Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.1, Feb. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.1.225

시스템 접근관리에 대한 의사결정 프로세스 연구

조 영 석,† 임 종 인, 이 경 호‡
고려대학교

A Study on Decision Making Process of System Access Management

Young-seok Cho,† Jong-in Im, Kyung-ho Lee‡
Korea University

요 약

최근 정보보호인증 및 보안감사의 감독과 절차가 강화되고 있지만 내부자에 의한 정보유출 및 보안사고는 지속적으로 늘어나고 있다. 2011 Cyber Security Watch Survey에 의하면 2010년 한 해 동안 발생한 보안사고 중 21%가 내부자에 의해 발생한 것으로 조사되었다. 기업들은 대외서비스와 달리 내부시스템 보안사고의 경우 즉각적으로 인지하지 못하거나 발생 시 비용증가, 신용도하락 등의 이유로 외부에 공시하지 않고 일시적 미봉책으로 해결하는 경우가 많았다. 본 논문은 시스템 접근관리에 대한 문제점을 실증적으로 연구하였으며, 타 시스템 또는 사업장에서 활용이 가능한 표준 프로세스를 제시하였다. 이를 통해 기업들이 쉽고 체계적으로 시스템 접근관리에 대한 문제점을 조사하고 분석하며 개선하는데 도움을 줄 것이다.

ABSTRACT

Recently, the administration and supervision of Information Security Certification and Security Inspection has been enforced but information leakage and security accidents by insiders are increasing consistently. The security accidents by insiders ran to 21% in 2010, by the 2011 Cyber Security Watch Survey. The problem is that immediate recognition is difficult and stopgap measure is mostly adopted without company's external notice apprehensive for cost increase or credit drop in case of internal security accidents. In the paper, we conducted the regression study on security access management then proposed the standard process available for other systems and businesses sites. It can be very useful for many companies to investigate, analyze and improve the problem of security management conveniently.

Keywords: Security Management, Regression Study

I. 서 론

최근 2011 Cyber Security Watch Survey [1]에 의하면 2010년 한 해 동안 발생한 보안사고 중 21%가 내부자에 의해 발생한 것이라고 밝혔다. 오늘날 내부자의 침입 행위는 네트워크 및 기반시설 보안에 가장 심각한 위협으로 부각되고 있다.

이에 따르면, 조직의 정보나 데이터 유출은 외부자 침입에 의한 것보다 내부자의 침입에 의해서 발생하는 경우가 많았다. 내부자 사고의 유형은 인증되지 않은 접속에 의한 기업정보 손상이 63%로 가장 높았으며, 고의적이지 않은 기업정보 유출이 57%로 그 다음 비율을 차지하고 있었다. 두 유형 모두 접근권한, 계정관리, 정보관리에 관련된 것으로 내부자의 행위를 관리하는 것과 연관된 것이다[2].

지금까지 내부자에 대한 침입 차단 및 탐지 기법 중

접수일(2014년 12월 10일), 수정일(1차: 2015년 1월 19일, 2차: 2015년 2월 10일), 게재확정일(2015년 2월 13일)
† 주저자, yseokcho@korea.ac.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

에 접근제어 모델이 가장 많이 사용되고 있다. 접근제어란 식별 및 인증을 통해 시스템 혹은 정보에 대한 접근이 허용된 사용자가 허가된 범위 내에서만 가능하도록 하는 기술적인 방법이다. 하지만, 접근제어가 실제 업무현장에서 완벽하게 이를 차단하지 못하는 경우가 존재하며 문제를 야기하는 경우도 발생한다.

본 논문은 시스템 접근관리에 대한 실증연구를 통해 문제점 들을 분석해 보고 효과적인 대안을 제시해 본다.

II. 관련연구

접근제어 모델은 크게 MAC(Mandatory Access Control)과 DAC(Discretionary Access Control) 그리고 RBAC(Role-based Access Control)으로 구분할 수 있다[10].

DAC 모델은 사용자 계정에 기반하여 자원에 접근을 허용하는 자율적인 특징을 가지고 있다. 이는 현재 자원에 대한 소유권을 가지고 있는 사용자 혹은 그룹이 다른 사용자나 다른 그룹에 관한 권한을 임의적으로 할당할 수 있는 임의적 접근제어 시스템이다[Fig. 1].

이는 ACL(Access Control List)에 정의된 정책의 수정을 통하여 사용자가 자원에 대한 권한을 부여하거나 받을 수 있다. 따라서, 객체에 대한 접근 및 사용이 용이하며 접근변화의 반환시간이 감소하는 장점이 있다. 하지만, 전적으로 사용자 주체의 신분에 근거하기 때문에 해킹이나 트로이목마와 같은 공격에 의해 신분이 노출된다면 보안에 매우 취약하며 객체를 소유한 개인 및 그룹의 임의적 할당으로 인하여 몇 명의 개인이 동일한 자료에 소유권을 가지게 될 지 모르는 위험성이 존재한다. 또한, 데이터를 소유한 사용자 혹은 그룹의 유동성으로 인해 자원에 대한 접근 역시 유동적으로 변화된다. 사용자 혹은 그룹 및 ID 기반 접근통제 모델이기 때문에 사용자 계정의 ID와 PW 정보 가로채기 등으로 인하여 인증을 수행하고 인가를 쉽게 얻어낼 수 있으며, 사용자 신분에 따라 임의적으로 자원의 할당이 이루어지기 때문에 수없이 많은 다수의 사용자가 발생될 수 있다. 이러한 경우 사용자에 의해서 이루어진 자원의 변동 발생에 대한 추적의 어려움과 보안상의 문제를 가지게 된다.

RBAC 모델은 사용자에게 할당된 역할에 기반하여 자원에 대한 접근이 이루어지며, 관리자는 사용자에게 특정한 권리와 권한이 정의된 역할을 할당한다. 이 때, 사용자들에게 할당된 역할과 사용자들의 연관성을 통하여 자원에 접근할 수 있고, 특정한 자원을 수행할 수 있다. RBAC은 사용자(User), 역할(Role), 권한(Permission)으로 구성되어 사전 정의된 역할이 할당되어지고 이때 접근제어 정책이 제약조건(Constraints)으로써 각 세션들마다 적용되어진다[Fig. 2]. 이러한 방식은 권한관리를 매우 단순화시켜주고 특정한 보안정책을 구현하는데 유연성을 제공하는 장점이 있다.

그러나, 조직 내의 권한과 책임을 나타내기 위하여 역할계층이 존재하고 있으며, 각 계층들 간의 상속성이 존재한다. 이로 인해 권한상속 및 위임 과정에서 발생할 수 있는 역할의 위임 오류 혹은 적절하지 않은 역할로의 접근이 발생될 수 있다. 또한, 어떠한 검증도 없이 일련의 역할이 충족되면 자원의 접근이 쉽게 가능하기 때문에 사용자와 역할, 권한이 어떻게 상호적으로 할당되었는지 파악이 필요하다[14].

많은 시스템들이 접근제어를 위해 RBAC 모델을 사용하고 있으며 계정관리 시스템과 연동하여 사용자의 접근을 통제하고 있다. 접근통제에는 정책, 인증, 권한, 네트워크 등 다양한 요소들이 존재한다. 이 중 계정관리(ID Management)는 접근통제(Access Control)의 주요한 요소이며, 계정의 생성, 발급, 이용, 폐기의 Life Cycle 단계에서 문제가 발생한다면 접근통제 자체가 붕괴될 수 있는 위험성이 존재한다.

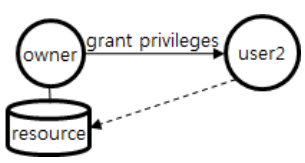


Fig. 1.resource authority grant of DAC model

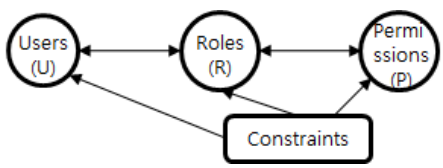


Fig. 2. configuration and interaction of RBAC model

III. 실증연구

3.1 시스템 선정

실증연구를 위한 대상서버를 선정한다. 기업 내부에는 그룹웨어, MIS, ERP, DataWarehouse, EIS(Executive Information System), NRCS(Newsroom Computer System) 등 업무의 목적과 종류에 따라 다양한 시스템 들이 존재하는데 이 중 직원들의 사용률이 가장 높으며 개인 및 민감한 기업정보를 보관하고 있는 ERP 시스템을 대상으로 한다.

ERP(Enterprise Resource Planning)는 전사적 자원관리 시스템이다. 기업에 존재하는 모든 리소스(경영자원)에 대해 최적의 활용방안을 제시하는 프로그램이라고 할 수 있다. 물류, 인사, 급여, 생산, 자재, 무역, 영업, 회계, 원가 시스템의 유기적인 집합체이며, 업무 패키지 또는 통합 기간업무시스템으로 알려져 있다.

ERP 시스템은 지금껏 기술 환경 변화에 민감하지 않았다. 이유로는 ERP가 회사 입장에서 직접 고객을 상대하는 Front Office 업무이기 보다는 내부 직원에 의해서만 사용되는 Back Office 업무이기 때문에 유행에 민감하지 않고 폐쇄적이었으며, ERP 제품이 IT적인 측면보다는 경영적인 측면이 더욱 강조되었기 때문이다[10].

최근 기업들이 업무효율성 증대를 목표로 ERP 시스템을 경쟁적으로 도입하면서 ERP 시스템의 보안관리 또한 중요해지고 있다. 매년 ISMS 인증심사 및 보안감사를 받고 있지만 실제 ERP시스템을 통한 정보유출 및 보안사고는 지속적으로 발생하는 것으로 조사되었다. 정작 망 분리 및 보안관리 규정 등은 모두 충족하지만 내부 보안관리는 취약하다고 할 수 있다. 타 시스템과 다르게 효율성만을 강조하다 보니 사전통제 보단 문제 발생 시 사후 적발로 인한 담당자 징계 및 법적 소송으로 해결하는 경우가 많았다. 조사결과, 실제 ERP시스템에 의한 정보유출은 대부분 직원들의 도용된 계정사용에 의해 근무시간 대에 회사 내부에서 발생하고 있었으며 업무현장에선 계정도용이 공공연하게 이루어지고 있는 경우도 있었다.

3.2 요인 탐색

요인 탐색을 위해 국내 지상파 방송사 중 한 곳의 연간 접속로그를 조사하여 도출된 요인들과의 연관성을 분석하였다.

국내 지상파 방송사 중 한 곳의 ERP 시스템은 인하우스 방식으로 개발되었으며, PowerBuiler 12.0 및 MSSQL 2008로 구성된 C/S 환경이다.

이 시스템은 EIISFB(예산), EIISFA(회계), EIISBF(편성), EIISBM(제작), EIISBU(사업), EIISBA(광고), EIISPA(인사), EIISMI(경영정보)의 8개 서브시스템으로 이루어져 있으며, 기업의 전체 직원 수는 961명이다.

요인 탐색을 위해 다음과 같이 4개의 요인을 선정한다. 첫 번째 요인으론 회사의 직급, 직무, 부서 등의 인사조직, 두 번째는 근속연수, 연령, 최종학력 등의 사회경력, 세 번째는 전공, 성별, 거주지, 혼인여부 등의 개인이력, 마지막으로, 접속하는 요일, 시간대, 장소 등의 사용 환경이다[Table 1].

Table 1. main causes of account management

Factor	Specific Factor	Remark
Personnel Organization (Factor1)	(1) Staff Level	President, Vice President, Auditor General, Department Manager Level, General Manager Level, Deputy General Manager Level, Assistant Manager Level, Chief Level, Staff Level, Dispatched Worker, Freelancer Worker
	(2) Job Position	President, Vice President, Auditor General, Chief of Division, Managing Director, Director General, Director, Executive Director, Section Chief, General Manager, Director of Special Affairs, Assistant Director, Deputy Director General, Deputy General Manager, Staff

	(3) Job Classification	Broadcasting Work, Technical Work, Managerial Work, Journalist Work
	(4) Division	38 Divisions of Head office
Society Career (Factor2)	(5) Service year	less than 1 year, 1~2 years, 2~5 years, 5~10 years, 10~20 years, more than 20 years
	(6) Age	over 50's, 40's, 30's, under 20's
	(7) Level of Education	Higher Graduate School Diploma, Univertisy Diploma, College Diploma, Less High School Diploma
Individual History (Factor3)	(8)Major	Electronic Engineering, Broadcasting Programs, Sociology, Filmologie, Journalism and Broadcasting, Physics, Etc
	(9)Sex	Man, Woman
	(10) Residence	Gangnam, Gangseo, Gangbuk, Gangdong, Gyeonggi, Etc
	(11) Marriage	Married, Single
Usage Environment (Factor4)	(12)Day of Week	Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday
	(13)Time Slot	Morning(08~13), Afternoon(13~18), Evening(18~24), Midnight(24~08)
	(14) Usage Place	From third basement level To first floor, Second floor of Head Office, Third floor of Head Office, Fourth floor of Head Office, Fifth floor of Head Office, Broadcasting Center, Hanbang Building, Damyeong Building, Yuil Building, Outside

3.3 요인 검정

연간 접속로그를 분석한 결과, 계정도용 비율이 전체 접속량의 4.2%에 해당하는 것으로 나타났다. 이는 계정관리에 심각한 문제점을 보여준다.

SECVIZ[3]를 이용한 Visualization 분석을 통해 요인들과의 연관도를 조사해 보니 프리랜서, 파견직 등의 외부직원이 부장급(계정)을 이용하여 제작시스템(EIISBM)에 많이 접속하는 것을 발견할 수 있었다[Fig. 4].

특징별로 살펴보면 첫째, 직급이 낮을수록 계정도용 빈도가 높은 것으로 나타났다. 직렬로는 방송직이 가장 많았으며 부서로는 유아·어린이부, 초·중·학창의인성부, 진로직업·청소년부, ENG영상부, 교육뉴스부 등의 프로그램 제작부서가 높게 나타났다.

둘째, 근속년수가 1년 미만 또는 1~2년에 해당하고 연령이 20대인 대졸자의 계정도용 비율이 높게 나타났다.

셋째, 방송학, 방송영상학, 사회학, 신문방송학, 영화학, 미디어영상학, 캐릭터애니메이션학, 멀티미디어 등 방송관련 학과 졸업생들 중 강남에 거주하는 미혼 남자에 의한 계정도용 비율이 높았다.

넷째, 접속 시간대 및 사용 장소별로 살펴보니 월요일 오후(13~18시) 본사 5층의 계정도용 비율이 높게 나타났다.

3.4 회귀 분석

로그분석을 통해 회사의 직급과 계정도용과의 연관성이 발견되어 회귀분석을 실시하였다.

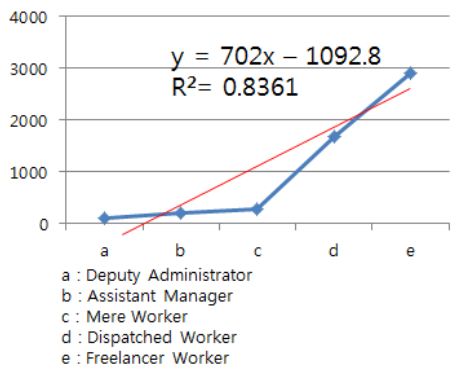
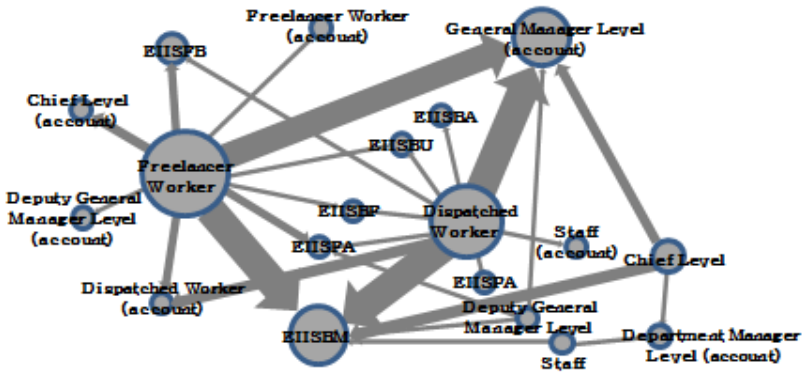


Fig. 3. relation between job position and account theft



node: factor direction: relation weight : frequency

Fig. 4. correlation between main factors

회귀분석은 요인들과 특정 변수 사이의 인과 관계를 분석하는 기법이다. 개별 요인이 회귀분석에서 의미를 가지기 위해서는 유의도가 0.05 이하가 되어야 한다.

회귀분석 결과, 계정도용에 영향을 미치는 요인은 '직급'으로 나타났다(유의확률 〈 0.05)[Table 2]. 분석 결과를 해석하면 다음과 같다.

첫째, 직급이 낮을수록 계정도용 빈도가 높으며 파견직, 프리랜서 등 외부직원 들의 경우 특히 높게 나타났다[Fig. 3]. Visualization 분석에서 이미 이들은 부장급(계정)을 사용하여 제작시스템(EIISBM)에 빈번하게 접속하는 것을 확인하였다[Fig. 4]. 방송직 직렬과 프로그램 제작부서의 도용이 많은 이유는 제작업무의 특성과 밀접한 관련이 있다.

둘째, 근속연수가 2년 미만이고 20대 대졸자의 도용건수가 많은 이유는 파견직, 프리랜서의 도용 비율이 높은 것과 연관된다.

셋째, 방송관련 학과 졸업생들 중 강남에 거주하는 미혼 남자의 계정도용이 많은 이유는 프리랜서, 파견직 등 외부직원과 연관된다. 이들은 회사 근처 1인 가정을 이루고 있는 비율이 높은 것으로 함께 조사되었다.

넷째, 월요일 오후(13~18시) 본사 5층의 계정도용 비율이 높은 이유는 월요일 오후 시간대에 제작업무가 가장 많으며 본사 5층은 위에 열거한 프로그램 제작부서 들이 주로 위치한 곳이다. 이는 계정도용이 회사 내부에서 근무시간 대에 주로 이루어지는 것을 보여준다.

결론적으로, 요인들을 종합해보면 직급과 계정도용과는 반비례 관계에 있었으며 특히, 프리랜서, 파견직 등 외부직원 들의 계정도용이 심각하다고 할 수 있다[Fig. 3].

Table 2. regression analysis between job position and account theft

Model	Factor	Coefficient of Normalized (B)	Standard Error	Significance Probability
1	Staff Level	702.00	0.46	0.04
2	Dependent Variable	count of account theft		

3.5 계정도용 사유에 대한 비율분석

계정도용의 원인을 분석하기 위해 도용직원들을 대상으로 인터뷰를 실시하였다. 인터뷰 방식은 전화, 메일, 면담 등을 통해 사전조사 결과를 전달하고 사유를 수집하여 분석하였다. 조사된 계정도용 사유는 다음과 같다[Table 3].

첫째로, 부장 결재권한 이용 비율이 62%에 해당하였다. 프로그램 제작부서의 경우 외근, 출장 등으로 인한 부장 공석이 잦으며 그에 반해 업무 특성상 신속한 결재가 빈번하게 필요했다. 이는 직원들의

Table 3. reason ratio of account theft

Rank	Reason	Ratio
1	use approval right of manager	62%
2	no account	35%
3	no right necessary for business	11%
4	others	2%

대리결재 비율을 높게 만들었다. ERP 시스템의 경우 업무효율성 극대화에 초점이 맞추어 설계되어 있으며 문제 발생에 대한 사전통제보단 사후적발에 의한 담당자 징계 및 소송을 통한 해결 건수가 평상시 많다. 이는 내부시스템 관리를 접근통제로만 해결하기 어려운 부분이며, 매년 ISMS 인증심사 및 방통위 보안감사를 받고 망 분리 및 보안관리 규정은 모두 충족하지만 내부시스템의 정보유출 및 보안사고가 지속적으로 발생하는 이유이다. 한마디로, 내부보안은 취약하다고 할 수 있다. 계정도용으로 인한 사고는 지속적으로 발생하고 있지만 개선되지 않고 오히려 늘어나고 있으며, 회사 차원의 관리로(전체 메일, SMS 공지 등) 외부에 알려지지 않고 정확한 통계조사가 어렵다.

회사의 보안관리자는 전체 직원 중 1명이며 보안관리 위탁사를 관리하는 업무 형태로 실제 내부보안 관리를 수행하는데 어려움이 있었다.

둘째, 본인 계정이 없는 비율이 35%에 해당하였다. 파견직, 프리랜서 등 외부직원의 경우 인적자원부에서 관리하지 않고 해당 부서에서 직접 관리하며, 수요 부서가 독립적으로 이용하다 보니 외부직원의 전체적인 통제가 불가능했다.

계정발급 절차가 복잡하고 해당 부서에서 직접 신청해야 하며 계정신청 자체가 필수가 아니므로 소수의 계정으로 외부직원들이 공유해서 업무를 수행하는 경우가 많았다〔Table 4〕. 용역계약과 계정발급 프로세스가 분리되어 있고 외부직원의 관리는 해당부서에서 담당하고 있으며 별도의 발령관리를 하지 않기 때문에 실제 계약서와 다르게 조기 퇴사한 경우 파악이 불가능했다.

Table 4. process of account issuance

Work Scope	Procedure
External Staff Hiring Registration	electronic draft by employee (service contract attached) → arbitrary decision by manager
External Staff Account Issuance	electronic draft by deputy employee(security pledge attached) → arbitrary decision by manager → internal dispatch by administrator of IT management division → arbitrary decision by manager of IT management division → account issuance by administrator of IT management division

셋째, 업무 수행에 필수적인 권한이 없는 경우가 11%에 해당하였다. 파견직, 프리랜서 등의 외부직원 비율이 전체 직원의 35%에 해당하며 계정도용의 84%는 이들 외부직원 들에 의해 발생하였다. 이들에게는 최소한의 권한만 주어지기 때문에 업무 특성을 고려한 추가적인 권한 작업이 필요하였다. 최소권한에 의한 업무분리 체계는 현장에서 잘 지켜지지 않았다.

IV. 개선모델 도출 및 검증

본 장에서는 실증연구를 통해 분석된 결과들을 바탕으로 개선모델을 도출하고 이를 적용하여 개선효과를 검증한다.

4.1 개선모델

첫째, 부장 공석 시 업무처리를 위한 결재권한 위임기능을 개발한다〔Fig. 5〕. 실제, 국내 지상파 방송사 4곳을 확인한 결과 ERP시스템의 결재권한 위임기능이 모두 없어 이에 대한 개발이 필요했다.

참고로, 현행 시스템의 결재 프로세스는 다음과 같다.

(1) 제작계획서 작성 → 부장승인 → 통제부서 승인 (방송제작기획부) → 기획예산부 승인 → 추산 생성
(2) 내용계획서 작성 → 부장승인 → 통제부서 승인 (방송제작기획부)
(3) 제작청구서 작성 → 부장승인 → 통제부서 승인 (방송제작기획부) → 기획예산부 통제 → 전표작성 → 부장승인 → 재무회계부 승인
(4) 전표작성 → 부장승인 → 기획예산부 승인 →재무회계부 승인

둘째, 외부직원의 관리 기능을 해당 부서들에서 조직법무부로 통합 이관한다. 또한, 외부직원 계약과 이들의 계정발급 프로세스를 일원화 한다. 외부직원 계약서를 ERP 시스템에 등록하고 등록 시 계정 자동 발급을 통해 1인 1계정을 부여한다. 현재는 비정형 형태의 전자기안만 작성하고 있으며 개선된 프로세스는 ERP시스템 계약등록 → 전자기안 템플릿 호출 → 전자기안 작성 → 부장전결 → 계정발급 형태

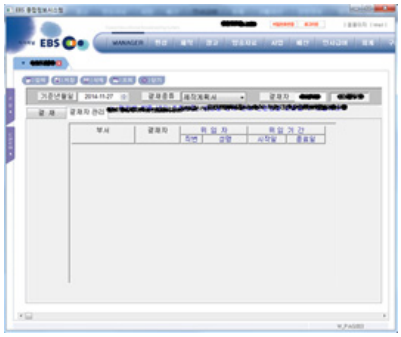


Fig 5. authority delegation interface

로 개발한다[Table 6].

셋째, 외부직원의 경우 직무별로 필요한 권한을 조사하여 세분화시켜 부여한다[Table 5]. 이는 두

Table 5. authority grant of external staff

External Staff	Window Count	Function Count	Data Level	Role Name
PD AD writer	13	21	1	Role1
advertising-editor	7	24	1	Role2
announcer makeup- artist illuminator sound- engineer contributing-editor acting- guidance reporter camera	3	6	1	Role3
MD	5	17	1	Role4
encoder	2	2	1	Role5
designer stage artist special effect prop man	29	97	1	Role6
material-examiner	2	2	1	Role7
dispatched-teacher	9	31	1	Role8
PC service- engineer	8	14	1	Role9
mail room phone service-engineer	11	2	1	Role10
front desk driver	1	1	1	Role11

Data Level (scope of inquiry) :
1 individual, 2 division, 3 head office,
4 entirety.
Window Count : count of accessible interfaces

Fig. 6. generation and grant of role

번째 항목의 계정 자동발급 시 권한과 통합되도록 하였다.

Table 6. ERP System function developement

Work Scope	Interface ID	Function Name	C	R	U	D
New	W_BMR 001	delegation of approval right	O	O	O	O
	W_BMR 002	registration of external staff service contract	O	O	O	O
		integration of electronic draft	O	O	O	O
		account issuance	O	O		

C: insert, R: select, U: update, D: delete

Table 7. development environment

Server	Version
DB Server	PowerBuiler 12.0
	MSSQL Server 2008
	Windows Server 2012
Distribution Server	PowerBuiler 12.0
	Microsoft Windows XP

4.2 시스템 개선 및 적용계획 수립

시스템을 개선한 후 계정도용이 빈번한 부서들 가운데 타겟 부서를 선정하고 개선방안 적용계획을 협의한다.

개선된 내용을 프로그램 제작부서(유아·어린이부, 초·중·학창의인성부, 교육뉴스부 세 곳)에 배포한 후

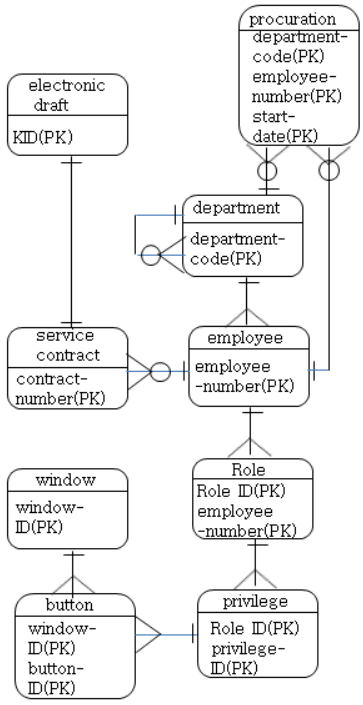


Fig. 7. improved ERD relation

적용 전과 후의 모니터링을 통해 개선효과를 정량적으로 측정한다.

4.3 개선안 적용에 따른 효과 측정

표본 부서에 Deploy 후 모니터링을 해 보니 적용 첫 주 계정도용 비율이 58% 감소하였으며, 2주 후에는 85%의 감소율을 보였다[Fig. 8]. 2차 인터뷰를 실시하여 조사한 결과 대부분의 직원들은 부장의 결재위임 기능 및 계정발급 절차의 간소화 부분에

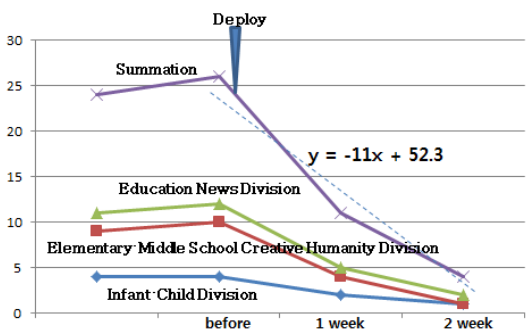


Fig. 8. reduction ratio of account theft after deploy

서 만족도가 높게 나타난 것으로 조사되었다.

4.4 접근관리 실증분석 프로세스

지금까지의 실증연구 과정과 절차를 표준화하여 타 시스템 또는 사업장에서도 적용이 가능하도록 프로세스를 제시한다[Fig. 9].

(1)먼저, 대상서버를 선정한다. 기업 내부에는 업무의 목적과 종류에 따라 다양한 시스템들이 존재하며 이중 직원들의 사용률이 높고 개인 및 민감한 기업정보를 보관하고 있는 서버를 탐색한다. 탐색결과, ERP 시스템을 대상으로 선정하였다.

(2)대상이 결정되면 서버의 Syslog 파일을 수집한다. Syslog 파일의 위치는 서버의 Operating System 별로 다음과 같이 나누어 질 수 있다.

Unix/Linux Server: /etc/syslog or /var
Windows Server: Eventviewer

(3)로그 파일이 수집되면 최근 1년 간의 시스템 접속 정보를 조사한다. 접속시스템 별로 인사 및 부서정보, IP주소를 통한 위치정보 등 다양한 factor들과 Mapping 하여 실태를 분석한다. 이때, 분류기준에 따른 광범위한 조사를 필요로 하며 요인분석을 통해 관련성을 추론할 수 있는 항목이어야 한다. 이 논문에선 직원들의 인사조직, 사회경력, 개인이력, 사용환경 측면의 14개 분류기준으로 데이터를 분석하였다.

(4)분류된 데이터를 이용하여 Visualization 분석을 실시한다. Visualization 분석이란 시스템 로그나 실험분석 결과 등에 대한 통계정보를 한 눈에 살펴볼 수 있도록 데이터들의 관계와 그룹핑을 표현하는 기법이다. 분석 툴 선정은 오픈소스 프로그램이며 분석이 용이한 SECVIZ를 이용하였다. 실제 Visualization 분석을 통해 외부직원들의 계정도용 비율이 높음을 발견할 수 있었다.

SECVIZ : http://www.secviz.org[3]

(5)Visualization 분석이 완료되면 요인분석을 통해 요인들과의 연관성을 탐색하고, 개별 요인들과 도출된 변수들 사이의 회귀분석을 실시한다. 회귀분석은 요인들과 특정 변수 사이의 인과 관계를 분석하는 기법이다. 개별 요인이 회귀분석에서 의미를 가지

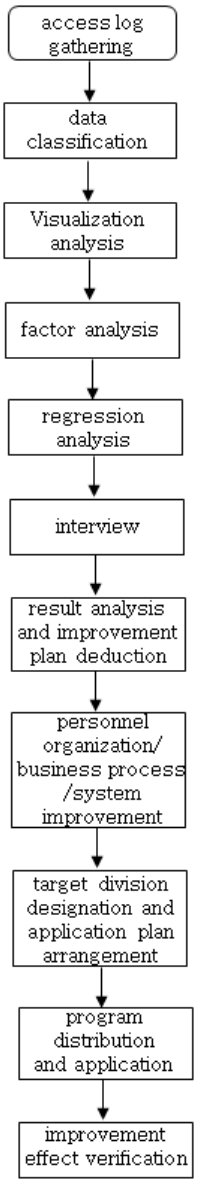


Fig. 9. regression study process

기 위해서는 유의도가 0.05 이하가 되어야 한다.

(6)담당자 인터뷰는 전화, 메일, 면담 등을 통해 조사결과를 전달하고 사유를 수집하여 분석한다. 이 경우 담당 부서 직원들의 적극적인 협조가 필요하다. 실제 조사과정은 익명 또는 인사 상의 불이익이 없는 순수 연구조사 임을 강조하는 등 응답률을 높일 수 있는 방법을 고안해야 한다.

(7)분석이 완료되면, 회귀분석 및 담당자 인터뷰 결과를 토대로 개선모델을 도출한다. 개선방향 설정은 사유에 따라 적절해야 하며 실현 가능성을 충분이 고려해야 한다. 이 논문에선 개선방안을 인사조직, 업무절차, 시스템개선의 측면으로 나누어 제시하였다.

(8)개선모델이 마련되면 타겟부서를 선정하고 적용계획과 일정을 협의한다. 타겟부서 선정은 효과 검증이 유리하도록 적용과 평가가 용이하여야 하고, 분석 결과를 토대로 유아·어린이부, 초·중·학창의인성부, 교육뉴스부로 정하였다.

(9)마지막으로, 개선된 내용을 타겟부서에 배포 및 적용한다. 배포 방식은 인프라 환경에 따라 적절하게 결정하고 적용된 시스템 사용에 대한 메뉴얼을 작성하여 교육하여야 한다. 조직 측면에선 규정 개편에 대한 의사결정과 절차의 복잡성으로 제한적으로 적용할 수 밖에 없었다.

(10)적용 전과 후의 모니터링을 통해 개선효과를 검증한다. 개선효과는 다양한 지표들을 통한 정량분석을 실시한다.

V. 결 론

이 논문에선 시스템 접근관리 상의 문제점을 실증적으로 분석하기 위한 표준 프로세스를 제안하였으며, 실제로 특정 기업에 이를 적용하여 입증해 보았다. 또한, 연구과정에서 발생한 프로세스의 단계별 의사결정 기준과 영향을 주었던 변수들에 대해 정리하였다.

먼저, 분석대상은 기업 내부에서 직원들의 사용률이 높고 민감한 개인 및 기업정보를 보관하고 있는 시스템으로 선정하였다.

선정 후, 서버의 Syslog 파일을 수집하여 연간 시스템 접속 정보를 다양한 factor 들로 분류하였다.

분류된 데이터들을 Visualization 분석을 실시하여 데이터들의 관계를 조사하고, 요인분석을 통해 factor 들의 연관성을 탐색하였으며, 개별 요인들과 도출된 변수들 사이의 회귀분석을 실시하였다.

담당자 인터뷰는 전화, 메일, 면담 등을 통하여 결과를 전달하고 사유를 수집하여 분석하였다. 조사과정에서 직원들의 적극적인 협조가 필요하므로 응답률을 높일 수 있는 방안을 고안하였다.

회귀분석 및 담당자 인터뷰 결과를 토대로 개선모델을 도출하였다. 개선방안은 인사조직, 업무절차, 시스템 개선의 측면으로 나누어 제시하였으며, 시스템의 특성과 예산 등을 고려하여 실현 가능성을 충분

이 반영하였다.

개선모델 완료 후, 적용과 평가의 용이성을 고려하여 타겟부서를 선정하고, 적용계획과 일정을 협의하였으며, 이에 따라 개선모델을 배포 및 적용하였다. 배포 방식은 인프라 환경에 따라 적절하게 결정하였으며, 사용자 메뉴얼을 작성하고 교육을 실시하였다. 규정 개편은 의사결정과 절차의 복잡성으로 제한적 적용이 가능하였다.

적용 후 모니터링을 통해 개선효과를 검증하였으며, 개선효과는 다양한 지표들을 통한 정량분석을 실시하였다.

끝으로, 많은 기업들이 이 프로세스를 활용한다면 현장에서 쉽고 체계적으로 시스템 접근관리에 대한 문제점을 실증적으로 분석하고 개선하는데 도움을 줄 것이다.

하지만, 산업별 시스템별로 다양한 변수들이 존재할 수 있으며 이 경우, 제시된 단계별 의사결정 기준과 변수들을 참고하여 각 기업의 특성에 맞는 프로세스를 응용한다면 기업들의 실제적 보안관리는 한층 강화될 것이다.

References

〔1〕 2011 Cyber Security Watch Survey, CERT, Jan. 2011.

〔2〕 Ji-hoon Song and Si-jin Lee, "The study of customized internal insider security model based on insider security accident," Korean Society For Internet Information, vo1. 12, no. 1, pp. 71-82, Feb. 2011.

〔3〕 SECVIZ, http://www.secviz.org/content/the-davix-live-cd

〔4〕 Baek-ho Sung, Byung-chul Park, Dong-kyoo Shin, Dong-il Shin, Ki-young Moon and Jae-seoung Lee, "A Study of the EAM based on the xml for e-Commerce," Korea Institute of Information Security and Cryptology, vol. 13, no. 2, Dec. 2003.

〔5〕 "E-business and extended ERP," Management and Information technology of MIT, Apr. 2000.

〔6〕 Tae-myeong Chung, "A study on generalization of security policies for ent erprise security management system," Korea Information Processing Society , vol. 9, no. 6, Jun. 2002.

〔7〕 "Priorities for ERP SECURITY," Ele ctrical Wholesaling, Aug. 2013.

〔8〕 "JD Edwards, System Foundation," JD Edwards Enterprise software, pp. 743-753, Jun. 1999.

〔9〕 Jung-man Son and Sang-wan Lee, "PMI based User Authentication Mana gement for ERP," Korea Industrial And Systems Engineering, no. 56, pp. 108- 111, Oct. 2003.

〔10〕 Chi-sung Won, Sang-hwan Leem and Wan-sub Um, "A study on the Inside Security of Enterprise Resource Planning," Korea Institute of Industrial Engineers, no. C11-5, pp. 1041-1043, Nov. 2005.

〔11〕 David A, Thomas K and Mark H, "ERP Critical Success Factors: An Exploration of the Contextual Factors in Public Sector Institutions," Proceed ings of the 35th Hawaii International Conference on System Sciences, Jan. 2002.

〔12〕 Mark Denning, Kate Hill, Bernard Do dd, Jonathan Lingard, Gray Elkingon, EricMatthews, Wendy Hewson and Jo nathon R. Tate, "using SAP R/3," QUE, pp. 743-753, Dec. 2003.

〔13〕 Sang-hwan Leem, "UML with ERP Security Framework implementation," International Journal of Management Science & Financial Engineering, no. SA01-5, pp. 664-667, May. 2005.

〔14〕 Eun Kim, Yun-seok Lee and Min-soo Jung, "A scheme of Permission Trac king based on RBAC and DAC from Digital Forensics Point of view," The Korean Institute of Communications and Information Sciences, pp. 675-676, Jun. 2011.

〈저자소개〉

조 영 석 (Young Seok Cho) 정회원
2000년 2월: 고려대학교 금속공학과 졸업
2006년 8월: 고려대학교 정보경영공학전문대학원 석사과정 수료
〈관심분야〉 위험관리, 정보보호컨설팅, ERP, 데이터베이스

임 종 인 (Jong In Im) 정회원
1980년 2월: 고려대학교 수학과 학사
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
현재: 고려대학교 정보보호대학원 원장, 고려대학교 사이버국방학과 교수, 개인정보보호위원회 위원, 대검찰청 디지털수사자문위원회 위원장, 금융보안연구원 보안전문기술위원회 위원장, 안전행정부 정책자문위원회 위원, 국방부 정보화책임관 자문위원, 한국저작권위원회 위원 등
〈관심분야〉 사이버국방, 정보법학, 디저털포렌식, 개인정보보호, 융합기술보안 등

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