 서비스 환경을 제공하기 위한 중요한 핵심요소라고 할 수 있다.

3.3 내부자에 의한 전자금융사고 패턴분석

최근 언론에서 발표된 금융회사 내부자에 의한 횡령이나 자금유용 사고를 분석해 보면, 금융관련 전문지식을 바탕으로 전산조작 등을 통하여 공격대상과 접근환경을 분석한 후, 지능적이고 치밀하게 사고를 은폐하고 있어 사고적발에 6개월에서 1년 이상 장시간 소요되고, 타 전자금융 사고대비 피해금액 규모가 상대적으로 큰 특징을 가지고 있으며, 다음과 같은 공통적인 패턴을 발견할 수 있다.

〈Table 3〉 Behavior of Financial Accidents by Step of Insider

Step	Content
Target Selection	Selection of vulnerable targets
Analysis of Collection Environment	Check location of electronic financial information
Check Required Privileges	Confirm access path and authority and placement control
Check control bypass	Security control status and bypass route check
Final confirmation of ownership	Final inspection of required authority before collecting information
Collect necessary information	Collection of users' e-financial information
Illegal capital transfer	Acquisition of illegal funds

- 공격목표선정: 최근 전자금융 사고예방을 위한 보안대책이 강화됨에 따라 OTP 또는 생체인증과 같이 본인이 소지하거나 소유하고 있는 강화된 보안매체를 사용하는 이용자를 공격대상으로 지정하지 않고, 상대적으로 보안이 취약한 보안카드를 이용하고 있거나 장기간 거래내역이 없고 해외체류정보를 이용한 추가 본인확인 절차를 우회할 수 있는 등 사고발생 가능성이 높은 이용자를 공격대상으로 삼는다.
- 정보수집환경 분석: 이용자의 전자금융 정보 중 주민등록번호 등 중요 고유식별정보 항목은 개발환경에 변환된 상태로 저장되어 있으나, 실제 해당 업무를 담당하거나 담당한 경험이 있는 내부자의 경우, 변환 정책을 우회한 미 변환 된 이용자 정보가 존재하는지, 로그파일이나 임시파일 등에 삭제되지 않은 정보가 존재하는지를 확인하여 실 운영환경에서 수집할 정보의 위치를 손쉽게 파악한다.
- 필요권한 확인: 수집할 정보의 위치가 확인되면 해당 DB 및 파일에 접근할 수 있는 권한을 보유하고 있는지, 보안솔루션 등으로 해당 정보에 접근을 통제하고 있는지의 여부를 확인한다.
- 통제 우회경로 확인: 통제수준이나 권한통제가 적용된 경우 배치작업으로 이용자의 전자금융정보를 탈취하거나, 통제수준의 취약점을 이용한 인증단계 우회 또는 해외체류정보를 조작하여 추가인증을 차단할 수 있는지 등을 확인한다.
- 보유권한 최종확인: 장기간에 걸쳐 이용자의 전자금융 정보의 위치, 필요한 권한, 우회경로가 확인된 경우, 대량의 이용자

정보 탈취 작업 수행에 대비하여 최종적으로 권한을 확인한다. 또한, 기존에 필요 권한 확인단계에서 수행한 접근시도 행위가 시스템관리자나 보안담당자에게 적발되지 않았을 경우, 실제 공격을 수행할 환경이 준비되었다고 할 수 있다.

- 필요정보수집: 무작위 대입공격 등을 이용하여 전자금융 보안프로그램 호출하거나 관리가 소홀한 개발환경 및 백업 등 로그파일을 통해 이용자 전자금융 정보를 수집한다.
- 불법자금이체: 수집한 이용자의 전자금융 보안정보를 활용하여 자금을 이체 또는 인출하거나 전자상거래 물품구입 등의 방법으로 고객의 금융자산을 탈취한다.

4. 전자금융 보안관리 현황 및 문제점

4.1 전자금융 보안관리 현황

각 금융회사는 전자금융 이용자의 식별과 인증, 자금이체 지시에 대한 부인방지를 위해 공인인증서 및 다양한 보안솔루션을 도입하여 운영하고 있으며, 전자금융 사기예방 대책 강화에 따라 보안매체, 추가인증, 전자금융 이상거래탐지시스템 구축 등 복잡하고 불편한 보안기능이 지속적으로 적용되어 왔다.

전자금융 보안프로그램은 크게 외부 사기범이나 해커로부터 전자금융서비스 이용환경을 보호를 위한 이용자 측면의 전자금융 보안프로그램과 시스템 내에서 전자금융 거래를 수행하는 과정에서 추가 검증을 위한 시스템 측면의 전자금융 보안프로그램으로 분류할 수 있다.

본 연구에서는 내부자가 업무처리 환경에서 접근할 수 있는 시스템 내 전자금융 보안프로그램에 대한 접근통제현황 및 이상행위 모니터링 탐지방법 제시를 통해 전자금융 사고를 미연에 방지할 수 있는 방안을 검토하고자 한다.

4.2 전자금융 보안관리 문제점

금융회사의 전자금융 보안프로그램에 대한 보호대책은 전자금융거래법 및 전자금융 감독규정 상 기준에 따라 내부통제 측면의 보호대책을 전반적으로 준수하고 있으나, 금융회사 업무처리 환경특성 상 내부자의 전자금융 보안프로그램 불법접근 및 오남용에 대한 시스템 기반의 체계적인 통제와 모니터링은 아직 관리가 미흡한 상태이다. 전자금융 보안프로그램의 통제취약점을 이용한 내부자의 위협행위는 다음과 같이 크게 3가지 영역에서 분석해 볼 수 있다.

4.2.1 관리전담자의 상호견제 부족

전담관리자를 지정하여 중요 데이터에 접근권한을 제한하고 업무역할에 따라 직무를 분리하는 등 최소권한 및 직무분리와 같은 기본 원칙을 엄격히 준수한다면 내부자가 조직을 대상으로 공격할 수 있는 위협이 매우 제한적이기 때문에 내부자 위협을 상당부분 줄일 수 있다. 직무분리는 특정 개인이 전체 업무프로세스를 제어할 수 없도록 직무를 적절히 분리하여 상호견제하는 것을 의미하며, 만일 특정 직원에게 직무가 편중된다면 업무편의 및 금전적 이득 등을 위해 부여된 특권을 이용하여 내부자 위협으로 발전할 수 있다. 대형 금융회사와 같이

인력 및 조직구조가 세분화된 경우에는 제3자 검토 등 다각적인 사고예방을 위해 여러 단계에 걸쳐 내부통제가 강화되어 있지만, 중소형 금융회사에서는 세분화된 직무분리가 어렵고 담당자 및 관리자의 승인 등 형식적으로 수행될 경우, 이용자 중요정보에 접근하는 것을 통제하기는 쉽지 않다.

4.2.2 전자금융 보안프로그램 운영환경 취약

금융회사의 전자금융 보안프로그램을 포함한 업무프로그램은 온라인거래와 배치작업 간의 정합성 유지를 위해 동일한 운영프로그램에 의해 처리되도록 설계되어 있다. 영업점 단말에서 수행되는 대면거래나 인터넷뱅킹 및 모바일뱅킹에서 수행되는 비대면 거래에서 전자금융 보안프로그램에 접근하는 경우에는 각 전자금융 업무프로그램 또는 접근 채널을 통합한 비밀번호 오류횟수를 체크하고 지정된 오류횟수를 초과할 경우, 거래를 강제로 차단하는 통제정책을 운영하고 있다. 하지만, 최근 금융회사 내부자의 사고사례와 같이 악의적인 내부자가 임의의 배치프로그램을 통해 전자금융 보안프로그램을 대상으로 무작위 대입 공격을 시도하는 경우에는 비밀번호 오류횟수를 제한하기 어려워 고객이 등록한 비밀번호가 노출될 가능성이 높다.

4.2.3 배치프로그램 검증소홀

배치프로그램에 의한 일괄작업은 작업의 목적 및 결과에 대해 상위관리자, 동료검토 등 강화된 제3자의 사전 승인절차를 걸쳐 변경관리 전담자에 의해 운영환경에 적용된다. 전자금융 보안프로그램은 일반적인 전자금융 업무프로그램과 달리 초기 개발 이후, 알고리즘에 변화가 거의 없으며, 업무 특성 상 보안담당자 또는 전자금융 업무담당자의 직무순환이 쉽지 않기 때문에 특정 직원이 암호 알고리즘의 구조 및 체계에 대한 파악이 가능하다. 또한, 프로그램 특성 상 전담자 외에 제3자가 전자금융 보안프로그램 접근에 대한 내용을 파악하기 어려워 정상적인 배치프로그램으로 위장하여 운영환경에서 실행될 경우, 이용자의 중요정보에 접근할 위험이 존재한다.

5. 전자금융 보안관리 강화 방안

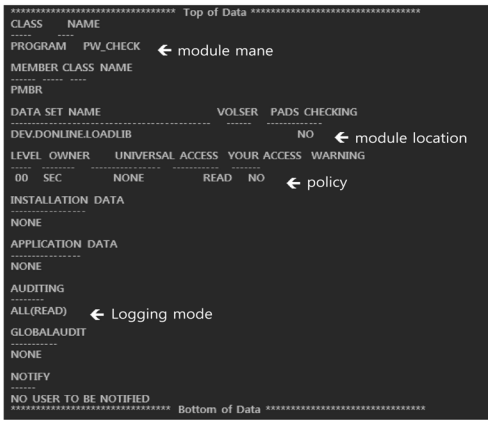
5.1 전자금융 보안프로그램 모니터링 강화

최근 금융회사 내부자에 의해 발생하는 전자금융사고의 대부분은 앞에서 설명한 전자금융 보안프로그램의 관리취약점을 이용하여 발생되었으며, 전자금융 보안프로그램에 대한 접근패턴을 이상거래 탐지시스템과 연계하고 실시간으로 분석하여 모니터링을 강화함으로써 내부자에 의한 유사 금융사고를 예방할 수 있다.

5.1.1 메인프레임 보안환경

글로벌 금융회사 및 국내 일부 대형 금융회사에서 사용하고 있는 메인프레임 시스템은 전용 보안솔루션인 RACF(Resource Access Control Facility)를 이용하여 시스템 자원에 대한 보호기능을 제공하고 있다. 하지만 메인프레임 보안솔루션에서 제공하는 기능은 시스템의 중요자원을 보호하기 위한 접근통제기능에 제한적으로 사용되고 있으며, 전자금융 보안프로그램

등 중요 프로그램에 대한 접근이력을 분석하고 이상 징후를 모니터링 하는 영역에는 아직 활용되지 못하고 있다. 내부자의 전자금융 보안 프로그램 접근기록을 전자금융 이상거래탐지 시스템과 연계하여 추가로 수집하고, 이상 징후를 분석 및 탐지한다면 내부자의 전자금융 보안 사고를 사전에 예방할 수 있는 대안이 될 수 있을 것이다.



〈Figure 2〉 Example of Mainframe RACF Setup Profile Information

<Figure 2>에서 메인프레임의 RACF 정책 설정 화면에 pw_check라는 전자금융 보안프로그램에 지정된 권한 이외의 접근이 발생할 경우, 감사로그 남도록 설정한 화면예시를 나타내고, <Table 4>는 설정화면에 대한 설명이다.

〈Table 4〉 Mainframe RACF Settings Profile Description

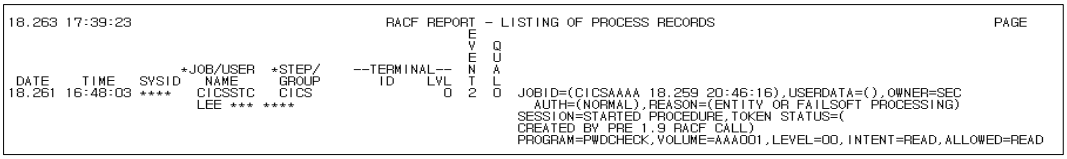
Classify	Detection item
CLASS	Resource control profile group
DATASET NAME	Location of the controlled security module
UNIVERSAL ACCESS	General status access - NONE: Unaccessible - READ: Possible - UPDATE: Possible, Module editable - ALTER: Possible, Module deleteable
AUDITING	Audit log storage status ALL(READ): Save events if it runs

수집된 감사로그는 RACF 유틸리티를 이용하여 <Figure 3>과 같이 위반사항을 추출할 수 있다.

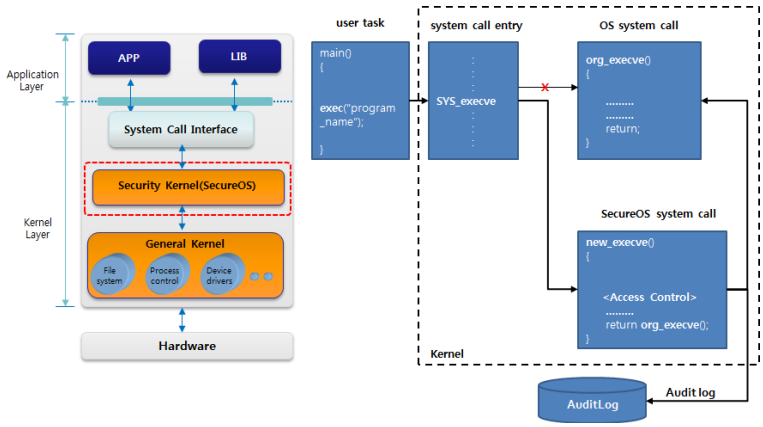
- QUAL 0: 온라인 거래가 아닌 배치프로그램 실행서버 등 동일 내부 IP 대역에서 반복적으로 접근로그가 발생하는 경우, 무작위 대입공격행위 의심
- QUAL 1: 내부IP 대역에서 접근로그가 발생하는 경우, 내부자의 사전 환경조사행위 의심

5.1.2 서버시스템 보안환경

서버시스템의 SecureOS 보안솔루션은 사용자영역에서 시스템 관리자원에 대한 실행, 읽기 등의 이벤트가 발생하는 경우, OS시스템 호출 전에 SecureOS의 보안 커널에서 접근통제 여부



〈Figure 3〉 Mainframe RACF Monitoring log Sample



〈Figure 4〉 Server Security Architecture

를 판단하고, 감사로그를 생성하는 아키텍처를 제공한다.

서버시스템에서 제공하는 보안솔루션도 시스템 관리자원에 대한 접근통제 정책을 기본적으로 적용하는데 제한적으로 사용하고 있어, 전자금융 보안프로그램 등 중요 접근분석이 필요한 로그수집과 전자금융 이상행위 탐지를 위한 연계기능 적용은 역시 미흡한 상태이다. 서버시스템 역시 보안솔루션으로부터 수집된 전자금융 보안프로그램의 접근제어 로그를 전자금융 이상거래탐지시스템과 연계하여, 내부자의 반복적인 무작위 대입공격이나 비인가자의 보안환경 사전확인 시도 등 위협행위를 사전에 인지할 수 있다.

<Figure 5>에 서버시스템의 SecureOS 보안솔루션에 pw_check라는 전자금융 보안프로그램 접근 시 로그를 생성하기 위해 보안정책을 설정하고 지정된 권한 이외의 접근시도가 발생한 경우 감사로그 남도록 적용한 화면예시를 설명하였다.

〈Figure 5〉 Electronic Financial Security Program Access Control Log Screen

5.2 전자금융 이상거래 탐지영역 확대

전자금융 이상거래 탐지를 위해 수집되는 정보의 유형은 전자금융 이용자의 환경정보로부터 수집되는 전자금융 이용매체 환경정보, 전자금융 거래를 수행할 때 거래정보로 부터 수집되는 거래유형 정보, 금융보안원 전자금융 이상정보 공유시스템이나 금융결제원 등을 통해 수집되는 사고유형정보가 있으며 세부 내용은 <Table 5>와 같다.

내부자에 의한 전자금융 보안사고를 예방하기 위해서는 기존의 전자금융 이상거래탐지를 위한 수집영역 외 <Table 6>과 같이 추가로

〈Table 5〉 Information Collected for Analysis of Electronic Finance Abnormalities

classify	Major Collection Items
User media environment information	IP, MAC, VPN information Proxy access status Certificate expired status Security program use status Security media OS information (Android, IOS, Windows) H/W Unique number (HDD, CPU, NIC etc.) Location information
Financial transaction type information	Transaction time Transaction information (transaction code, screen code) Transfer amount the remitter Account information(new and not used) Repetitive and multi-account transfer Total number and amount of transfer Attempt to change personal information
Accident type information	Error limit exceeded Blacklist registration status past incidents External agency shared information

보안프로그램 접근정보, 접근한 이용자정보, 작업수행 정보, 접근한 이용자 보안매체 정보 등 전자금융 보안솔루션 접근로그와 호출 파라미터로부터 내부자 이상행위 정보를 실시간 수집하여야 한다.

〈Table 6〉 Additional Information for Analysis of Insider Abnormalities

Classify	Collection Items
Insider usage information	Access Security Program Name Access time About Accessors(ID, JobID) IP information Operation performance information (automation, individual) Access user name(bankingID) Security card serial number Customer identifier, etc.

5.3 내부자 이상행위 탐지 룰 도출

수집된 정보는 이상행위를 판단하는 기존의 방식과는 달리 동일한 유형의 과저 정상 행위와의 구분을 위해 프로파일링을 통한 머신러닝을 이용한 기준값을 축적한다. 비정상 행위는 평소와 다른 행위(Unusual Activity)를 실시간으로 탐지하고, 정상적인 행위와의 편차 및 이벤트 발생주체의 위험수준에 따라 등급이 분류된다.

- 위험등급 High 사례
  - 전자금융 거래로그와 중요 이용자정보 변경 시점이 불일치(원장 임의수정 의심)
  - 내부IP대역에서 일정시간 내 동일고객 ID의 비밀번호 검증실패로그가 임계치 초과(내부자의 무작위 대입공격 의심)

- 위험등급 Medium 사례
  - 내부자 PC IP 대역에서 전자금융 보안프로그램 접근시도 발생(내부자 사전환경조사 의심)
  - 일정시간 내 외부 동일 IP 대역에서 복수의 고객 ID의 로그인 시도가 임계치 초과(외부자의 무작위 대입공격 의심)

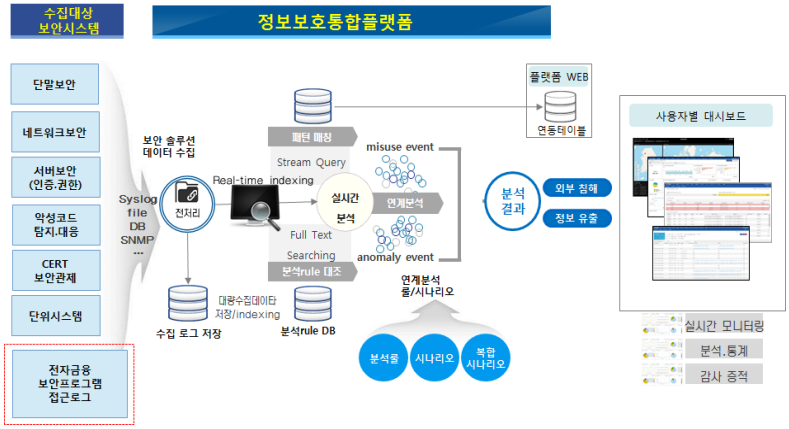
위험등급이 High인 경우는 사고발생 가능성이 높은 상황이므로 정보보호통합플랫폼에서 내부자 IP 격리 등 긴급 대응하고, 전자금융 이상거래탐지시스템에서 해당 고객 ID의 전자금융 서비스 긴급차단 후 사후조사를 실시하여야 하며, 위험등급이 Medium인 경우는 사고발생을 위한 사전단계로 수집된 이벤트를 기준으로 전자금융 보안프로그램 접근사유 및 접근실패원인 등 정밀조사 결과에 따라 대응하여야 한다.

5.4 정보보호 통합플랫폼 연동체계 구축

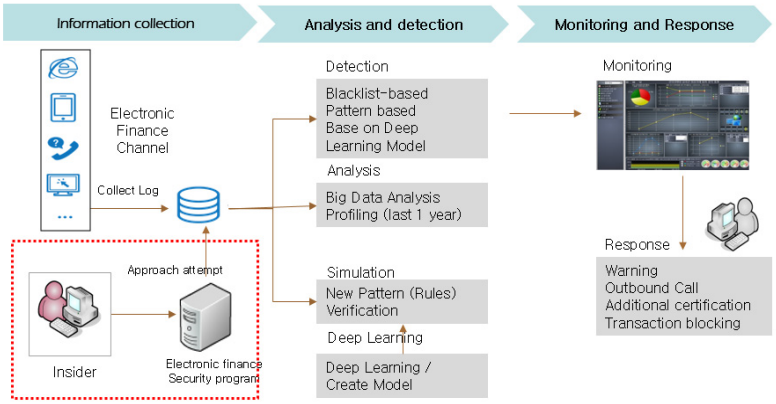
내부자의 비정상적인 전자금융 보안프로그램 접근이력은 수집된 내부자 정보(접근시간, 사용자 ID, 작업 ID, 접근시도 IP, 접근성공/실패여부 등)를 정보보호 통합플랫폼과 연계하여, 사전에 등록된 이상행위 탐지룰을 통해 특정 IP에서 임계치를 초과하는 반복적인 전자금융 보안프로그램 호출, 내부 IP에서 전자금융 보안프로그램 접근시도 등을 통해 전자금융 사고를 유발할 가능성이 있는 이상 징후를 발견할 수 있다. 이상 징후가 발견된 경우, 정보보호 통합플랫폼에서 대시보드를 통해 경보발생으로 실시간 모니터링 하고, 해당 IP의 네트워크 강제 접속차단 및 행위자에 대한 조사를 통해 정상여부를 확인한다.

5.5 전자금융 이상거래탐지시스템 연동체계 구축

보안솔루션에서 수집된 전자금융 보안프로그램 접근기록은 전자금융 이상거래탐지를 위한 하나의 정보수집 채널로서 분석서버에 실시간 연동되어 빅데이터 처리엔진에 의해 분석된다. 내부자는 정상적인 내부 업무처리 환경에서 이용자의 정보를 조회하거나 무작위 대입공격을



〈Figure 6〉 Security Platform Diagram



〈Figure 7〉 FDS Analysis Diagram

통해 비밀번호 등 중요 정보를 탈취할 가능성이 높으므로, 전자금융 이상거래탐지시스템의 장기간 접근이력의 프로파일링을 통해 정상거래와 내부자의 이상행위를 분석할 수 있는 탐지룰을 만들고, 탐지된 상황의 위험도에 따라 대응등급을 분류한다. 비정상 접근시도로 판단되는 해당 고객의 전자금융 거래가 발생할 경우, 로그인 시점, 금융거래 시점, 최종 전자서명 시점에 Alert 발생, 추가인증, 아웃바운드 상담 등 이용자 보호를 위한 전자금융 이상거래 대응체계와 연동하여 처리하여야 한다.

6. 결 론

본 연구에서 기존의 금융회사의 전자금융 이상거래 탐지시스템의 환경에 시스템 보안솔루션을 이용하여 내부자의 이상행위 정보를 추가로 수집하고, 탐지룰에 의해 연계분석을 통해 추가적인 전자금융 사고를 예방할 수 있는 방안을 제시하였다.

내부자가 업무처리 환경에서 고객의 전자금융 이용정보를 탈취하여 발생하는 금융사고는 기존의 직무분리, 승인 및 제3자 검토기능을 강화하는 것도 중요하지만, 근본적으로 전자금융 보안프로그램에 대한 접근기록에 대한 분석 및 모니터링을 통해 원천적으로 예방하는 것이 필요하다. 비정상적인 행위는 전자금융 이용자의 프로파일링을 통한 비정상적인 거래를 탐지하는 것과 마찬가지로 내부자 행위에 대한 프로파일링을 통해 판단해야 한다.

이상 징후가 발견된 경우, 정보보호 통합플랫폼에서 대시보드를 통해 경보발생으로 실시간 모니터링 하고, 해당 IP의 네트워크 강제 접속차단 및 행위자에 대한 조사를 통해 정상여부를 확인하여야 하고, 전자금융 이상거래탐지시스템에서 주기적으로 최근 수집데이터를 대상으로 학습시켜 최적의 딥러닝 모델을 도출하고, 이러한 과정을 반복하여 이상거래 탐지의 오탐을 최소화하여 내부에서 발생하는 무작위 대입공격 및 정상적인 원장 접근을 위장한 오남용 행태를 판단함으로써 정교화된 이상거래

탐지를 통해 전자금융 이용고객의 불편을 최소화하고 전자금융 사기로부터 이용자를 보호할 수 있을 것이다.

References

[1] Alpaydin, E., Introduction to Machine Learning, Second edition, MIT Press, Cambridge, Massachusetts, 2014.

[2] Choi, E. S. and Lee, K. H., “A Study on Improvement of Effectiveness Using Anomaly Analysis rule modification in Electronic Finance Trading,” Journal of The Korea Institute of Information Security & Cryptology, Vol. 25, No. 3, Jun, 2015.

[3] Data Breach Investigations Report 2015, https://enterprise.verizon.com/resources/reports/dbir.

[4] Duda, R. O., Hart, P. E., and Stork, D. G., Pattern classification: John Wiley & Sons, 2012.

[5] Eldardiry, H., Sricharan, K., Liu, J., Hanley, J., Price, B., Brdiczka, O., and Bart, E., “Multi-source fusion for anomaly detection: using across-domain and across-time peer-group consistency checks,” JoWUA, Vol. 5, No. 2, pp. 39-58, 2014.

[6] Financial Supervisory Service in Korea, http://www.fss.or.kr/promo/bodobbs_view.jsp?seqno=21371.

[7] Grand Theft Data in McAfee, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-data-exfiltration.pdf.

[8] Guyon, I. and Elisseeff, A. An introduction to variable and feature selection, Journal of Machine Learning Research, Vol. 3, pp. 1157-1182, 2003.

[9] Han, H. C., Kim, H. N., and Kim, H. K., “Fraud Detection System in Mobile Payment Service Using Data Mining,” Journal of The Korea Institute of Information Security & Cryptology, Vol. 26, No. 6, 2016.

[10] ISO/IEC/JTC1/SC27, ISO/IEC DTR 13335-1, Guidelines for the Management of IT Security-Part 1: Concepts and Models of IT Security.

[11] ISO17799, What is ISO17799(the ISO Security Standard)?.

[12] Jeong, S., H., Kim, H. N., Shin, Y. S., Lee, T. J., and Kim, H. K., “A Survey of Fraud Detection Research based on Transaction Analysis and Data Mining Technique,” Journal of The Korea Institute of Information Security & Cryptology, Vol. 25, No. 6, pp. 1525-1540, 2015.

[13] Kim, H. D., Kim, J. H., Park, M. S., Cho, S. H., and Kang, P. S., “Insider Threat Detection based on User behavior Model and Novelty Detection Algorithms,” Journal of the Korean Institute of Industrial Engineers, Vol. 43, No. 4, pp. 276-287, 2017.

[14] Kim, Y. G. and Choi, J. Y., “A Study on the Korean company’s readiness against to Insider Threat,” Korea Computer Science Conference, pp. 1087-1089, 2017.

[15] Liang, N. and Biros, D., “Validating Common Characteristics of Malicious Insiders: Proof of Concept Study, In System Sciences (HICSS),” 2016 49th Hawaii International Conference on (pp. 3716-3726), IEEE, Feb 2016.

[16] Lunt, T. F., Jagannathan, R., Lee, R., Whitehurst, A., and Listgarten, S., “Knowledge-based intrusion detection,” In AI Systems in Government Conference, Proceedings of the Annual (pp. 102-107). IEEE, 1989.

[17] Mundie, D. A. Perl, S., and Huth, C. L., “Toward an ontology for insider threat research: Varieties of insider threat definitions,” In Socio-Technical Aspects in Security and Trust (STAST), 2013 Third Workshop on (pp. 26-36), IEEE, Oct 2013.

[18] Na, O. C. and Chang, H. B., “Security Knowledge Classification Framework for Future Intelligent Environment,” The Journal of Society for e-Business Studies, Vol. 20, No. 3, pp. 47-58, 2015.

[19] Park, E. Y. and Yoon, J. W., “A Study of Accident Prevention Effect through Anomaly Analysis in E-Banking,” The Journal of Society for e-Business Studies, Vol. 19, No. 4, pp. 119-134, 2014.

[20] Ponemen Institute, 2017 Global Study on Application Security May 2017.

[21] Shin, H. W., “Methodology to analyze insider risk for the prevention of corporate data leakage,” Korea Computer Science Conference, Vol. 39, No. 1(C), 2012.

[22] Ted, E., Goldberg, H. G. Memory, A., Young, W. T. Rees, B, Pierce, R., and Essa, I. Detecting insider threats in a real corporate database of computer usage activity, In Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining (pp. 1393-1401), ACM, 2013.

[23] Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E., “The insider threat to information systems and the effectiveness of ISO17799,” Computers & Security, Vol. 24, No. 6, pp. 472-484, 2005.

저 자 소 개

이재용	(E-mail: jaeyong.lee@kbfg.com)
1993년	청주대학교 전자계산학과 (학사)
1992년～현재	KB국민은행 근무
2017년～현재	고려대학교 정보보호대학원 석사과정
관심분야	정보보호, 보안위험분석, 금융암호학, 역할기반접근통제(RBAC)

김인석	(E-mail: iskim11@korea.ac.kr)
1973년	홍익대학교 전자계산학과 졸업 (학사)
2003년	동국대학교 정보보호학과 졸업 (석사)
2008년	고려대학교 정보경영공학과 졸업 (박사)
2009년～현재	고려대학교 정보보호대학원 교수
관심분야	전자금융보안, IT감사, 전자금융법규