Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.2, Apr. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.2.343

금융IT인력의 보안사고 위험도에 기반한 정보접근 통제 정책 연구

심 재 윤,† 이 경 호‡
고려대학교 정보보호대학원

A Study on Information Access Control Policy Based on Risk Level of Security Incidents about IT Human Resources in Financial Institutions

Jae-yoon Sim,† Kyung-ho Lee‡
Graduate School of Information Security, Korea University

요 약

국내 금융권은 은행창구를 통해 전통적 수신, 여신 상품을 판매하던 구조에서 금융 소비채널의 변화 및 금융상품의 패러다임 변화를 겪으며 무한경쟁시대로 진입하고 있다. 이에 따라, 금융서비스의 개인화는 점점 가속화되고 있으며, 금융 관련 개인정보의 가치는 더욱 높아지고 있다. 2014년 카드사 정보유출사고에서 보았듯이, 대부분의 대형 금융관련 정보유출 사고는 해당 정보에 접근 권한을 가진 인력에 의해 발생한다. 따라서, 이러한 대량의 금융 관련 개인정보에 접근 권한이 있는 인력에 대한 기존의 정보 접근 통제정책 적용기준에 문제는 없는지 확인해 볼 필요가 있으며, 보안사고의 위험도에 영향을 미치는 요인에 따라 정보 접근 통제정책을 보완할 필요가 있다. 본 논문에서는 직무상 대량의 금융 정보에 접근 권한이 필요한 금융IT인력에 대해 직무, 직책 및 접근 정보의 민감도를 기준으로 보안사고의 위험도 측정에 필요한 영향 요인이 무엇인지 양적분석을 수행하고, 분석결과를 반영한 정보 접근 통제정책을 실무적 사례에 적용해 봄으로써 금융IT인력의 보안사고 위험도를 최소화할 수 있는 방안을 제시한다.

ABSTRACT

The financial industry in South Korea has witnessed a paradigm shift from selling traditional loan/deposit products to diversified consumption channels and financial products. Consequently, personification of financial services has accelerated and the value of finance-related personal information has risen rapidly. As seen in the 2014 card company information leakage incident, most of major finance-related information leakage incidents are caused by personnel with authorized access to certain data. Therefore, it is strongly required to confirm whether there are problems in the existing access control policy for personnel who can access a great deal of data, and to complement access control policy by considering risk factors of information security. In this paper, based on information of IT personnel with access to sensitive finance-related data such as job, position, sensitivity of accessible data and on a survey result, we will analyze influence factors for personnel risk measurement and apply data access control policy reflecting the analysis result to an actual case so as to introduce measures to minimize IT personnel risk in financial companies.

Keywords: RBAC, Sensitivity of Information, Risk Level of Security Incidents, Business Continuity

접수일(2014년 11월 4일), 수정일(1차: 2014년 12월 8일, 2차: 2014년 12월 15일), 게재확정일(2014년 12월 15일)

† 주저자, smilebanker@korea.ac.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

I. 서 론

현재 국내 금융권은 기존 은행창구를 통해 수신, 여신 등의 전통적 금융상품을 판매하던 시대에서 스마트폰으로 대변되는 금융소비 채널의 변화, 파생상품 등의 다양한 금융기술이 활용된 금융상품 패러다임의 변화로 절대적 우위의 시장지위를 가진 금융사가 없는 무한경쟁시대에 진입하고 있다. 이러한 변화는 데이터마이닝, 데이터마트를 통한 고객성향 분석 등 금융서비스의 개인화를 더욱 가속화시키고 있으며, 이에 따라 금융 관련 개인정보의 가치도 더욱 상승하고 있다. 이를 여실히 보여주는 것이 고객 개인정보이다. 예를 들면, 고객 이름, 전화번호, 집 주소와 같은 단순 고객 개인정보는 한 건당 50~300원의 가격으로 불법적으로 거래된다고 한다. 게다가 주민등록번호, 신용등급, 대출이력 등의 고객 개인정보는 더 높은 가격을 형성하고 있다[1]. 따라서, 2014년 카드사의 정보유출사고에서 보았듯이, 대량의 금융관련 개인정보에 접근 권한을 가진 사람에 대한 정보 접근 통제정책은 매우 중요하며, 기존의 정보 접근 통제정책에 문제가 없는지 확인해볼 필요가 있다.

본 논문에서는 직무상 대량의 금융 정보에 접근 권한이 필요한 금융IT인력에 대해 직무, 직책 및 접근 정보의 민감도를 기준으로 보안사고의 위험도 측정에 필요한 영향 요인이 무엇인지 설문을 통해 분석하고, 분석결과를 반영한 정보 접근 통제정책을 실무적 사례에 적용해 봄으로써 금융IT인력의 보안사고 위험도를 최소화할 수 있는 방안을 제시한다.

II. 관련 연구

2.1 인력보안과 정보 접근 통제 정책의 중요성

인력보안이란, 그 일에 선택된 사람들에 대해서는 안전하며 효율적 업무의 수행을 보장하기 위한 중요하고 필수적인 관리수단을 의미한다. 임종인(2002)은 '인력보안의 주요한 보호대상으로는 조직의 모든 사업을 계획·집행하게 되거나, 하고 있거나, 하였던 자, 영업비밀 등 핵심기밀이나 중요정보 자산을 보유하게 되거나, 보유하고 있거나, 보유했던 자를 그 대상으로 하는 것이 일반적이다'라고 하였다[2].

차인환(2009)은 인력 보안 관리를 위해 도출된 지표로 인력 보증, 개인 역량, 보안 통제 등을 제시한다. 인력 보증과 깊은 상관이 있는 항목은 배경조사, 자력평가, 보안인증이고, 개인 역량과 높은 상관관계를 보여준 항목은 보안의식, 보안교육, 보안평가이고, 마지막으로 보안통제와 관계 깊은 항목은 업무통제, 사고통제, 접근통제이다. 이것은 기존의 연구와는 달리 인력 보안에 초점을 맞추어 관리지표를 도출함으로써 인력 보안관리의 이론적 기초를 마련하였지만 인력 보안의 실제 사례와 관련짓거나 실제 조직에 적용한 연구가 아니기에 한계가 있다고 할 수 있다[3].

최창래 외(2014)는 금융회사 내 IT도급 정책과 관련된 외주인력 보안리스크를 줄이는 정책적 방안을 제시한 연구에서 금융 IT업무 과정 내에서 분석, 설계와 같이 본질적 업무는 IT 담당 내부 직원이 담당하고 개발 설계 상의 요구를 숙지하는 한편, 외주직원은 주어진 가이드라인에 맞게 코딩 업무를 담당해야 함을 제안한다. 그리고 이를 통해 금융 프로그램의 비용, 품질을 제고할 뿐만 아니라, 아웃소싱에서 비롯되는 위험을 줄일 수 있음을 주장한다[4].

심명섭(2013)은 IT 외주용역 보안을 관리적, 기술적, 물리적 영역으로 세분하고, 각 영역에 해당하는 보안 수준을 제고함으로써 인력보안 수준을 높이는 방안을 제시한다. 더 나아가 IT 외주용역 보안에 있어서 관리적 보안이 기술적, 물리적 보안보다 중요하다는 결론을 제시한다[5].

대부분의 보안관리 체계는 인력보안관리 부분을 하나의 기능으로 분류하여 구체적인 인력보안 관리 표준을 제공하지 못하므로 실질적인 인력보안 업무 수행이 제한되는 실정이다. 또한 인력보안 관리 주제를 직접적으로 연구한 노력은 국내외 모두 아주 부족한 편이다[6].

정보 유출의 사회적 비용은 시장에서 유출된 정보의 양과 시장가격으로만 계산되지 않는다. Table 1.와 같이 정보 유출이라는 일종의 정보 침해사고 관련

Table 1. Classification of social costs in information infringement incidents[7]

Indirect costs	Cost for System management and Replacement	Loss of corporate image
Direct costs	IR response cost. Labor cost for accident correspondence. Decrease in sales due to reduced customer.	Legal costs Fall in stock price
	Explicit costs	Potential costs

사회적 비용은 직접비용(Direct Costs)과 간접비용(Indirect Costs), 명시적 비용(Explicit Costs)과 잠재적 비용(Implicit Costs)으로 나누어 분석될 수 있다. 유진호(2008)는 정보유출로 인한 '시스템 관리와 교체, 지적재산권 비용, 사고 조치에 따른 인건비, 사고로 인한 매출 하락, 기업의 대외 이미지 실추, 법률 서비스 비용, 주식 가격 하락 등은 조직의 명운을 결정할 만큼 영향력이 큰 사회적 비용'이라고 하였다[7].

이러한 비용을 초래한 사건들이 지난 2011년 4월부터 현재까지 국내 금융사에서 발생하였다. Table 2.에서 주요 정보 유출사고 중 2건을 제외하면 모두 내부인력 및 아웃소싱 인력에 의해 발생한 사고였다.

규모 면에서도 대부분이 내부자 및 아웃소싱 인력에 의한 보안 사고였다. 특히, 2014년 1월에 발생한 카드 3사 보안사고는 DB 관리자 권한을 가진 외주 인력에 의해 1억 4천만 여 건의 고객 개인정보가 유출된 사고였다. 따라서, 정보유출 사고의 큰 위협요인인 내부 및 외부 인력의 위험도를 측정하는 요인을 분석하고 기준을 설정하는 것은 매우 중요하며, 이러한 정보유출 사고의 핵심인 정보 접근 통제정책에 분석결과에 따른 기준을 반영하여야 한다.

Table 2. Main incidents of information leakage in financial corporations[4]

Time of occurrence	Company	Number of information leakage	Source of incident
June 2014	C Bank	11,000	Outsourced staff
December 2013	K Card, L Card, N Card	140 million	Outsourced staff
May 2013	M Insurance	160,000	Internal staff
April 2013	S Bank	34,000	Internal staff
March 2013	I Capital	5,800	Internal staff
February 2012	C Bank	103,000	Outsourced staff
August 2011	S Card	470,000	Internal staff
July 2011	H Card	97,000	Internal staff
May 2011	H Damage insurance	150,000	Hacking
April 2011	H Capital	1,750,000	Hacking

2.2 RBAC 선행연구

역할기반 접근통제 모델은 미 국가기준 표준화기구(NIST: National Institute of Standards and Technoloty)에서 표준을 2004년에 정립하였으며 표준안에서는 비즈니스 시스템 환경과 용도에 맞게 적용단계를 구분하였다.

핵심(Core) RBAC는 사용자(User), 역할(Role), 허가(Permission), 세션(Session)으로 구성되고, 허가는 객체(Object)와 운영(Operation)의 집합이다.

위계적(Hierarchical) RBAC는 역할 계층을 지원하기 위한 요구사항을 추가로 구성하고, 역할계층을 트리나 역트리구조로 제한하는 형태와 다중상속 개념을 포함하는 일반 형태로 구분된다.

제약적(Constrainted) RBAC는 핵심(Core) RBAC와 위계적(Hierarchical) RBAC에 직무분리를 추가하였다. 직무분리는 정적 직무분리와 동적 직무분리로 구분된다[8][9].

역할기반 접근 통제 정책은 기업환경 뿐만 아니라 데이터베이스, 운영체제 등에 적용될 수 있는 매우 유연한 접근정책으로, 임의적 또는 강제적 접근통제 정책보다 정보에 대한 추상적인 접근통제와 효율적인 접근권한 관리를 수행할 수 있는 장점을 가지고 있다. 가장 큰 특징은 정보에 대한 권한(permission)들은 사용자에게 직접 할당되지 않고, 정의된 역할에만 배정한다는 점이다. 따라서 사용자가 원하는 정보에 대한 연산을 수행하기 위해서는 먼저 해당 정보에 대한 연산을 실행할 수 있는 권한을 가진 역할의 소속원(member)이 되어야 한다[10].

RBAC 모델에서는 권한의 관리(permission management)를 기업 환경에서의 역할과 정보 객체간의 관계로 설정, 관리함으로써 사용자와 정보 객체수가 대단히 많은 기업환경에 매우 적합한 특성을 제공한다. 또한 최소권한원칙(least privilege principle), 임무분리(SOD: separation of duty), 자료추상화(data abstraction)와 같은 주요 보안원칙들 역시 지원하고 있다[11].

Fig.1.는 역할 기반 접근 통제 모델의 주요 구성요소와 구성요소간의 관계를 나타낸다.

- 역할(Role): 역할은 역할 기반 접근통제 모델의 핵심 요소로서, 주어진 기업 환경에서 정의된 업무 기능에 의해 정의된 권한과 책임의 집합체이

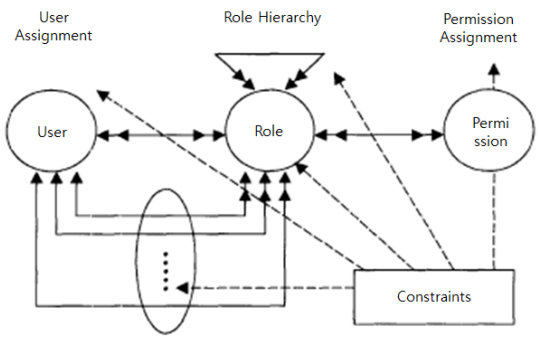

Fig. 1. Relationship between component items of RBAC

다.

- 역할계층(Role Hierarchy): 역할 계층은 배정된 권한들 사이에 포함관계가 있는 역할들 간의 부분 순서 관계로서 기업의 권한과 책임 체계와 매우 유사하여 기업의 권한 체계를 모델링 하는데 유용하다.
- 사용자(User): 사용자는 시스템을 사용하는 주체로서 직접 권한에 할당되지 않고 권한 부여된 역할에 할당됨으로써 객체에 접근할 수 있다.
- 권한(Permission): 권한은 객체에 대해 수행가능한 접근 모드들의 집합이다. 허가정보, 접근권한, 특권 등이 권한과 같은 의미로 사용된다.
- 세션(Session): 세션은 한 사용자와 여러 개의 역할 등으로 구성된 집합으로 표현될 수 있으며, 사용자는 세션을 통하여 자신에게 배정된 역할들을 수행한다.
- 사용자 배정(User Assignment)과 권한 배정(Permission Assignment): 객체에 대한 접근 권한은 역할에 배정하고(권한 배정), 사용자는 책임과 직무에 맞는 역할에 할당된다.(역할 배정)
- 제약조건(Constraints): 제약조건은 위에서 정의된 모든 구성요소들에 대하여 적용되며 각 구성요소가 가지는 특성을 제한사항이나 조건 등으로 기술한다. 제약조건의 예로서는 임무분리, 한 역할에 할당될 수 있는 최대 사용자의 수, 시간 제약사항 등이 있다[12][13][14].

2.3 A금융사의 IT인력 정보 접근 통제정책 사례연구

A금융사는 국내 수위 수준 용량의 z/OS[1] 기반 메인프레임 고객사로 세계적으로도 단일시스템 운영 기준으로 매우 큰 규모의 DB2[2] 환경에서 대용량 데이터베이스를 운영하는 금융사이다. 또한, CIO와 CISO 직책을 분리함으로써, 체계적인 정보보호 대책 수립 및 정책을 설계하여 시행하고 있다. 금융IT 인력의 정보 접근 통제정책이 실무에서 적용되는 사례를 분석하기 위해 A금융사의 정보 접근 통제정책 기준을 데이터 파일 접근권한, 데이터베이스 접근 권한으로 분류하여 조사하였다.

2.3.1 데이터 파일 접근 권한 정책

아래 Fig.2.은 A금융사가 금융 관련 정보가 발생하여 최초 집적되는 계정계 시스템에 대해 IT인력의 데이터 파일 접근 통제정책을 적용한 사례를 보여준다.

A금융사는 RBAC(Role Base Access Control)에 기반한 RACF(Resource Access Control Facility)[3] 솔루션을 이용해 직무기준에 따른 권한을 사용자에 부여하는 정보 접근 통제정책을 적용하고 있다. 이것은 Fig.2.에서처럼, A금융사의 직무분류기준인 'XAA' 직무그룹에 해당 직무그룹에 속한 모든 데이터 파일의 접근 권한을 부여한 후, 'XX1942', 'XX0107' 등의 사용자에 'XAA' 직무그룹에 부여된 모든 데이터 파일의 접근권한을 허용하고 있음을 의미한다.

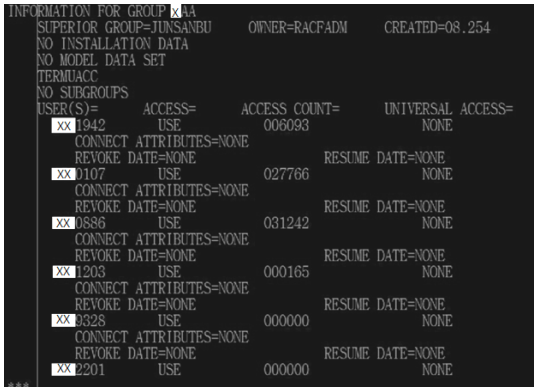

Fig .2. Example of information access control policy about IT human resources through RACF solution based on RBAC in financial institution 'A'

1) IBM사 메인프레임 시스템의 대표적 운영체제
2) IBM사가 개발한 대표적 DBMS로 세계적으로 오라클사의 오라클 DBMS와 DBMS 시장을 양분하고 있음.
3) IBM의 z/OS나 z/VM 운영체제 기반에서 접근 통제, 감사 기능을 제공하는 보안시스템[15]

2.3.2 데이터베이스 접근 권한 정책

아래 Fig.3.~Fig.5.는 A금융사가 계정계 시스템에 대해 IT인력의 데이터베이스 접근 통제정책을 적용한 사례를 보여준다. A금융사는 RBAC에 기반하여 DB 관리자가 사용자에 대한 데이터베이스 접근 권한을 'GRANT' 등의 DDL(Data Definition Language)문을 사용하여 직무그룹기준으로 부여하는 데이터베이스 정보 접근 통제정책을 적용하고 있다. DBMS 레벨에서 이렇게 직무그룹기준으로 관련된 DB테이블에 대해 일괄 부여된 접근 권한을 상위 레벨인 RACF 정책에서 사용자 ID에 적용 및 통제함으로써, 해당 직무그룹에 속한 사용자들의 RBAC 기반 데이터베이스 정보 접근 권한을 관리한다.

Fig.3.는 A금융사가 DB 자원과 관련하여 직무그룹기준의 데이터베이스 접근 권한을 부여하거나, 업무 프로그램이 IT 응용프로그램 변경관리 프로세스 등을 통해 적용된 경우에 해당 업무 프로그램에 접근할 수 있는 권한 부여와 같이 정형화된 절차를 통해 적용된 데이터베이스의 모든 접근 권한 건수를 조사해본 결과이다.

Fig.3.의 총접근권한건수 중 직무그룹기준으로 DB관리자가 직무그룹에 부여한 권한건수는 아래 Fig.4.과 같이 조사되었다. 이것은 A금융사가 직무그룹과 관련한 DB 테이블의 접근 권한을 Fig.2.에서처럼 'XAA'와 같은 직무그룹에 적용한 후, 사용자에 해당 직무그룹의 DB 테이블에 대한 접근 권한을 부여함으로써, 직무그룹보다 작은 단위의 세부직무를 수행하는 사용자도 직무그룹단위의 DB 테이블에 대한 모든 접근 권한을 가지게 된다. 참고로, Fig.4.의 GRANTOR는 권한을 부여한 사용자로 'XXXDBA'는 DB 관리자를 의미하며, GRANTEE

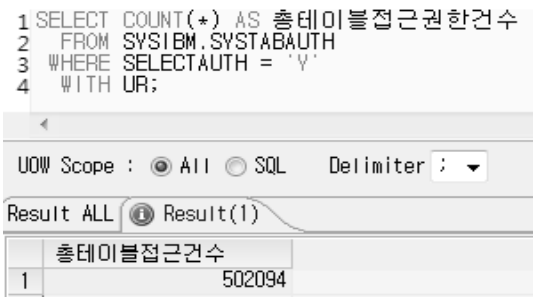

Fig. 3. Total count of access authorities associated with DB resources in financial institution 'A'

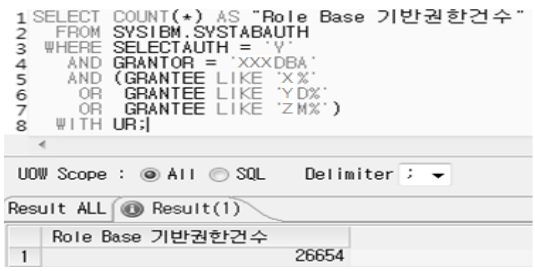

Fig. 4. Total count of which based on RBAC among access authorities associated with DB resources in financial institution 'A'

는 권한을 부여받은 사용자로 부여된 모든 사용자 권한 중에 A금융사가 정의한 직무그룹코드에 DB 테이블의 접근권한이 부여된 권한만을 추출하였다.

Fig.5.는 Fig.4.의 직무그룹에 부여된 DB 테이블의 접근 권한 일부를 추출해 본 것이다. 예를 들면, Fig.5.에서와 같이 'XAA' 직무그룹에 'TxxxxxxAF', 'TxxxxxxBH', 'TxxxxxxCA', 'TxxxxxxCL' 테이블에 대한 접근 권한이 부여되어 있다면, 'XAA' 직무그룹에 대한 DB 테이블 접근 권한을 부여받은 사용자가 세부 직무상 'TxxxxxxAF' 테이블만을 접근하여도 직무수행에 문제가 없는 경우에도, 직무에 필요한 정보 접근 권한보다 더 많은 정보에 접근할 수 있는 권한을 획득하게 된다. 이러한 직무그룹단위의 정보 접근 권한정책은 권한 관리의 편의성을 제공한다. 그래서 선행 연구로 2.2에서는 이러한 직무기반의 정보 접근 권한정책에 대해 자세히 알아보기 위해 권한 부여 기준이 되는 RBAC에 대한 연구를 수행하였다.

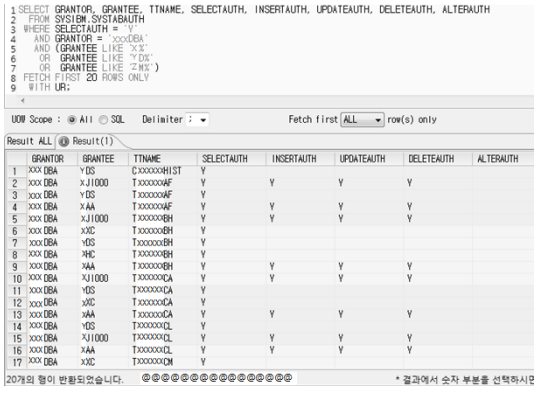

Fig. 5. Sampling rows of which based on RBAC among access authorities associated with DB resources in financial institution 'A'

III. IT인력에 대한 정보접근 통제 영향요인 연구

III에서는 최근의 금융기관 보안사고와 관련하여 정보 접근 통제정책에 대하여 실증적으로 검증하기 위해서 A금융회사를 모델로 접근하였다. A금융사의 정보 접근 권한정책의 기준이 되는 RBAC 기반의 정보 접근 통제정책이 대량의 금융 관련 개인정보를 다루는 금융IT인력의 보안사고 위험도 측정에 필요한 영향 요인 기준에 부합하는지 확인하고, 보완 또는 개선할 내용은 무엇인지 영향 요인 분석결과를 토대로 확인해본다.

3.1 본 연구에서 사용한 방법

연구방법은 아래와 같다.

첫째, 직무상 대량 금융 정보의 접근 권한이 필요한 금융IT인력에 대해 직무, 직책 및 접근 정보의 민감도 등의 독립변수가 보안사고의 위험도에 영향을 준다는 가설을 설정하고, 가설 검증을 위해 다양한 직무, 직책을 수행하는 금융IT인력에 대한 설문을 통해 가설을 검증한다. 둘째, 가설 검증결과에서 채택된 독립변수를 적용하여 금융IT인력에 대한 기존의 RBAC 기반의 정보 접근 통제정책의 개선방안을 제시해본다. 셋째, 제시한 개선방안을 2.3에서 조사해본 A금융사에 적용해본 사례 검증을 통해 실효성을 확인해본다. 마지막으로, 제시한 개선방안을 기준으로 금융IT인력의 직무수행에 대한 실무적인 관점에서 결론을 맺고, 향후 연구에서 보완 및 추가되어야 할 부분을 제시한다.

3.1.1 금융IT인력 설문조사 가설설정과 변수설정

설문 조사를 기초로 검증하기 위한 보안사고의 위험도 측정에 필요한 영향요인을 독립변수로 정의하여 설정한 가설은 Table 3.과 같다.

사고 시나리오 발생가능성 및 위협 정도란, Table 4.와 Table 5.에서 보듯이 사고 시나리오 각각의 발생가능성과 위협 정도를 곱한 값으로, 설문에서 발생가능성은 '높음, 중간, 낮음, 관련 없음'으로, 영향 정도는 '매우 위협적이다, 위협적이다, 보통이다, 낮다, 전혀 위협적이지 않다'로 구분되어 표현되었다.

가설 1에서 직무 중요도란, Table 6.에서와 같이 인력이 담당하는 직무의 보안사고 시 영향도로, '매

Table 3. Hypotheses

1	The higher the impact of job is, the higher the likelihood and threat degree of incident scenarios is.
2	The higher the level of position is, the higher the likelihood and threat degree of incident scenarios is.
3	The higher the sensitivity of information is, the higher the likelihood and threat degree of incident scenarios is.
4	The higher the level of position is, the higher the sensitivity of information is.

Table 4. Scenario Likelihood Criteria

Level	Description
High	Always occurring
Middle	Sometimes occurring
Low	Almost not occurring
N/A	Not applicable

Table 5. Scenario Impact Criteria

Level	Description
Very threat-ening	Severe incidents are induced and public ripple effect is high
Threat-ening	Security-sensitive data are leaked out, which is deemed illegal
Middle	Incidents are involved with breach of enterprise rules or state law
Low	Information is handled that is not that important to enterprises
None	Incidents are about publicized data or data that are not significant to enterprises in terms of security

Table 6. Job Impact Criteria

Level	Description
Very High	Job related to information leakage that incurs serious damage to enterprise or havs public influence
High	Job related to information leakage that involves sensitive information and the violation of law
Med-ium	Job related to information leakage that involves the violation of enterprise rules or state law
Low	Job related to information whose leakage is not significant
Very Low	Job related to publicized or insignificant information

우 중요하다, 중요하다, 보통이다, 낮다, 전혀 중요치 않다'로 구분되는 항목이다.

가설 2에서 금융 IT인력의 직책은 Table 7.에서처럼 기본적인 직책을 기준으로 하되 동일한 직책일 경우에 내부 인력이 외주 인력보다 높은 등급을 가진다.

가설 3에서 정보의 민감도란, Table 8., Table 9. 및 Table 10.에서와 같이 설문에서 기존의 정보

Table 7. Personnel Position Level

Personnel category	Position	Level
Internal personnel	Deputy General Manager	10
	Senior Manager	8
	Manager	6
	Assistant Manager	4
	Senior Clerk	2
Outsou-rced personnel	Chief Manager	9
	Senior Manager	7
	Manager	5
	Assistant Manager	3
	Senior Clerk	1

Table 8. Criteria of Security Perspective Sensitivity on Information

Level	Description
Very High	Information leakage that incurs serious damage to enterprise or have public influence
High	Information leakage that involves sensitive information and the violation of law
Medium	Information leakage that involves the violation of enterprise rules or state law
Low	Information whose leakage is not significant
Very Low	Publicized or insignificant information

Table 9. Criteria of Financial Sensitivity on Information

Level	Description
Very High	Severe financial asset damage to enterprise
High	Considerable costs for substitution or recovery
Medium	Costs of substitution or recovery that can be covered by budget item switch
Low	Low financial burden on enterprise
Very Low	No financial damage incurred

Table 10. Criteria of Business Perspective Sensitivity on Information

Level	Description
Very High	Extremely major influence on business, critical damage to most services or critical service disruption
High	Major influence on business, likely damage to some services or service disruption
Medium	Influence on business, delay of some significant services
Low	Minor influence on business
Very Low	No influence on business

중요도에 보안, 금전, 비즈니스 측면의 민감도 기준을부여한 것이다.

3.2 금융회사 IT 직무와 정보 분류

3.2.1 금융회사 IT 업무상의 직무 현황

2.3에서 사례로 확인해 본 A금융사는 총자산 기준 국내 수위 수준의 금융회사이다. A금융사의 IT 업무상 직무 현황은 Table 11.과 같다.

Table 11. Jobs of IT banking business(4)

Finance Committee, Financial Company IT System Business	
Inte-rnal pers-onnel	✓ Planning of deposit, loan, exchange transaction system ✓ Development of deposit, loan, exchange transaction system ✓ Operation of deposit, loan, exchange transaction system ✓ IT strategies, Financial Management regulations ✓ IT budgets, resource planning and management ✓ IT resources and purchasing management ✓ IT construction supervision resources and purchasing management ✓ IT audit planning and implementation ✓ Application of access control policies to oursourced staff ✓ Application of separation duties to outsourced staff

	✓ Establishment of internal information protection policy. Revision of guidelines and information protection related regulations. ✓ Development and implementation of information protection on electronic financial ✓ IT internal control implementation (System restrictions, Account Management, etc.) ✓ Development and implementation plan and enforcement on vulnerability analysis and evaluation. ✓ Development of business program (Analysis and design) ✓ Development of external business program for dissimilar IT interface support ✓ Risk information system business ✓ Management of foreign branch system
Out-sour-ced staff	✓ IT systems development and operation of task among deposit, loan, exchange transaction.(Payment through ATM, money transfer and balance inquiry, etc.) ✓ Development and management of groupware, e-mail, personnel system, such as the accounting system used by the co-operation between subsidiaries ✓ Development of the business program, which is an essential element (except for the analysis and design) ✓ Operation and management of network's hardware and software ✓ Operation and management of disaster recovery center ✓ Construction and operation of monitoring system against infringement attempts ✓ Installation and operation of security system to prevent electronic information infringement .(hacking, cracking) ✓ Simple tasks of executing IT system ✓ Managing infrastructure such as Generators, UPS, constant temperature humidity chamber ✓ Development of business program(except for analysis and design) ✓ Other outsourceable tasks

내부인력 직무는 계정계 전산시스템 기획, 개발, 운영 관련 업무, IT 본부 내의 전체적 관리 업무, 외주인력 관리, 규정 지침 관리, 내부통제 관리, 업무 프로그램의 개발.분석 및 설계, 대외 업무 개발, 리스크 정보계 업무, 국외 점포 시스템 관리등이다.

외주인력 직무는 계정계 전산시스템 개발 및 위탁 운영 업무, 정보계 개발 및 위탁 운영 업무, 네트워크 운영 및 관리 업무, 재해복구센터 운영 및 관리 업무, 보안 시스템 운영 및 관리 업무, 단순 배치성 업무, 제반 전산시설 관리 업무, 업무 프로그램의 분석 및 설계를 제외한 개발업무, 기타 상주 외주인력 수행 가능 업무 등이다.

3.2.2 금융회사 IT 직무 관련 정보

A금융사의 IT 직무 관련 정보는 크게 고객 정보, 계정계 정보, 재무 정보, 사원 정보, 기타 정보로 나눌 수 있다. 고객 정보에는 고객 개인정보와 고객 신용정보가, 계정계 정보에는 대표적으로 예금, 대출, 환거래 정보 등이 있다. 재무 정보에는 주식거래내역, 채무 정보, 거래처 사업자 번호, 리스크 관리 정보 등이 있고, 사원 개인정보와 기타 공통 기반성 데이터도 직무 관련 정보에 포함된다. Table 12.는 A금융사의 IT 직무 관련 정보를 나타낸 것이다.

Table 12. IT Banking-related Information

Customer information	Customer personal information
	Customer credit information
Account system information	Savings/loan/exchange transaction information
	Account information
	Fund transfer information
Financial information	Stock transaction information
	Liability information
	Business register number of corporate customers
	Risk management information
Employee information	Employee personal information
Others	Business dates, business branch information, etc.

3.3 금융사의 IT 사고 발생 시나리오

Table 13.의 금융회사 IT 사고 발생 시나리오는 2006년부터 2014년까지 발생한 국내외 대형 보안 사고들을 분석하여 정보유출 단계별로 발생 가능한 시나리오들을 작성하였다. 정보 유출이 일어날 수 있는 DB, 어플리케이션, 사용자 PC 등의 대상을 중심으로 시나리오를 구성하였다. Table 13.는 장기간 발생한 기존의 사고관련 데이터를 기초하여 시나리오가 작성되었다는 점에서 향후 보안사고가 발생할 때마다 사고 발생 시나리오를 지속적으로 업데이트하여 사고 발생 시나리오에 미리 대비할 필요가 있다. 3.4에서는 이러한 사고 시나리오의 위험수준을 높이는 인력의 위험도 영향요인을 확인해 보기 위해, 3.1.1에서 설정한 가설을 통해 설문조사를 실시하고 결과를 상관분석 하였다.

Table 13. Incident Scenarios

Attempted access to Operation DB by non DB administrator like developers, subcontractor, internal staff (success or Failure)
Attempted access to DB by DB administrator account during non-office hours (success or Failure)
Multiple DB queries that exceed the amount of normal queries
For personnel who only have inquiry authority to arbitrarily save sensitive data in PC or external storage media
Inquiry of sensitive data by the same account connected from different IP addresses
Inquiry of sensitive data by an account unregistered in DB table
Saving of sensitive data as files in the internal storage of DB
Booting in safe mode, inquiring sensitive data, and then saving them in USB, etc.
Deleting security programs without permission, connecting to DB, and inquiring and saving sensitive data
A)Saving inquired sensitive data in PC à B)Copying the data to storage media(USB, external hard driver, DVD) or via e-mail, messenger, SNS, etc.
A)System administrator PC infected by malicious code à B) Connection by external system, or external attacks
A) Connection by external system, or external attacks à B) Connection by external system, or external attacks
Login attempt by an application user(developers, outsourced staff, internal employee) from an IP address different from previous access sources (success or failure)
Attempted access to applications by a user during non-office hours((holidays, overtime) (success or failure)
Multiple DB queries that exceed the amount of normal queries
For application user to save sensitive data through application in PC, USB, etc.
Connection to applications and inquiry of sensitive data by an account from different IP addresses
Deleting security programs without permission, connecting to application, and inquiring and saving sensitive data
A)Saving in PC sensitive data inquired through application à B) Copying the data to storage media(USB, external hard driver, DVD) or via e-mail, messenger, SNS, etc.
Printing out PC files containing sensitive data
Possessing in PC or shared folders sensitive data unnecessary for tasks
Decrypting encrypted sensitive data
Sending an e-mail containing sensitive data
A)Accessing object of attack through remote access or during work and saving sensitive data à B) Sensitive data in PC leaked out

3.4 금융 IT인력 설문 조사에 기초한 상관분석

금융IT인력의 보안사고의 위험도 측정에 필요한 영향 요인을 알아보기 위해 금융 IT 주요 직무, 직무 관련 정보, 사고 발생 시나리오에 기초하여 A금융사의 IT 업무 종사자 53명을 대상으로 설문을 실시하였으며, 이 중 44명(83%)이 설문에 응답하였다. 설문 응답자의 구성과 설문의 주요 내용은 각각 Table 14., Table 15.과 같다.

Table 3.의 가설을 검증하고자 Pearson 상관분석을 이용하였다. 여기서 도출되는 상관계수는 두 변수 간의 선형적인 상관성을 보여주는 값이며, 이 값의 범위는 -1과 +1 사이이다. 상관계수가 양수이

Table 14. Demographic of Survey

Personnel category	Position	Employment period(year)	Number of survey
Internal personnel	Deputy General Manager	20 or more	1(2%)
	Senior Manager	14~19	5(11%)
	Manager	8~13	4(9%)
	Assistant Manager	4~7	11(25%)
	Senior Clerk	less than 4	1(2%)
Outsourced personnel	Chief Manager	18 or more	5(11%)
	Senior Manager	12~17	2(5%)
	Manager	8~11	6(14%)
	Assistant Manager	4~7	8(18%)
	Senior Clerk	less than 4	1(2%)
Total			44

Table 15. Questionnaire Contents

	Description
Basic Contents	Department, Position level, Internal/Outsourced staff
Job-related Contents	Jobs, Significance of jobs, Job-related information, Impact of job-related information
Scenario-related Contents	Risk scenarios, Likelihood of occurrence of scenarios, Degree of threat of scenarios in terms of security, finance, and business

면 두 변수는 양의 관계에 있어서 같은 방향(우상향)으로 움직인다는 것을 의미하고, 상관관계가 음수이면 두 변수는 음의 관계에 있어서 한 변수의 값이 증가할 경우 다른 변수의 값은 감소한다는 것을 의미한다. 유의 수준이 〉 0.05 이면 상관관계가 없고, 유의 수준이 〈 0.05 이면 상관관계가 있다. 상관계수가 -1.0 ~ -0.7 사이면 강한 음의 선형관계, 상관계수가 -0.3 ~ -0.7 사이면 뚜렷한 음의 선형관계, 상관계수가 -0.1 ~ -0.3 사이면 약한 음의 선형관계, 상관계수가 -0.1 ~ 0.1 사이면 거의 무시될 수 있는 선형관계, 상관계수가 0.1 ~ 0.3 사이면 약한 양의 선형관계, 상관계수가 0.3 ~ 0.7 사이면 뚜렷한 양의 선형관계, 상관계수가 0.7 ~ 1.0 사이면 강한 양의 선형관계를 보여준다.

Table 16.에서와 같이 직무 중요도, 직급과 사고 시나리오 발생가능성 및 위협 정도는 각각 0.125, 0.179의 약한 양의 선형관계를 보였고, 직급과 정보 민감도는 0.083의 거의 무시될 수 있는 선형관계를 보였다. 이를 통해 가설 1, 2, 4에서 상정한 상관관계가 뒷받침되기 어려움을 알 수 있다. 반면, 정보의 민감도와 사고 시나리오 발생가능성 및 위협 정도는

Table 16. Results of Pearson Correlation Analysis

		Likelihood and impact of incident scenario
Impact of jobs	Pearson Correlation Coefficient	.125
	Significance Probability (Both sides)	.417
	N	44
		Likelihood and impact of incident scenario
Position level	Pearson Correlation Coefficient	.179
	Significance Probability (Both sides)	.244
	N	44
		Likelihood and impact of incident scenario
Sensitivity of information	Pearson Correlation Coefficient	.655**
	Significance Probability (Both sides)	.000
	N	44
		Sensitivity of information
Position level	Pearson Correlation Coefficient	.083
	Significance Probability (Both sides)	.591
	N	44

** Correlation coefficient is meaningful within the significance level of 0.01(both sides)

0.655의 뚜렷한 양적 선형관계를 보였고, 이 상관계수는 0.01의 유의수준 내에서 유의미하였다. 이는 가설 3 "정보의 민감도가 높을수록 사고 시나리오 발생가능성 및 위협 정도가 높아질 것이다"을 뒷받침한다고 할 수 있다.

위의 상관분석 결과를 기초로 가설 1, 2, 4는 기각하고 가설 3은 채택하였다 (Fig 6).

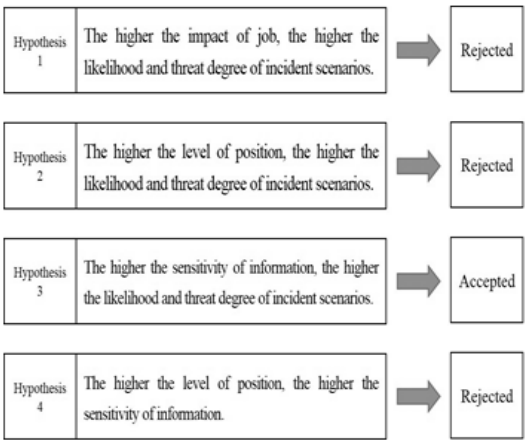

Fig. 6. Result of Hypothesis Test based on Correlation Analysis

3.5 정보 접근 통제에 대한 금융IT인력 위험도 측정

앞서 2.3에서 사례로 제시했던 A금융사의 직무기준 정보 접근 권한 부여 정책에 따른 IT인력의 위험도는 Fig.7.과 같다.

위험도를 결정하는 다른 독립변수의 변량이 변동되지 않는다면, A금융사는 RBAC기반의 정보 접근 통제 정책을 적용하므로, 위험도는 Fig.7.과 같이 전산 인력에 대한 정보 접근 통제 수준에 따라 결정된다.

3.4의 상관분석에서 유의미한 상관관계를 보인 가설3의 변량은 금융IT인력 보안사고의 위험도 측정에 필요한 영향 요인을 제시함으로써, 기존의 정보 접근 통제 정책에 정보의 민감도에 따른 정보 접근 통제가 적용되어야 함을 의미한다. 따라서, Fig.7.의 기존 위험도 산정 기준에 가설 3의 유의미한 결과인 정보의 민감도를 반영한 정보 접근 통제 정책에 따른 금융IT인력의 위험도는 아래 Fig.8.과 같이 구할 수 있다. 앞서, Fig.7.의 '전산 인력에 대한 RBAC 기반 정보 접근 통제 수준'은 A금융사와 같이 RBAC 기반의 정보 접근 통제 수준을 적용하는 많은 기업들에 적용이 가능하나, RBAC 기반의 정보 접근 통제 정책을 적용하지 않는 기업들 역시 기존의 정책에 정보의 민감도를 반영하여 적용이 필요하다. 따라서, 해당 독립변수는 Fig.8.에 '전산 인력에 대한 현재 정보 접근 통제 수준'으로 일반화하여 적용한다.

Fig.8.은 기존의 정보 접근 통제정책에 정보의 민감도에 따른 정보 접근 통제를 적용하여 정보에 접근하는 사용자들이 취급하는 정보의 민감도 합을 가장 작은 값에 최대한 수렴하도록 함으로써, 금융IT인력의 보안사고 위험도를 최소화해야 함을 의미한다. 정보 접근 통제 정책에 따른 IT인력의 위험도를 결정하는 다른 독립변수들이 모두 동일하다고 가정하면, 정보의 민감도에 따른 정보 접근 통제 적용 수준이 높을수록 위험도는 비례하여 낮아진다.

정보의 민감도에 따른 금융IT인력의 보안사고 위험도 분포는 아래의 Fig.9.과 같이 분석되었다.

Fig.9.은 산출된 정보의 민감도, 사고 시나리오 발생가능성 및 위협 정도의 값들을 백분위로 산출한 다음, 0.66~0.99(상), 0.33~0.66(중), 0~0.33(하)의 영역으로 구분하여 나타내었다. 금융IT인력의 보안사고의 위험도 측정 결과를 시각화한 Fig.9.은 정보 접근 통제정책의 유용한 근거자료로 활용될 수 있다. 이를테면, 정보의 민감도와 사고 시나리오 발생 가능성이 모두 상인 인력에 대해서는 적절한 통제방안을 마련하고 권한을 줄인다든가, 인력에 대한 모니터링을 강화하는 등의 관리적 보안 조치를 강화

Risk of IT human resources based on Information Access Control Policy
= F(∑(Total Value of authorized information to IT human resources),
∑(f(Possibility of threat by accident scenario,
Level of threat by accident scenario)),
∑(Level of Information Access Control based on RBAC about IT human resources)
)

Fig. 7. Formula which calculates risk level about current information access control policy based on just RBAC in financial institution 'A'

Risk of IT human resources based on Information Access Control Policy
= F(∑(Total Value of authorized information to IT human resources),
∑(f(Possibility of threat by accident scenario,
Level of threat by accident scenario)),
∑(f(Current Level of Information Access Control about IT human resources,
Applied Level of Information Access Control based on Sensitivity of Information))
)

Fig. 8. Generalized formula which calculates risk level about information access control policy based on the impact factor 'Sensitivity of Information' derived as result of correlation analysis

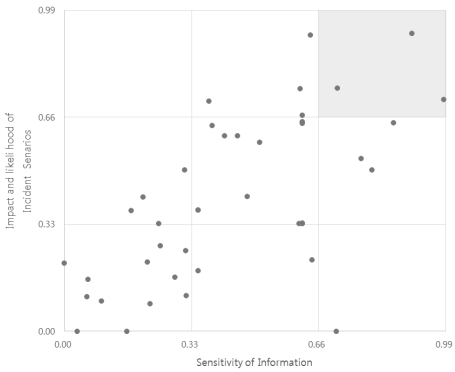

Fig. 9. Individual risk level of IT human resources who participated in this survey

할 수 있다. 더 나아가, 조직의 위험 수용 정도(Risk Appetite)를 조사한 다음, 본 연구의 결과와 결합시키면 조직 내의 보안사고 위험 인력을 식별하고 관리하는 데 있어서 효과적일 것으로 판단된다.

IV. 연구결과 적용사례

정보 접근 통제정책에 따른 금융IT인력의 위험도에 유효한 영향 요인인 정보의 민감도를 현재 RBAC 기반의 정보 접근 통제정책을 적용하고 있는 A금융사의 데이터 파일 접근 통제, 데이터베이스 접근 통제에 적용해보았다.

4.1 데이터 파일 접근 통제 정책에 적용

A금융사는 2.3에서 확인했듯이, RBAC 방식의 RACF 솔루션을 사용하여 데이터 파일 정보 접근 권한을 통제하고 있다. 현재 직무 부여 기준에 따라 적용된 정보접근 권한 통제 방법은 설문의 상관분석 결과에 따라, 정보의 민감도 기준으로 재구성해야 한다. 그러나, 현재 IT인프라를 운영하고 있는 기술인력의 재배치, 기술습득의 시간제약 등으로 인한 비지니스 연속성(business continuity)의 침해가 발생할 수 있어 기존 직무 부여 기준의 정보 접근 권한 통제를 일시에 변경할 수 없다. 따라서, 현재의 비지니스 연속성을 유지할 수 있는 범위내에서 정보의 민감도에 따른 직무의 재편성을 통해 정보 접근 통제가 추가 적용될 수 있도록 해야 한다. 2.3에서 확인해 본 A금융회사의 정보 접근 통제 사례에 비지니스의 연속성을 유지하는 범위내에서 정보의 민감도 영향요인을 반영하여 정보의 민감도를 반영한 RACF 정책

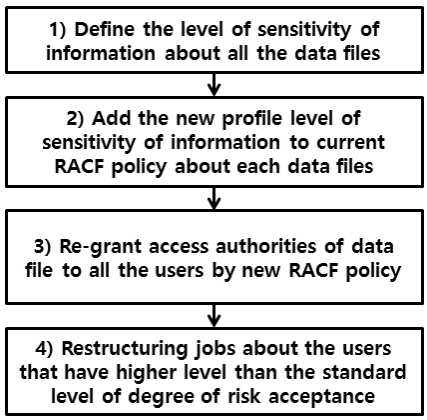

Fig. 10. Process of applying new profile level reflected sensitivity of information to current RACF policy

을 Fig.10.과 같은 절차에 따라 조정할 수 있다.

먼저, 모든 데이터 파일에 대해 보안적, 재무적, 비즈니스적 민감도에 따른 수준을 정의한다. 두 번째로, 각각의 데이터 파일에 적용된 현재의 RACF 정책에 앞서 정의한 정보의 민감도에 따른 새로운 프로파일(profile) 수준을 추가한다. 세 번째로, 정보의 민감도 요인이 적용된 새로운 프로파일 권한으로 현행 직무그룹단위의 접근 권한을 세분화하여 모든 사용자에 재부여한다. 마지막으로, 각 사에서 정의한 위험도 허용정도의 기준수준보다 높은 수준의 데이터 파일 접근 권한을 가진 사용자에 대해 직무를 재조정한다. 이 중, 가장 중요한 것은 RACF 정책을 반영한 프로파일에 보안적, 재무적, 비즈니스적 민감도를 반영한 새로운 프로파일 수준(new profile level)을 정의하여 적용하는 것이다.

Fig.11.는 특정 직무그룹에 대해 정보의 민감도를 반영해 세분화한 새로운 데이터 파일의 접근 권한 프로파일의 예를 보여준다.

예를 들어, 현재의 'XAA.LOAN.**' 으로 지정한 프로파일에 대한 접근 권한이 여신직무그룹에 대한

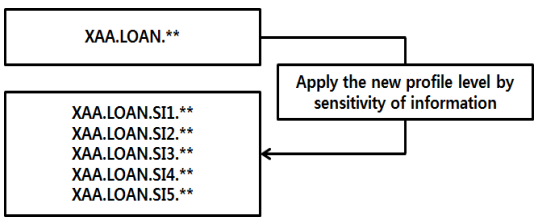

Fig.11. Apply the new profile level to current RACF policy by sensitivity of information

전체 데이터 파일에 대한 접근 권한을 의미한다면, 각 데이터 파일의 보안적, 재무적, 비즈니스적 민감도에 따라 산출된 정보의 민감도 수치를 반영한 새로운 프로파일 정책인 SI1~SI5를 정보의 민감도 등급으로 정의함으로써, 'XAA.LOAN.**'의 접근 권한 부여 정책을 'XAA.LOAN.SI1.**'와 같이 세분화하여 부여한다.

현재의 직무에 대해 새로운 프로파일을 적용한 각 사용자의 데이터 파일 정보 접근 권한에 대한 해당 파일의 민감도 수준의 합은 해당 사용자의 위험도 수준과 비례하며, 이 때 해당 수치가 해당 회사가 정의한 위험도 허용기준보다 높다면 해당 사용자에 대해 비즈니스 연속성을 침해하지 않는 범위내에서 직무를 재조정한다.

4.2 데이터베이스 접근 통제 정책에 적용

데이터베이스 접근 권한 정책에 적용하는 절차는 데이터 파일 접근 권한 정책에 적용하는 절차와 유사하다. Fig.12.은 현재의 데이터베이스 접근 권한 정책에 정보의 민감도를 반영하여 위험을 최소화하는 절차를 나타낸 것이다. 데이터 파일 접근 권한 정책의 적용은 앞서 RBAC기반의 RACF 정책을 적용하는 사례에서 비즈니스 연속성의 침해가 없어 기존 직무기준의 권한 부여 정책을 무시하고 모든 직무에 대해 처음부터 다시 모든 사용자의 직무를 재편성하는 경우와 모든 직무를 재편성하는 것이 해당 회사의 비즈니스 연속성을 침해하여 기존 직무그룹을 유지하면서 직무그룹내의 세부직무 수준에서 재편성하는 경우의 두 경우 모두 정보의 민감도 수준에 따른 새로운 프로파일 레벨 적용을 통해 위험도를 최소화하는 적용절차가 동일하다. 이에 반해, 데이터베이스 접근 권한 정책에 적용시 전자의 경우는 Fig.5.의 직무그룹에 일괄 적용된 RBAC 기반의 DB 테이블 권한을 무시하고, 사용자에 DB 테이블의 권한을 직접 부여하는 기술적 보안을 적용하며, 후자의 경우는 Fig.5.의 직무그룹에 일괄 적용된 RBAC 기반의 DB 테이블 권한을 유지하면서 직무그룹 하위레벨의 세부직무를 재편성하는 관리적 보안정책을 통해 모든 사용자에 대한 DB 테이블 접근권한의 정보의 민감도의 합이 최소가 되게 함으로써 최소한의 위험수준에 수렴하도록 한다. 후자의 경우와 같이 현재의 직무그룹을 유지하면서 세부직무를 재편성하는 관리적 보안이 필요한 이유는 데이터 파일 접근 권한의 경우 논리적 파일 명명규칙(naming-rule)의 변경을 통해 두 경우 모두 통제가 가능하지만, 데이터베이스의 경우 논리적 명명기준인 테이블명 자체에 해당 테이블의 정보의 민감도 수준을 반영하는 것이 쉽지 않으며, 설령 반영할 수 있다고 하여도 DBMS의 속성상 테이블명만으로 정보의 민감도 기준에 따른 접근 통제를 기술적으로 구분하여 통제할 수 없기 때문이다.

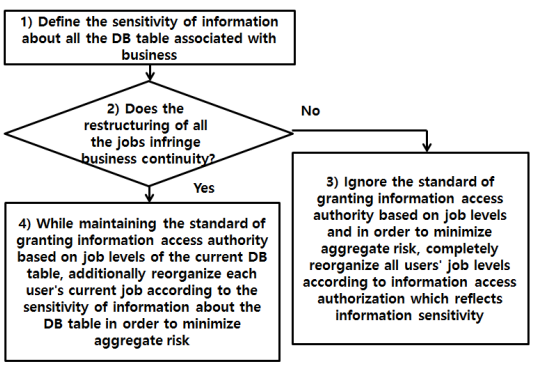

Fig. 12. Process of applying new policy reflected sensitivity of information to current database access control policy

Fig.13.~Fig.15.은 A금융사의 특정사용자ID를 선택하여, RBAC 기반으로 직무그룹에 부여된 Fig.5.의 권한을 RACF 정책을 통해 사용자에 부여하던 방식에서 정보의 민감도에 따라 직무를 일괄 재편성한 후, 재편성한 직무에 대한 DB 테이블의 접근 권한을 DBMS 레벨에서 직접 부여하는 기술적 보안을 테스트 적용한 사례이다. 적용 과정 및 결과는 다음과 같다.

- 먼저 Fig.13.과 같이 테스트 대상 테이블인 'TxxxxxxAF' 등 4개 테이블에 대해 RBAC 기반의 직무그룹에 부여된 접근 권한이 아닌 다른 방식의 권한 부여가 있는지 확인 절차를 수행하였으며, 직무그룹에 부여된 접근 권한 외에는 없음을 확인하였다.
- 다음 절차로 특정사용자ID 'T12345'를 선택하여 RACF 정책 레벨에서 해당 사용자ID에 부여되어 있던 테스트 대상 4개 테이블의 접근권한을 포함한 직무그룹인 'XAA'의 접근권한을 REVOKE 하였다.
- Fig.14.와 같이 테스트 대상 4개 테이블에 접근할 수 있는 직무그룹권한 'XAA'가 REVOKE된 사용자ID 'T12345'에 수행직무에 반드시 필요한 대상 테이블로 설정한 4개의 테이블에 대한 접근

권한을 DB관리자가 'GRANT' 문을 수행하여 직접 부여하였다.

- Fig.15.은 사용자ID 'T12345'의 DB 테이블 접근 권한으로 테스트 대상 4개 테이블 중 1개를 QUERY한 결과이며, 정상 수행됨을 확인하였다.
- 본 테스트 적용 수행 결과로, RACF 정책레벨에서 사용자에 RBAC 기반의 직무그룹에 부여되어 있던 DB 테이블의 권한을 삭제하여도 해당 사용자가 DB 테이블에 접근하여 직무를 수행하는데 문제가 없음을 확인하였다. 또한, 사용자ID 'T12345'가 직무를 수행하는 데 반드시 필요한 DB 테이블로 접근 권한을 제어함으로써, 기존 직무그룹권한인 'XAA'에 부여되어 있던 DB 테이블의 접근 권한이 많을수록 위험도의 감소효과는 커짐을 알 수 있다. 그러나, DBMS 레벨에서는 'XAA'로만 일괄 통제되던 관련 직무의 DB 테이블에 대한 접근 권한 정보가 각 사용자별로 부여됨으로써, 관리되어야 할 접근 권한 정보의 수가 크게 증가하였다.

```
SELECT COUNT(*) AS "Not Role Base 접근권한건수"
  FROM SYSIBM.SYSTABAUTH
 WHERE SELECTAUTH = 'Y'
   AND GRANTOR = 'XXXDBA'
   AND (GRANTEE NOT LIKE 'X%'
   AND  GRANTEE NOT LIKE 'YD%'
   AND  GRANTEE NOT LIKE 'ZM%')
   AND TTNAME IN('TXXXXXXAF',
                 'TXXXXXXBH',
                 'TXXXXXXCA',
                 'TXXXXXXCL')
 WITH UR;
```

Result ALL | Result(1)

	Not Role Base 접근권한건
1	0

Fig.13. Confirmation of whether there is access authorization not based on RBAC

```
SELECT GRANTOR, GRANTEE, TTNAME,
       SELECTAUTH, INSERTAUTH, UPDATEAUTH,
       DELETEAUTH, ALTERAUTH
  FROM SYSIBM.SYSTABAUTH
 WHERE SELECTAUTH = 'Y'
   AND GRANTOR = 'XXXDBA'
   AND (GRANTEE NOT LIKE 'X%'
   AND  GRANTEE NOT LIKE 'YD%'
   AND  GRANTEE NOT LIKE 'ZM%')
   AND TTNAME IN('TXXXXXXAF',
                 'TXXXXXXBH',
                 'TXXXXXXCA',
                 'TXXXXXXCL')
 WITH UR;
```

UOW Scope : All SQL Delimiter : Fetch first ALL row(s) only

Result ALL | Result(1)

	GRANTOR	GRANTEE	TTNAME	SELECTAUTH	INSERTAUTH	UPDATEAUTH	DELETEAUTH	ALTERAUTH
1	XXXDBA	T12345	TXXXXXXAF	Y				
2	XXXDBA	T12345	TXXXXXXBH	Y				
3	XXXDBA	T12345	TXXXXXXCA	Y				
4	XXXDBA	T12345	TXXXXXXCL	Y				

Fig.14. Result of searching for information access authority after executing DDL statement GRANT' which directly grant access authority for the DB table

```
SELECT COUNT(*) AS "테이블건수"
  FROM XXXDBA.TXXXXXXAF
 WITH UR;
```

UOW Scope : All SQL Delimiter

Result ALL | Result(1)

	테이블건수
1	12732326

Fig.15. Result of executing a query to check whether DB table access is performed normally through access authority

4.3 실효성 및 문제점 도출

3.5에서와 같이, 정보 접근 통제 정책에 따른 금융IT인력의 위험도는 다른 독립변수가 동일하다고 가정하면, 정보의 민감도에 따른 정보 접근 통제의 적용수준이 높을수록 위험이 낮아진다. 이것은 현재 대부분의 금융회사들이 채택하고 있는 RBAC 기반의 정보 접근 통제 방식에 데이터 파일 또는 DB 테이블에 대한 정보의 민감도를 정의하고, 이를 반영하여 적용하지 않기 때문에 비즈니스의 연속성을 감안하여 실무적으로 보안사고의 위험도를 낮출 수 있다는 점에서 본 논문에서 제시한 적용방안의 실효성이 높다고 할 수 있다. 그러나, 정보 접근 권한 통제의 관리 편의성이 높은 기존의 RBAC 접근 통제 방식에 비해 권한 정보의 관리대상이 크게 증가하게 되므로, 정보 접근 권한을 통제하는 관리자의 업무량이 이에 비례하여 증가하게 된다. 따라서, 정보의 민감도를 반영한 정보 접근 통제 정책을 적용함과 동시에, 권한 정보에 대한 관리의 효율성을 높일 수 있는 방법이 필요하다. 4.4에서는 이러한 보안 사고의 위험도를 크게 낮추는 독립변수인 정보의 민감도를 반영한 데이터 접근 권한 통제정책에 따라 불가피하게 발생하는 관리 대상 접근 권한 정보의 급증에도, 접근 권한 정보처리자의 실질적 업무량의 증가를 차단함으로써 추가 인력 투입없이 유지보수 할 수 있는 방안을 제시하고, 이를 A금융사의 데이터베이스 접근 권한 처리 프로세스에 구현 및 적용하여 실증한다.

4.4 접근권한 정보 증가에 따른 효율적 관리방안

4.1.1. 문제점 분석 및 해결 방안 제시

정보의 민감도를 반영한 데이터 접근 통제 정책 적용에 따라 발생하는 관리대상 접근권한 정보의 증

가는 비용관점에서 다음과 같은 문제의 해결이 필요하다.

첫 번째, 관리대상 접근권한 정보 증가에 따른 스토리지 용량 확보가 필요하다. Fig.4.에서와 같이, 테스트를 진행했던 A금융사의 RBAC 기반 데이터베이스 접근 권한 정보의 수는 26,654건이었으며, 이에 대해 직무기준을 무시하고 모든 사용자 ID에 대해 테이블 기준으로 모든 권한을 부여하는 경우를 시뮬레이션 해본 결과, 관리대상 접근 권한 정보 건수는 최대 1,152,355건으로 확인되었다. 이는 A금융사의 경우, RBAC 기반의 직무그룹당 평균 43.2개 수준의 테이블에 대한 'CRUD'[4] 접근 권한 정보가 부여되어 있음을 의미하며, 이에 따라 기존 RBAC 기반 데이터베이스 접근 권한 정보 저장용량에 비해 약 43.2배 수준의 스토리지가 필요함을 의미한다. 따라서, 이러한 데이터베이스 접근 권한 정보의 증가에 따른 필요 용량을 Table.17과 같이 산출해보았다. Table 17.에서 'Length'는 테스트를 진행했던 A금융사 DBMS인 DB2의 테이블에 대한 접근권한 정보 테이블인 'SYSIBM.SYSTABAUTH'[5]의 접근권한 정보 건당 로우(row)의 길이를 의미한다. A금융사가 현재의 RBAC 기반의 접근권한 정책을 모든 사용자ID에 테이블 단위로 부여하는 경우, 접근 권한 정보의 증가에 따른 스토리지의 필요용량은 최대 약 1.31GB이다. 'SYSIBM.SYSTABAUTH' 테이블의 경우 로우(row)의 길이인 1,225 바이트(byte) 중 1,176 바이트의 데이터 타입(type)이 가변적인 'varchar' 로 구성되어 있어, 실제 물리적으로는 1.31GB보다 훨씬 적은 양의 용량이 필요하게 되며, 정보의 민감도에 따라 각 사용자ID에 테이블 접근권한을 선별하여 적용하는 경우 추가 필요 용량은 더 감소하게 된다.

Table 17.에서 산출한 필요 용량인 1.31GB는 가장 보수적으로 산출된 수치로, 세계시장에서 스토리지 부문의 수위 수준 시장점유율을 가진 B사의 하이엔드급 스토리지의 List Price가 TB당 1억원 초반 수준임을 감안할 때, 스토리지 추가 비용은 매우 미미한 수준이다. A금융사가 국내 수위 용량 수준의 z/OS 기반 메인프레임을 운영하는 고객사임을 감안할 때, 정보의 민감도를 반영하여 데이터베이스 접근권한 정책을 일괄 재편성하여도, 스토리지 추가 비용은 고려하지 않아도 될 것이라 판단된다.

Table 17. Calculation of the necessary quantity due to increase in a number of DB authorities-related information to be managed

Criteria	Count	Length	Quantity
Current	26,654	1,225	about 31MB
Adjusted policy	1,152,355	1,225	about 1,31GB

두 번째, 관리대상 접근 권한 정보 증가에 따른 접근 권한 정보관리자의 추가 투입이 필요하다. 이는 비즈니스 어플리케이션 개발자들에 대한 테이블 권한 관리의 업무량이 접근 권한 정보의 증가량에 비례하여 폭증함을 의미하며, 전담인력의 투입이 필요한 수준이다. A금융사의 경우, Table 17.에서와 같이 기존의 RBAC 기반의 접근 권한 부여 정책을 사용자ID에 테이블 단위의 접근 권한 부여 정책으로 일괄 변경하는 경우, 일일 정규 근무시간 8시간을 기준으로 업무처리 가용수준을 감안할 때, 접근 권한 처리 업무에만 약 3.3명 이상의 추가 인력이 투입되어야 하는 것으로 확인되었다. 이는 2013년 제1금융권 연평균급여 7,538만원을 적용하면, 약 2.49억원의 인력 투입 비용이 발생함을 의미한다[16]. 따라서, 이러한 추가 인력 투입 문제에 대한 해결방안이 필요하며, Fig.16.과 같은 프로세스를 제시한다.

Fig.16.은 비즈니스 어플리케이션 개발자들이 테이블 생성 또는 기생성된 테이블에 대한 'CRUD' 권한 부여를 요청하는 경우, 이에 대한 GRANT, REVOKE 등의 접근 권한 부여에 필요한 DDL(Data Definition Language) 구문을 자동 생성하도록 구현함으로써, 접근 권한 정보처리자의 워크로드(workload)를 최소화하는 방안이다. 따라서, 접근 권한 정보처리자가 스크립트(script) 등의 정형화된 형식에 테이블명, 사용자ID, 'CRUD' 요청 접근권한 정보 항목을 입력하게 함으로써, 처리 프로세스를 단순화하고, 이 정보를 단순 입력후 해당 스크립트를 실행하면 추가 인력 투입을 발생시키는 단계인 DDL 구문 생성 및 구문의 실행을 자동으로 처리한다. 이는 워크로드가 집중되는 단계를 자동화 처리하여 관리대상 접근 권한 정보 처리 인력의 추가

4) 생성(Create), 읽기(Read), 갱신(Update), 삭제(Delete)의 데이터 처리 기능을 일컫는 용어

5) DB2 DBMS에서 사용자 테이블 또는 뷰(view)에 대한 접근 권한 정보를 관리하는 테이블

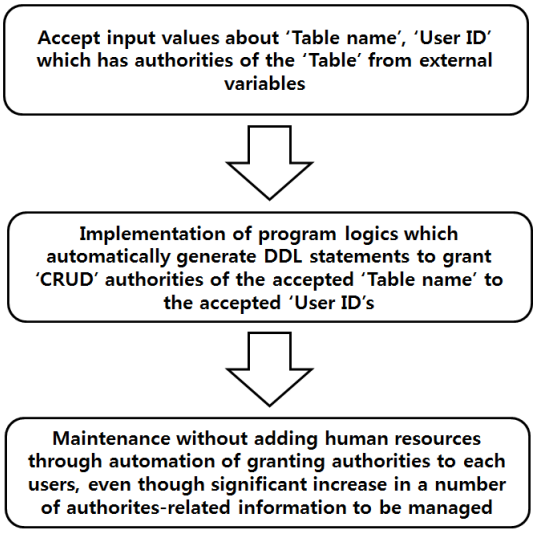

Fig.16. Process for maintenance of new policy reflected sensitivity of information to current database access control policy without adding human resources

투입을 없애고, 전체 프로세스를 정형화함으로써 권한 관리 처리의 수기수행에 따른 운영리스크를 제거한다.

4.1.2. 자동화 프로세스 구현 및 실증

Fig.16.에서 제시한 접근 권한 처리 프로세스의 자동화를 구현하기 위해 IBM의 REXX (REstructured eXtended eXecutor)[6] 언어를 이용해 정보의 민감도를 반영한 테이블 단위의 권한 부여 정책을 접근 권한 처리 프로세스에 자동 처리되도록 DDL 구문을 생성 및 실행하는 프로그램을 구현하였다. Fig.17.은 비즈니스 어플리케이션과 관련된 테이블 생성시에 테이블 생성, 접근 권한 부여, 구문 실행 로직을 반영한 전체 소스코드 중 DDL 구문 생성 로직을 처리하는 일부을 보여준다.

본 소스 부분은 접근 권한 정보처리자가 외부 변수(external variables)로 테이블명, 사용자ID, 'CRUD' 요청 접근권한 정보 항목을 입력하는 경우, 'do while' 구문을 이용하여 입력된 접근 권한 부여 요청 개수에 상관없이 DDL 구문을 생성하도록 구현되었다. 'CRUD' 요청 접근권한 정보 항목은 입력된 테이블에 대해 SELECT, INSERT, UPDATE, DELETE 권한 중 어떤 접근 권한 부여를 요청하는지에 대한 구분을 의미하며, 이 구분에 따라 입력된 사용자ID에 해당 테이블의 권한을 부여하게 된다.

Fig.17.의 153번 라인의 소스코드는 이러한 기준에 따라, DDL 구문을 생성하는 부분 중 'SELECT' 권한 생성 부분을 보여주고 있으며, 각 사용자ID에 대해 입력된 테이블의 'CRUD' 권한에 대한 DDL 구문을 각각 생성한 후, 내부 중복제거 로직처리를 통해 사용자ID, 테이블명 기준으로 병합(merge)함으로써, 특정 테이블에 대한 특정사용자ID의 접근 권한 부여가 하나의 DDL 구문으로 생성되도록 로직을 구현하였다. Fig.18.은 Fig.17.의 소스코드를 적용하여 접근 권한 정보처리자가 비즈니스 어플리케이션 관련 테이블, 사용자ID, 'CRUD' 요청 접근권한 정보 항목을 개수에 관계없이 입력하도록 하여 테이블 생성을 처리하면서, 해당 권한이 해당 사용자ID에 부여하는 DDL 구문을 자동 생성하고 실행되도록 JCL(Job Control Language)[7]를 생성한 것이다.

A금융사는 테이블 정보 및 테이블 권한 요청 정보가 메타데이터 시스템을 통해 관리가 되기 때문에,

Fig.17. Applied source-code of algorithm to automatically generate DDL statements to grant 'CRUD' authorities of the accecpted 'Table name' to the accepted 'User ID' from external variables

6) IBM이 제공하는 많은 컴퓨터 운영체제를 지원하는 구조화 프로그래밍 언어로 상용 버전과 오픈 소스 인터프리터가 모두 존재함[17].

7) IBM 메인프레임 운영 체제에서 배치 작업을 실행 또는 서브 시스템을 시작하는 방법에 대해 시스템에 지시하기 위해 사용되는 스크립트 언어의 이름[18]

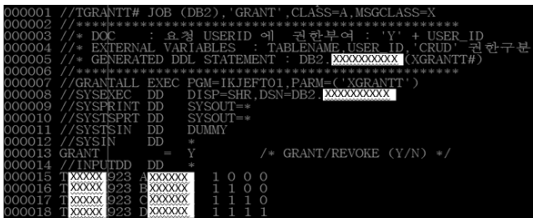

Fig.18. JCL script for automatically generation and execution of DDL statements when administrator create tables associated with business applications

본 JCL을 생성하는 프로그램 소스도 별도 구현하여 메타데이터(metadata)[8] 정보를 활용하여 입력 변수를 자동으로 생성하도록 하였으며, 입력 변수인 비즈니스 어플리케이션 테이블에 대한 컬럼, 용량 등의 속성정보 등은 Fig.17.의 소스에 기 저장되어 있는 메타데이터 정보를 활용해 테이블 생성 구문을 처리하도록 구현되어 있다.

따라서, A금융사는 테이블의 생성, 접근 권한 부여와 관련된 전 프로세스가 자동화 처리가 가능하지만, 이를 적용 검토하는 회사는 메타데이터 시스템의 구성 수준에 따라 자동화 범위를 정할 수 있고, 메타데이터 시스템이 구성되어 있지 않더라도 접근 권한 정보처리자는 정형화된 JCL 스크립트만을 관리하여 외부 변수만을 수기로 입력함으로써 DDL 생성, 실행 등의 워크로드가 집중된 단계를 자동으로 처리할 수 있으며, DDL 구문의 수기처리에 따른 운영리스크를 제거할 수 있다.

Fig.19.는 Fig.18.의 JCL 스크립트를 수행하여 테이블 생성 및 해당 테이블에 대해 입력된 사용자 ID에 접근 권한을 부여하는 DDL 구문이 생성된 화면이다. 접근 권한 정보처리자의 워크로드는 비즈니스 어플리케이션 담당자가 요청한 내용을 분석하여 이 DDL구문을 생성하는 단계에 집중되며, 수기분석 및 생성에 따른 운영리스크도 발생하기 때문에, 이러한 부분을 본 논문에서 실증한 것처럼 자동화 처리하면, 기존 RBAC 기반의 접근 권한 부여 정책에 정보의 민감도를 반영하여 발생되는 관리해야 할 접근 권한 정보의 증가수준에 관계없이 해당 단계의 워크로드 증가를 없앨 수 있어, 추가 인력의 투입없이 정보의 민감도를 반영한 접근 권한 처리 프로세스의 운

8) 어플리케이션 데이터 또는 데이터 컨텐츠의 개별 인스턴스에 대한 내용을 저장한 '데이터에 대한 데이터'를 의미함[19].

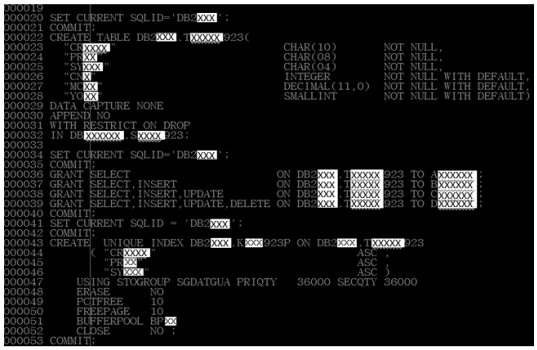

Fig.19. Automatically generated DDL statements to create tables and to grant 'CRUD' authorities after execution of JCL script

영이 가능하다.

V. 결론 및 향후 과제

보안사고는 현재까지 연구되어 온 다양한 방식의 인력보안 기준과 정보 접근 통제 정책을 선의의 노력을 다해 적용함에도 불구하고 지속적으로 증가하고 있다. 따라서, 본 논문에서는 보안사고의 핵심인 정보 접근 통제에 대하여 직무상 대량의 금융 관련 개인정보에 접근하는 금융IT인력의 위험도를 측정하기 위한 의미있는 영향 요인들을 설문을 통해 분석하여 정보의 민감도가 매우 중요하다는 것을 도출할 수 있었다. 또한, 2013년 한 보도에 따르면 포춘 500대 기업중 71%는 z/OS 기반의 메인프레임을 사용하고, 미국 25개 소매점중 23개사, 전세계 10대 보험사 중 9개사가 메인프레임을 사용하고 있어, 국내 수위 수준의 메인프레임 용량을 운영하는 A금융사의 데이터 파일 및 데이터베이스에 대한 접근 통제 방식을 분석한 후, 정보의 민감도 요인을 기존의 정책에 반영하는 안을 제시하고 실증함으로써 대용량 데이터를 다루는 많은 회사에서 채택하는 메인프레임 환경에서 논문에서 제시하는 권한 관리 정책의 적용가능성을 검증하였고, 관리해야 할 접근 권한 정보의 급증에 따른 워크로드 급증 문제를 해결하는 프로세스를 제시하고 실증함으로써 프로세스의 경제성 및 효율성을 확보하였다[20].

많은 기업들은 관리의 편의성 및 효율성이 높은 RBAC 방식의 정보 접근 통제 방식을 통해 충실한 정보 보안의 노력을 하고 있으나, 정보의 민감도를 반영한 정보 접근 통제에 대해서는 간과하여 왔다.

그러므로, 기존의 RBAC 방식에 본 논문에서 제시한 정보의 민감도를 반영하여 다음과 같이 정보 접근 통제를 개선, 적용할 것을 제안한다.

첫째, 비지니스 연속성 등을 위해 현행 직무 기준의 정보 접근 통제 방식을 유지해야 하는 경우, 비지니스의 연속성을 유지하는 범위내에서 정보의 민감도를 반영하여 최소한의 인력위험도에 수렴하도록 세부 직무를 재편성해야 한다.

둘째, 비지니스 연속성 유지 등에 문제가 없어 직무 기준의 정보 접근 통제 방식을 정보의 민감도로 직무 재편성이 가능한 경우, 직무를 정보의 민감도 기준으로 재편성해야 한다.

본 논문에서는 인력보안의 중요요소인 정보 접근 통제에 대한 IT인력 위험도 영향 요인을 도출하는 연구를 수행하였으나, 정보의 민감도를 기준으로 현행 직무 기준의 정보 접근 통제 정책을 일괄 변경하는 경우 비지니스의 연속성을 침해할 수 있다. 따라서, 비지니스의 연속성을 침해하지 않고 정보 접근 통제 정책에 정보의 민감도를 최대한 반영할 수 있는 기술적, 관리적 방안이 지속적으로 연구되어 기업에 적용됨으로써 비지니스 유지의 중요한 인적자원인 IT인력에 따른 보안사고의 위험을 최소화해 나가야 한다. 또한, 본 논문에서 정보의 민감도를 반영한 정보 접근 통제정책의 적용사례로 제시한 메인프레임 운영환경 외의 다른 운영환경 또는 프레임워크를 채택하고 있는 시스템에서도 해당 환경에 맞게 커스터마이징하여 확대 적용하는 것이 필요하다.

References

〔1〕 Ki-wan Ko, "www.hankyung.com/news/app/newsview.php?aid=2014012750251"

〔2〕 Jong-in Lim, "Law and Technology in the Cyber Space," 2002

〔3〕 In-hwan Cha, "An Empirical Research on Developing Personnel Security Management Indicators in Information Security," Kwangwoon University, 2009

〔4〕 Chang-Lai Choi, "Study on IT Outsourcing Policy Based on Operational Risks of Financial Industries," Korea Institute of Information Security & Cryptology, Aug. 2014

〔5〕 Myoung-sup Sim, "An Empirical Study on the Improvement of Security Levels in IT Outsourcing Service," Konkuk University, 2013

〔6〕 Mikko et al. "A Critical Assessment of IS Security between 1990~2004," 2005

〔7〕 Jinho Yoo at el, "Estimating Economic Damages from Internet Incidents," 2008, Information Society, vol.15, no.1

〔8〕 ANSI/INCITS 359-2004, "Information Technology-Role Based Access Control, International committee for Information Technoloty Standards," 2004

〔9〕 Seong-min Jung, "Application Method of Efficient Role Extraction and Safe Role-based Access Control for Developing Financial Application," Journal of Information Security, Vol. 18, No. 5, Oct. 2008

〔10〕 John Barkley, "Computing simple role based access control models and access control lists," Proceeding of 2nd workshop on Role-based access control, august, 1997, pp127-132

〔11〕 Ravi S. Sandhu, Edward J. Coyne, "Role-based access control models," IEEE Computer, February 1996, pp3-47

〔12〕 Ferraiolo D. F.,"Proposed NIST Standard for Role-Based Access Control," ACM Transactions on Information and System Security, Vol.4, No.3, August 2001

〔13〕 NIST, "American National Standard for Information Technoloty - Role Based Access Control (Draft 4/4/2003)," American National Standards Institute Inc. 2003

〔14〕 Sylvia O., "Database Applications of Role-Based Access Control," The University of Western Ontario, Nov. 2001

〔15〕 Difinition of RACF, "http://en.wikipedia.org/wiki/Resource_Access_Control_Facility"

〔16〕 The average salary of bank employees in 2013, http://www.hankyung.com/news/app/newsview.php?aid=2014033147361

〔17〕 Definition of REXX, http://ko.wikipedia.org/wiki/REXX
〔18〕 Definition of JCL, http://en.wikipedia.org/wiki/Job_Control_Language
〔19〕 Definition of Metadata, http://en.wikipedia.org/wiki/Metadata
〔20〕 Jeong-hwan Kim, "A Study on SQL Performance-Based IT Application Change Management Process to Prevent Failures of Online Transactions," Korea Institute of Information Security & Cryptology, Oct. 2014

〈저 자 소 개〉

심 재 윤 (Jae-yoon Sim) 정회원
2000년 2월: 아주대학교 정보 및 컴퓨터공학부 학사
2013년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 인력보안, 금융정보보안, 위험관리

이 경 호 (Kyung-Ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사
2009년 8월: 고려대학교 정보보호대학원 박사
1994년 2월~현재: 삼성그룹, nhn, 시큐베이스 등 근무
2011년 9월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 위험관리, 정보보호컨설팅, 정보보호 및 개인정보보호정책