Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.25, NO.6, Dec. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.6.1607

금융회사 서버 Privilege 계정 운영방식 결정 모델

이 석 원,† 이 경 호‡
고려대학교

Decision Making Model for Selecting Financial Company Server Privilege Account Operations

Suk-Won Lee,† Kyung-Ho Lee‡
Korea University

요 약

서버 Privilege 계정은 법규에 따라 운영 되어야 한다. 그러나 농협은 서버 Privilege 계정 운영에 대한 법규 미준수와 운영 미흡으로 서버의 모든 데이터가 삭제되는 농협 전산망 해킹 사건이 발생하였다. 본 연구에서는 금융회사의 서버 Privilege 계정 운영방식을 결정하기 위한 모델을 제시하기 위해 금융회사의 Privilege 계정 운영 현황을 조사하여 문제점을 도출하고, 개선방안을 제시한다. 또한, Privilege 계정 운영현황 조사를 통해 선정된 평가요인은 AHP(Analytic Hierarchy Process)를 사용하여 의사결정 모델과 공식을 제시하고 검증한다.

ABSTRACT

The server privilege account must be operated through law and regulation. However, due to regulation non-compliance and inadequate operation on financial company server privilege, an incident that every server data being deleted by hacker occur which is later being named as 'NH Bank Cyber Attack'. In this paper, the current operation status on financial company privilege accounts is being analysed to elicit problems and improvement. From the analysis, important evaluation factors will be also selected and applied generating the decision making model for financial company server privilege account operation. The evaluation factor deducted from privilege account status analysis will be used to present and verify the decision making model and formula through AHP(Analytic Hierarchy process).

Keywords: Server Privilege Account, AHP, Information Security, Decision Making

I. 서 론

1.1 연구배경 및 목적

2011년 4월12일 농협 전산망 해킹 사건이 발생하여 내부서버 180대(전체 440대), 웹서버 45대(전체 98대), 테스트 서버 48대(전체 49대) 총 273대(전체 587대) 서버의 모든 데이터가 삭제되어 농협 전산망이 마비되는 사고가 발생하였다[1].

이 사건에서 해커는 서버에 접근하기 위해 각 서버의 최고관리자 계정 비밀번호를 획득하였으며, 이를 통하여 데이터를 삭제할 수 있었다. 특히, 농협은행은 서버의 최고관리자 계정을 협력업체와 공유하였을 뿐만 아니라, 비밀번호를 '1', '0000'처럼 단순하게 설정해 두거나, 최대 7년 동안 동일한 비밀번호를 유지하는 등 전산 보안을 허술하게 관리해왔다[2].

2011년 당시 금융회사들은 전자금융감독규정시행세칙(2009년7월27일)에 의해 비밀번호를 숫자와 문자 등을 혼합하여 6자리 이상을 부여하고, 분기 1회 이상 정기적으로 변경해야한다는 규정이 있었다[3].

Received(11. 04. 2015), Modified(12. 04. 2015), Accepted(12. 07. 2015)
† 주저자, soslee78@hanmail.net
‡ 교신저자, kevenlee@korea.ac.kr(Corresponding author)

하지만, 농협은행은 '전자금융감독규정시행세칙' 규정과 자체 '전산업무처리지침'에 명시된 비밀번호 관련 지침을 제대로 이행하지 않아 농협 전산망 해킹 사건이 발생하는 원인을 제공하였다[2]. 이 사건 이후 이러한 문제점을 보완하기 위해 2011년 10월 10일 '전자금융감독규정'이 개정되었다[4].

이와 관련하여 개정된 주요 내용을 보면 '제12조(단말기 보호대책)3.비밀번호는 생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정하고 분기별 1회 이상 변경할 것', '제26조(직무의 분리)7.정보보호 기술부문 인력과 정보보호인력', '제32조(내부사용자 비밀번호 관리)2항 나.비밀번호 보관 시 암호화, 다.시스템마다 관리자 비밀번호 다르게 부여'[4] 하도록 개정되었다.

본 연구에서는 서버의 최고관리자 계정 즉, 'Privilege 계정'에 대해서 농협 전산망 해킹 사건 이후 서버 Privilege 계정[1]의 운영방식 현황을 설문조사 및 FGI(Focus Group Interview)를 통하여 문제점을 도출하고 개선방안을 제시한다. 또한, 운영방식이 합리적으로 선택할 수 있도록, 서버 Privilege 계정의 운영방식 선정 시 고려해야할 평가 요인들을 선정하고, 우선순위를 분석함으로써 AHP를 이용한 의사결정 모델과 공식을 제시하고 검증한다.

1.2 연구방법 및 구성

본 연구에서는 Privilege 계정 운영방식 현황에 대한 자료수집을 위해 국내 20개 금융회사 Privilege 계정 담당자와 설문을 통해서 자료를 수집한다. 이중 14개 금융회사를 대상으로 FGI(Focus Group Interview)를 통하여 문제점을 도출하고 Privilege 계정 운영방식에 영향을 미치는 평가 요인을 선정한다.

선정된 평가 요인은 국내 14개 금융회사 Privilege 계정담당자와 보안컨설팅 전문가 16명을 대상으로 다기준 의사결정(MCDM : Multiple Criteria Decision Making)시 널리 사용되는 AHP 모델을 사용하여, 그 결과를 분석한다.

본 연구의 구성은 다음과 같다. 제Ⅰ장 서론에서는 연구배경/목적, 연구방법/구성에 대해서 기술한다. 제Ⅱ장에서는 선행연구로서 계정관리에 관한 연구와 AHP 모델 연구를 기술한다. 제Ⅲ장에서는 Privilege 계정 운영방식 현황, 문제점 도출 및 개선방안을 제시한다. 제Ⅳ장에서는 Privilege 계정 운영방식 의사결정 모델과 공식을 제시하고, 사례를 통해 검증한다. 제Ⅴ장 결론에서는 본 연구의 시사점에 대해서 기술한다.

1) Privilege 계정 : UNIX, LINUX, MAINFRAME, WINDOWS(NT) 서버의 관리자 권한이 부여된 계정

Ⅱ. 선행연구

2.1 계정관리에 관한 연구

계정관리란 사용자, 서비스, 그리고 정보통신기기 등 네트워크에 연결되는 개체의 Identity의 속성, 신원증명서(Credentioal), 정보이용 자격(Entitlement) 등을 포함한 Identity의 생성, 이용, 폐기를 위한 전체 생명주기를 관리해주는 플랫폼 기반구조로, 조직의 내부망·외부망으로부터 접속해오는 사용자 또는 단말기를 인증하고 해당하는 권한을 확인하여 정보자원에 대한 적절한 접근권한을 인가해주는 과정이다[5].

접근권한관리란 사용자와 시스템의 통신과 다른 시스템 및 자원에 대한 상호작용을 식별과 인증, 권한부여하는 과정이다[5].

계정관리 관련 문헌을 통해 그 동안 연구해온 계정관리 및 접근권한관리 방안을 고찰한다. 김호동 [16]은 Kerberos, GSSAPI(Generic Security Services Application Program Interface) 및 SSH(Secure Shell) 를 이용하여 SSO(Single Sign On)를 구축하는 연구를 진행하였다. 평상 시 Kerberos를 통해 GSSAPI 인증을 하고, Kerberos 서버에 장애가 발생할 경우에는 SSH를 이용한 Password 인증을 통해 접속하도록 SSO를 구축하였다. 윤관식[17]은 사용자 정보만으로 사용자의 권한을 제어하는 기존 EAM(Enterprise Access Management) 시스템의 문제점을 제시하고, 이용자 정보 외에도 디바이스 정보, 네트워크 정보, 위치 정보, 시간정보를 활용하여 사용자의 권한을 제어하는 방안을 제시하였다. 이용한[18]은 비즈니스 어플리케이션에 대한 접근제어 모델로 CIAAC(Context Information-based Application Access Control)를 제시하였다. CIAAC는 하드 코딩된 어플리케이션 접근제어 규칙을 컨텍스트 개념을 도입해 분리 정의함으로써 비즈니스 어플리케이션이 본연의 업무처리에 집중하게 하고, 비즈니스 어플리케이션의 운영자가 환

경변화에 따라 쉽고 유연하게 접근제어 정책을 변경할 수 있다고 제언하였다.

계정관리 및 접근권한관리에 대한 기술은 SSO, IM(Identity Management), EAM(Enterprise Access Management), IAM(Identity and Access Management), PM(Password Management)이 있다. 각 기술의 선행연구 결과 SSO는 단일 인증으로 한 시스템에 사용자가 인증한 이후 접근 권한이 있는 다양한 어플리케이션 시스템에 자동으로 인증하는 기술이고[5], IM은 계정을 통합 관리하여 계정의 신청·승인 등 계정을 효율적으로 관리하는 기술이다[6]. EAM은 자동화된 Role 정책에 따라 업무시스템 권한이 부여되며, 사용자의 속성정보를 기준으로 공통된 역할을 분류하여 최소자원만 접근하도록 관리를 지원하는 기술이고[6], IAM 시스템은 SSO, EAM, IM을 통합한 기술이다[5]. PM은 서버 계정의 패스워드를 시스템에서 일정 규칙에 맞게 주기적으로 변경하고, 중요한 계정은 관리자의 승인 시에 패스워드를 발급하는 등의 계정의 패스워드를 관리하기 위한 기술이다.

접근권한관리를 위한, 접근제어 모델은 MAC(Mandatory Access Control), DAC(Discretionary Access Control), RBAC(Role Based Access Control)로 구분된다[7]. MAC은 주체와 객체에 각각 보안 등급이 정해져 있으며, 시스템 내에서 정해져 있는 등급비교를 통해 접근제어를 수행하는 기법이다. DAC은 시스템 객체의 소유자가 정한 정책에 따라 주체의 접근을 제어하는 방식으로 오늘날 대부분의 운영체제 시스템에서 채택한 기법이다. RBAC은 각 주체 또는 객체에 권한을 주는 것이 아니라, 주체에게 특정 권한이 부여된 역할을 할당하는 기법이다[8]. 이중 많은 시스템들은 접근제어를 통제하기 위해 RBAC 모델을 사용하고 있으며, 계정관리 시스템과 연동하여 사용자의 접근을 통제하고 있다[7].

2.2 AHP 모델 연구

본 연구에서는 Privilege 계정 운영방식을 선정하기 위해 AHP(Analytic Hierarchic Process)를 활용한다. Saaty[15]에 의해 개발된 AHP는 복수의 대안에 대한 복수의 평가기준이 존재하는 다기준 의사결정 문제를 해결하기 위한 대표적인 기법으로, 다양한 유형의 의사결정 문제에 폭넓게 활용되어 왔다[9].

AHP는 주어진 의사결정 문제를 목표, 평가 요인, 대안으로 구성되는 계층(Hierarchy)으로 Fig 1. 과

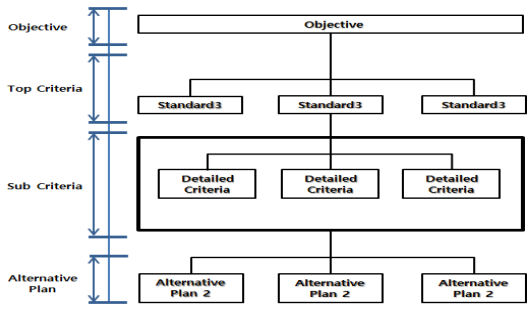

Fig. 1. Example of AHP Layered Model

같이 모형화 하고, 각 계층 내 의사결정 요소들 간의 쌍대비교(Pairwise Comparison)를 수행함으로써 최종 우선순위를 도출한다. AHP는 계층 모형 구축, 쌍대비교, 부분 우선순위 도출, 일관성 평가, 최종 우선순위 도출 및 대안 선택의 5단계로 이루어진다[9].

AHP는 다양한 유형의 MCDM 문제 해결에 효과적으로 연구되고 있다. 성기훈 등[12]은 AHP를 기반으로 SNS 제공환경에서 정보보호의 중요 위협요인을 분석하고, 정보보호 투자 결정 기준을 도출하는 연구를 진행하였다. 연구결과 SNS 제공환경에서 '개인 프로파일 위조 및 명예훼손'과 '산업 스파이가' 정보보호의 중요 위협으로 분석되었으며, '서비스 이미지'가 정보보호 투자 결정기준에서 가장 중요한 요인으로 도출되었다. 정용욱 등[13]은 속성기반의 악성코드 유사도 분류에 대한 문제점을 개선하기 위해 속성에 대한 가중치 분석 연구를 진행하였으며, AHP 기법을 활용하여 속성별 중요도를 도출하였다. 연구결과 AHP 분석 결과 '원격 동적 라이브러리', '제어 및 명령'이 중요도가 높은 속성으로 도출되었다. 김동욱 등[11]은 정보통신기술의 발전과 스마트 시대 전환에 따른 정보보호 문제에 대한 정책 대응방안을 모색하는 연구를 진행하였으며, AHP 분석을 통해 우리나라의 정보보호 정책 및 전략에 관한 우선순위를 제시하였다. 연구결과 정책중요도 측면에서는 '법제도 정비'의 중요도가 가장 높게 평가되었으며, 정책 시급성 측면에서는 '추진체계 정비'의 중요도가 가장 높게 평가되었다. 윤석웅 등[10]은 이용하여 VoIP 정보보호 점검항목의 중요도 연구를 진행하였으며, AHP분석 결과 기술적 보안 영역에서는 '네트워크 보안'이, 관리적 보안 영역에서는 '침해사고 대응'이, 물리적 보안 영역에서는 '출입 및 접근 보안'이 가장 중요한 항목으로 분석되었다. 신영진 등[14]은 공공분야 개인정보 정책 집행과제의 우선순위를 분석하였으며,

AHP를 통해 개인정보보호 수준 진단 지표의 중요도를 도출하였다. AHP 분석 결과 개인정보 정책·기술적 측면의 지표가 가장 높게 나타나 개인정보보호 환경을 조성하기 위한 기반 확충이 가장 우선시 되어야 함을 제언하였다. 신상필 등[9]은 AHP를 활용한 모바일 오피스 시스템의 구현방식 선정에 관한 연구를 진행하였으며, 연구결과 '업무생산성', '보안성'이 모바일 오피스 시스템 구현방식 선정 시 가장 중요한 요인으로 도출되었다. 이처럼 AHP는 우선순위를 도출하기 위한 다양한 연구에서 활용되고 있으며, 현존하는 의사결정에 대한 이론 중 가장 광범위하게 인정을 받아 다양하게 활용되고 있는 이론이다[19]. AHP는 의사결정 시 두뇌가 단계적 분석과정을 활용한다는 사실에 착안하여 개발 되었으며 어떤 분야든 의사결정이 요구되는 사항에 적용 가능한 범용적 모델이라고 할 수 있다[19]. 또한 쌍대비교를 통해 체계적이고 합리적인 의사결정을 가능하게 해주기 때문에 '서버 Privilege 계정 운영방식 결정'을 위한 최적의 방법이라고 판단되었다. 따라서 본 연구에서는 다양한 연구에서 활용되고 있는 AHP를 모델에 적용하였으며, 적용방법과 결과는 제Ⅳ장에서 확인할 수 있다.

III. Privilege 계정 운영방식 현황 및 문제점

3.1 Privilege 계정 운영방식 현황

금융회사 Privilege 계정 운영방식 설문조사 결과, Table 1.과 같이 수작업 방식, 자체개발 방식 및 솔루션 방식 3가지 방식으로 운영하고 있다. 본 연구에서는 설문조사와 인터뷰를 통해서 3가지 방식의 현황, 장·단점, 문제점 및 개선사항을 도출한다.

Table 1. Privilege Account Operation

Handm-ade	Administrator periodically change privilege account password of each server through handmade technique. Record the password in the mana- gement register and it is kept in the safe. The approval of the Dire- ctor is required when using the account.
Self-Develo-pment	Privilege password of each server are changed periodically by Self-Development technique. Privilege password is encrypted. The appr-oval of the Director is required when using the account.
Solution	Privilege password of each server are changed periodically (every day or every use) by Solution. Privilege password is one-way or two-way encrypted. The approval of the Director is required when using the account.

3.1.1 수작업 Privilege 계정 운영방식

Table 2.는 14개 회사 중 수작업 방식을 사용하고 있는 7개 회사에 대한 현황을 보여주고 있다. 수작업 방식의 Privilege 계정 운영은 2011년 4월 농협 전산망 해킹 사건 이전에도 사용하는 방식이다. 7개의 금융회사 중 3개 회사(2, 5, 8)는 수작업 방식으로 WINDOWS Privilege 계정의 패스워드를 변경하고 있으며, 주기적으로 패스워드를 변경하고 있지 않다.

Table 3.은 Table 2.의 운영현황과 인터뷰를 통해서 조사된 수작업 방식 Privilege 계정 운영의 장·단점이다. 수작업 방식의 장점은 서버 장애 시 Privilege 패스워드를 서버 관리자가 숙지하고 있기 때문에 장애대응이 빠르다. 단점은 서버 관리자가 서버

Table 2. Operation Status of Handmade Privilege Account

Company	Privilege Account Password		Dep
	Change Method	Before April.2011	
Finance 2	Handmade (WINDOWS) (No Change Password)	Handmade	Server
Finance 3	Handmade	Handmade	Server
Finance 5	Handmade (WINDOWS) (No Change Password)	Handmade	Security
Finance 8	Handmade (WINDOWS) (No Change Password)	Handmade	Server
Finance 10	Handmade	Handmade	Server
Finance 11	Handmade	Handmade	Server
Finance 14	Handmade	Handmade	Server

Table 3. Operating Pros & Cons of Handmade Privilege Account

Pros	Cons
- Fast response on s-erver failure	- Slow to change pas-sword - High input error by user - Low security

마다 수작업으로 패스워드를 변경하기 때문에 패스워드 변경 속도가 늦고, 사용자 입력 오류가 발생한다. 또한, 패턴으로 패스워드를 변경하기 때문에 패턴노출에 대한 위험이 존재하여 보안성이 낮다.

3.1.2 자체개발 Privilege 계정 운영방식

Table 4.는 14개 회사 중 자체개발 방식을 사용하고 있는 1개 회사에 대한 현황을 보여주고 있다. 자체개발 방식은 Privilege 계정 패스워드를 자체개발 프로그램을 통해 일정한 패턴으로 일괄 변경하는 방식이다.

Table 4. Operation Status Self-Development Privilege Account

Company	Privilege Account Password		Dep
	Change Method (Present)	Before April.2011	
Finance 1	Self-Devel-opment	Handmade	Server

Table 5.는 Table 4.의 운영현황과 인터뷰를 통해 조사된 자체개발 방식의 서버 Privilege 계정 운영의 장·단점이다. 자체개발 방식의 장점은 자체개발 프로그램으로 패스워드를 변경하기 때문에 수작업에 비해 패스워드 변경속도가 빠르고, 패스워드 변경 시 오류발생이 낮다. 또한 서버 장애 시 Privilege 패스워드를 서버 관리자가 숙지하고 있기 때문에 장애대응이 빠르다. 단점은 수작업 방식과 동일하게 패턴을 활용하여 패스워드를 변경하기 때문에 패턴 노출에 대한 위험이 존재하여 보안성이 낮다.

Table 5. Operating Pros & Cons of Self-Development Privilege Account

Pros	Cons
- Fast to change pas-sword - Low error on chang-ing password - Fast response on s-erver failure	- Low security

3.1.3 솔루션 Privilege 계정 운영방식

Table 6.은 14개 회사 중 솔루션 방식을 사용하고 있는 9개 회사에 대한 현황을 보여주고 있다. 9개사 중

Table 6. Solution of Operating Privilege Account Status

Company	Privilege Account Password		Dep
	Change Method	Before April.2011	
Finance 2	PM Solution (UNIX)	Handmade	Server
Finance 4	EAM Solution (UNIX)	EAM Solution	Server
Finance 5	IM Solution (UNIX)	Handmade	Security
Finance 6	PM Solution	IM Solution	Server
Finance 7	PM Solution	Solution	Server
Finance 8	PM Solution (UNIX)	Handmade	Server
Finance 9	EAM Solution	Handmade	Server
Finance 12	PM Solution	Solution	Security
Finance 13	PM Solution	Handmade	Security

3개 회사(4, 5, 9)는 IM, EAM 솔루션을 사용하여 관리하고 있고, Privilege 계정의 사용시 마다 승인을 득하지 않고 있으며, 패스워드는 양방향 암호화되어 있어 복호화가 가능하다. 9개사 중 6개 회사(2, 6, 7, 8, 12, 13)는 PM솔루션을 통하여 Privilege 계정 사용시 마다 승인을 득한 후 발급된 Privilege 계정 패스워드를 입력하여 접속한다. 패스워드는 일방향 암호화 되어 복호화가 불가능하다.

Table 7.은 Table 6.의 운영현황과 인터뷰를 통해 조사된 솔루션 방식 Privilege 계정 운영의 장·단점이다.

솔루션 방식의 장점은 솔루션으로 서버의 Privilege 계정의 패스워드를 변경하기 때문에 패스워드 변경속도가 빠르고, 패스워드 변경에 따른 오류발생이 낮다. 또한 패스워드 사용 시 책임자의 승인을 득하고, 패스워드는 일1회 이상 변경되기 때문에 보안성이 높다. 단점은 솔루션 장애발생 시 계정의 패스워드를 알 수 없기 때문에 솔루션 장애발생에 따른 업

Table 7. Pros & Cons about Solution of Operating Privilege Account Status

Pros	Cons
- Fast to change pass-word - Low error on chang-ing password - High security	- Slow business process-ing on solution fail-ure - Slow response on s-erver failure

무처리가 지연된다. 또한, 서버 장애발생 시 Privilege 계정 사용이 필요한 경우 책임자의 승인이 필요하기 때문에 장애대응 시 지연이 발생한다.

3.2 Privilege 계정 운영의 문제점 및 개선방안

Table 8.과 같이 Privilege 계정 운영에 대한 4가지 문제점을 도출하였다.

첫 번째, Privilege 계정 운영에 대한 직무분리 미흡이다. Privilege 계정 운영은 보안부서 등의 제3의 부서에서 관리되어야 하지만 대부분의 금융회사는 서버관리자가 서버관리와 Privilege 계정을 운영하고 있었다. 이러한 문제점은 2010년 농협 전산망 해킹 사건 이후 개정된 전자금융감독규정 '제26조(직무의 분리) 7.정보보호 기술부문 인력과 정보보호인력' 위반이다. 직무분리가 미흡할 경우 서버 관리자의 Privilege 계정 사용 남용과 통제가 이루어지지 않는다.

두 번째는 Privilege 계정 공유이다. 비상 또는 장애발생 이외에도 운영을 위해 업무시스템 운영직원 및 외주직원과 공유하고 있었다. Privilege 계정을 공유하는 경우 외부노출과 악의적인 사용으로 금융사고가 발생할 수 있다.

세 번째는 Privilege 계정의 사용권한 부여 시 언제든지 Privilege 계정을 사용할 수 있다. Privilege 계정은 중요한 계정으로 관리자에게 권한을 부여받고, 사용시 승인을 획득한 후 사용해야 한다. 그러나 권한을 부여 받으면 언제든지 Privilege 계정을 사용할 수 있다. 계정 사용 후 Privilege 계정을 사용 목적에 따라 적합하게 사용했는지에 대한 사후검토를 수행하고 있지 않다. 또한, 서버관리자는 별도의 통제를 받지 않고 Privilege 계정을 사용한다.

마지막으로 WINDOWS의 Privilege 계정 관리 미흡이다. WINDOWS Privilege 계정은 패스워드를 주기적으로 변경하고 있지 않거나, 예외 처리하여 변경하고 있지 않았다. 이 문제점은 전자금융감독규정[4] '제32조(내부사용자 비밀번호 관리)'의 위반이다. 위의 서버 Privilege 계정 운영방식의 4가지 문제점에 대하여 전자금융감독규정 및 정보보호관리체계(ISMS) 인증 통제항목에서 제시하고 있는 개선방

Table 8. Problem of Operating Privilege Account

Company	Seper -ation of Duties	Share Account Status	Accounts approval	Windows Password Change Status
Finance 1	X	X	O	O
Finance 2	X	O	X	X
Finance 3	X	O	X	O
Finance 4	X	O	X	X
Finance 5	O	X	X	X
Finance 6	X	O	O	O
Finance 7	X	X	X	O
Finance 8	X	O	O	X
Finance 9	X	O	X	O
Finance 10	X	X	X	O
Finance 11	X	O	X	O
Finance 12	O	X	O	O
Finance 13	O	X	O	O
Finance 14	X	X	X	X

Table 9. Improvement about Operating Privilege Account

Problem	- Inadequate job segregation on privilege account - Inadequate separation of Shared privilege account duties of privil-ege accounts - Insufficient of approval when usi-ng privilege account - Insufficient management of Win- dows privilege account
Improvement	- job segregation on privilege acco-unt : Regulation On Supervision of Electronic Financial Activities - Article 16(Job Segregation), ISMS 6.1.2 (Job Segregation). - Separation of duties privilege ac- count Prohibition of sharing priv-ilege account : Regulation On Supervision of Electronic Financ-ial Activities - Article 13(Electr-onic data protection measures), ISMS 10.3.2 (User Identification) - Necessity of approval when priv-ilege account is used and Records Management of Personal History. : Regulation On Supervision of Electronic Financial Activities - Article 13(Electronic data prot-ection measures), ISMS 10.3.2 (U-ser Identification) - Strengthening management of Wi- ndows privilege account (ex: Pe-riodic password changes) : Regu-lation On Supervision of Electro-nic Financial Activities - Article 32(Internal user password mana-gement), ISMS 10.3.3(User Pass-word Management)

안은 Table 9.와 같다. 많은 금융회사들은 업무편의, 운영상의 이유로 문제점에 대한 개선이 미흡했다. 하지만 전자금융감독규정 및 정보보호관리체계(ISMS) 인증 통제항목에서 명시하고 있는 개선방안을 적용해야 법규를 준수하고, Privilege 계정을 안전하게 운영할 수 있다.

IV. Privilege 계정 운영방식 의사결정 모델

농협 전산망 해킹 사건 이후 금융회사 서버 Privilege 계정의 운영방식을 상기에서 조사한 결과 3가지 방식 중 하나의 방식으로 운영하고 있음을 설문과 FGI를 통해서 파악할 수 있었다. Ⅳ장에서는 3가지 운영방식을 합리적으로 선택 할 수 있도록 AHP를 사용하여 Privilege 계정 운영방식 선정을 위한 의사결정 모델과 공식을 제시한다.

Table 10. Decision Making using AHP & Formula Deduction FLOW

Step	Flow	Contents
Pre Ana-y sis	Poll of privilege operation/ FGI	Execution of poll/ FGI on finance company privilege account operation to select evaluat- ion factors
Step 1	Selection evaluation factors/ Implementation AHP layered Model	Selection 10 kinds of evaluation fac- tors through pre- analysis/ Implem- entation of AHP layered model
Step 2	Poll of AHP layered model/ Evaluation effectiveness	- Poll using AHP layered model Calculation con- sistency rate (under 0.1) of survey data / Evaluation effe- ctiveness
Step 3	Deduction weight of evalustion facter/ alternative plan	Analyse weight of evalustion facter/ alternative plan dividing 3 groups
Step 4	Deduction of Formula to Privilege Account Operation	Deduction formula (Handmade, Self- developement, So- lution) using res- ult value of group 3

4.1 AHP를 사용한 의사결정 모델과 공식 도출 절차 구성

AHP를 사용한 의사결정 모델과 공식 도출 절차는 Table 10.과 같이 4단계로 진행한다. 1단계 에서는 Privilege 운영방식의 의사결정을 위한 평가 요인 선정과 AHP 계층 모델을 설계한다. 2단계에서는 1단계에서 선정된 의사결정 요인들 간의 쌍대비교를 통해 얻어진 가중치가 논리적인 일관성을 유지하는지 알아보기 위하여 유효성 평가를 실시한다. 3단계에서는 평가 요인별 가중치 및 대안별 가중치 도출하고, 4단계에서는 3단계에서 도출한 평가 요인 가중치와 대안별 가중치에 대한 AHP 민감도 분석을 통해 3가지 방식의 공식을 도출한다.

4.2 1단계 : 평가 요인 선정 및 AHP 계층 모델 구현

AHP 사용을 위해 첫 번째로 Privilege 운영방식을 결정하는 평가 요인을 선정한다. 평가 요인 선정은 상기설문과 국내 14개 금융회사 Privilege 계정담당자 14명을 대상으로 FGI를 통해 10가지 요인을 선

Table 11. Evaluation Factors for Selecting Operation of Privilege Account

Top Rating	Lower Rating	Definition
Cost	Purchase	Purchase Costs of Privilege Account Operation
	Mainten- ance	Maintenance Costs of Pri- vilege Account Operation
	Labor	Labor Costs of Privilege Ac- count Operation
Business efficiency	Processing speed	Processing speed of cha- nging privilege account pas- sword
	Operat- ing Conven- ience	Operating Convenience of privilege account user
	Response	Efficiency of lesion response
Risk	Compli- ance with Laws	Whether Laws on Privilege Account is Complied
	Security	Risk of privilege account le- akage etc.
	Occurre- nce of Lesion	Risk on occurrence of lesion in operating privilege account
	Occurre- nce of Error	Risk of error when changing privilege account password

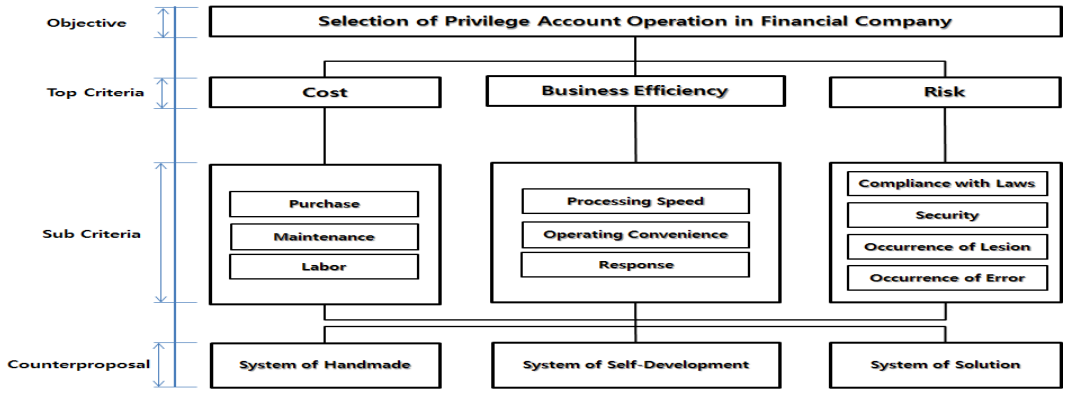

Fig. 2. AHP Layered Model for Selecting Operation of Privilege Account

정할 수 있었고, 선정된 10가지 요인은 Table 11.과 같이 상위평가와 하위평가 2단계로 분류되고, 상위평가는 비용, 업무효율성 및 위험으로 분류되고, 하위평가는 구매비용, 유지보수 비용, 인건비, 업무처리속도, 운영편의, 장애대응, 법률준수, 보안성, 장애발생 및 오류발생으로 분류된다. Table 11.에 제시된 2단계 평가기준을 기초로 Fig 2.와 같이 서버 Privilege 계정 운영방식 선정을 위한 AHP 계층 모델을 구축하였다. AHP 계층 모델은 서버 Privilege 계정 운영방식을 변경 또는 현 운영방식의 적정성을 검토하기 위한 기업에 가장 적합한 운영방식을 선정하는 것을 목적으로 한다. 상위평가 기준 간의 쌍대비교, 하위평가 기준 간의 쌍대비교 및 하위평가 평가기준에 대한 3가지 대안간의 쌍대비교를 통해 각 대안의 우선순위 점수를 도출하게 된다.

4.3 2단계 : AHP 계층 모델 설문조사 및 유효성 평가

Fig 2.에서 제시된 AHP 계층 모델을 바탕으로 설문지를 구성하고, 금융회사 Privilege 계정 담당자와 보안 컨설팅 전문가 2개의 그룹을 대상으로 9점 척도로 평가하는 설문지를 배포하고 회수하는 방식을 사용하여 쌍대비교를 수행한다. 쌍대비교를 통해 도출된 가중치가 논리적으로 일관성을 유지하는지 검증하기 위해 Saaty[15]가 개발한 '일관성 비율(CR, Consistency Ratio)'을 사용한다. Saaty[15]에 따르면 일관성 비율이 0.1이하일 때 쌍대비교행렬은 일관성이 있다고 제시하였다. 따라서 일관성 비율이 0.1 미만일 경우 일관성을 유지한다고 평가하여 분석대상에 포함하고, 일관성이 없는 0.1이상인 설문지의 경우 비합리적이라 평가하여 분석대상에서 제외한다. 그 결과 금융회사 Privilege 계정 담당자 설문 14부 중 일관성을 유지한 11부, 보안컨설팅 전문가 16부 중 일관성을 유지한 11부 총 22부의 설문지를 활용한다. 이를 Expert Choice 2000 소프트웨어를 이용하여 분석하고, 복수의 평가에 대한 결과를 종합하기 위해 Saaty[15]가 검증한 행렬의 역수성을 유지하는 기하평균(geometric mean)을 활용한다[9].

4.4 3단계 : 평가 요인별, 대안별 가중치 도출

본 연구에서는 AHP 모델을 적용하여 Saaty[15]가 제시한 일관성비율(CR)이 0.1이하인 설문지만 신뢰성 있는 설문지로 분류하고, Fig 2.처럼 AHP 계층 모델을 통해 10가지의 주요 평가 요인들에 대해 3개의 그룹으로 쌍대비교를 실시한다. 그룹의 구성은 그룹1. Privilege 계정 담당자, 그룹2. 보안컨설팅 전문가, 그룹3. Privilege 계정 담당자와 보안컨설팅 전문가로 구성하였다.

4.4.1 그룹1 결과

Table 12.는 그룹1의 평가 요인별 가중치를 계층별로 정리한 것이다.

상위평가는 위험(0.603), 업무효율성(0.315), 비용(0.082) 순위로 가중치가 분석되었고, 각 평가 요인들에 대한 최종 가중치는 상위평가의 가중치 값과 각 하위평가의 가중치를 값을 곱하여 계산되는데 최종가중치 산정 결과, 장애발생과 장애대응이 우선순위 1번, 2번으로 우선 순위를 높게 평가했다.

Table 13.은 Table 12.의 그룹1의 기준으로 도출된 평가 기준별 가중치를 바탕으로 3가지 대안의

Table 12. Weight of Group 1 Evaluation Factors

Top Rating	Weig-ht	Low Rating	Weig-ht	Final Weight	Priori-ties
Cost	0.082	Purchase	0.400	0.0328	8
		Maintenance	0.200	0.0164	10
		Labor	0.400	0.0328	8
Efficie-ncy	0.315	Processing speed	0.149	0.0469	7
		Operating Convenience	0.160	0.0504	6
		Response	0.691	0.2177	2
Risk	0.603	Compliance with Laws	0.225	0.1357	4
		Security	0.297	0.1790	3
		Occurrence of Lesion	0.377	0.2273	1
		Occurrence of Error	0.100	0.0603	5

Table 13. Weight of Standard Alternatives about Group 1

Top Rating	Lower Rating	Final Weight	Handm-ade	Self-Devlopment	Solution
Cost	Purchase	0.0328	0.021	0.013	0.003
	Mainte-nance	0.0164	0.011	0.004	0.001
	Labor	0.0328	0.004	0.012	0.021
Cost Total		0.082	0.036	0.029	0.025
Effici-ency	Process-ing speed	0.0469	0.003	0.013	0.030
	Operating Conven-ience	0.0504	0.033	0.030	0.007
	Response	0.2177	0.141	0.056	0.017
Efficiency Total		0.315	0.177	0.099	0.054
Risk	Complianc e with Laws	0.1357	0.010	0.035	0.088
	Security	0.1790	0.014	0.046	0.116
	Occurre-nce of Lesion	0.2273	0.147	0.038	0.016
	Occurre-nce of Error	0.0603	0.007	0.023	0.039
Risk Total		0.6023	0.178	0.142	0.259
Alternatively final weight			0.391	0.271	0.338
Alternatively the final priorities			1	3	2

우선순위를 산출한 결과를 나타낸 것이다. 대안의 최종 가중치는 수작업(0.391), 솔루션(0.338), 자체개발 (0.271)로 수작업 방식이 가장 적합한 대안으로 선정되었다. 분석 결과를 보면 비용, 업무효율성 측면에서는 수작업(0.036, 0.177), 위험측면에서는 솔루션(0.259)이 가중치가 높게 도출되었다. 그룹1의 분석결과는 법률준수, 보안성 측면보다, 장애발생, 장애대응 측면이 높아 다소 의외의 결과가 나타났고, 이 때문에 Privilege 계정 담당자는 솔루션을 도입함으로서의 솔루션의 장애발생과 장애대응 지연에 따른 문제점이 보안성, 법률준수 측면보다 높게 평가되어 솔루션 방식보다 수작업 방식을 최종 우선순위로 선정 되었다.

4.4.2 그룹2 결과

Table 14.는 그룹2의 평가 요인별 가중치를 계층별로 정리한 것이다. 상위평가에는 위험(0.604), 업무효율성(0.326), 비용(0.070) 순위로 가중치가 분석되었고, 최종가중치 값을 보면 법률준수와 보안성의 우선순위가 높게 평가했다.

Table 15.는 Table 14.의 그룹2의 기준으로 도출된 평가 기준별 가중치를 바탕으로 3가지 대안의 우선순위를 산출한 결과를 나타낸 것이다. 대안의 최종 가중치는 솔루션(0.419), 수작업(0.308), 자체개발(0.273)로 솔루션 방식이 가장 적합한 대안으로 선정되었다. 분석 결과를 보면 비용 측면에서는 자체

Table 14. Weight of Group 2 Standard Evaluation Factors

Top Rating	Weight	Low Rating	Weight	Final Weight	Priori-ties
Cost	0.070	Purchase	0.455	0.0318	8
		Mainten-ance	0.455	0.0318	8
		Labor	0.091	0.0064	10
Effici-ency	0.326	Processing speed	0.117	0.0381	7
		Operating Convenience	0.200	0.0652	4
		Response	0.683	0.2226	3
Risk	0.604	Compliance with Laws	0.400	0.2416	1
		Security	0.400	0.2416	1
		Occurrence of Lesion	0.100	0.0604	5
		Occurrence of Error	0.100	0.0604	5

Table 15. Weight of Alternatives about Group 2

Top Rating	Lower Rating	Final Weight	Handm-ade	Self-Devlo-pment	Solution
Cost	Purchase	0.0318	0.021	0.021	0.004
	Mainte-nance	0.0318	0.021	0.021	0.004
	Labor	0.0064	0.001	0.002	0.004
Cost Total		0.0700	0.043	0.044	0.012
Effici-ency	Processing speed	0.0381	0.003	0.010	0.025
	Operating Conven-ience	0.0652	0.042	0.025	0.007
	Response	0.2226	0.144	0.043	0.017
Efficiency Total		0.3259	0.189	0.078	0.049
Risk	Compli-ance with Laws	0.2416	0.016	0.064	0.157
	Security	0.2416	0.017	0.060	0.157
	Occurr-ence of Lesion	0.0604	0.039	0.012	0.005
	Occurr-ence of Error	0.0604	0.005	0.016	0.039
Risk Total		0.6040	0.077	0.152	0.358
Alternatively final weight			0.308	0.273	0.419
Alternatively the final priorities			2	3	1

개발(0.044), 업무효율성 측면에서는 수작업(0.189), 위험측면에서는 솔루션(0.358)이 가중치가 높게 도출되었다. 그룹2의 분석결과는 Privilege 계정 담당자와 동일하게 상위계층은 위험, 업무효율성, 비용 순으로 가중치를 평가하였으나, 각 요인별 최종 가중치는 보안성, 법률준수가 높아 Privilege 계정 담당자와 상이한 결과가 도출되었다. 이러한 상이한 결과는 보안컨설팅 담당자는 솔루션 운영 시 장애발생, 장애대응 보다 법률준수와 보안성을 높게 평가하여 수작업 방식보다 솔루션 방식을 최종 우선순위로 선정되었다.

4.4.3 그룹3(그룹1+그룹2) 결과

그룹1에서는 '장애발생', '장애대응'의 우선순위가 높게 평가되었으며, 그룹2에서는 법률준수와 보안성의 우선순위가 높게 평가되었다. 금융회사 서버 Privilege 계정 운영방식 결정 시 비용, 업무효율성, 위험 측면이 적절하게 고려된 모델을 수립하기 위해 그룹1과 그룹2를 기하평균 하였다. Table 16.은 그룹1과 그룹2의 값을 기하평균한 평가 요인별 가중치를 계층별로 정리한 것이다. 상위평가에는 위험(0.603), 업무효율성(0.315), 비용(0.082) 순위로 가중치가 분석되었고, 최종가중치 값을 보면 보안성이 우선순위 1번으로 가장 높고 장애대응 요인, 법률준수 요인 순으로 우선순위를 높게 평가했다.

Table 17.은 Table 16.의 그룹3의 기준으로 도출된 평가 기준별 가중치를 바탕으로 3가지 대안의 우선순위를 산출한 결과를 나타낸 것이다.

대안의 최종 가중치는 솔루션(0.425), 수작업(0.314), 자체개발(0.261)로 솔루션 방식이 가장 적합한 대안으로 선정되었다. 분석 결과를 보면 비용 측면에서는 솔루션(0.032), 업무효율성 측면에서는 수작업(0.180), 위험측면에서는 솔루션(0.339)이 가중치가 높게 도출 되었다.

Table 16. Weight of Standard Evaluation Factors about Group 3

Top Rating	Weight	Low Rating	Weight	Final Weight	Priori-ties
Cost	0.082	Purchase	0.297	0.024	9
		Mainten-ance	0.163	0.013	10
		Labor	0.540	0.044	8
Effici-ency	0.315	Processing speed	0.149	0.047	7
		Operating Convenie-nce	0.160	0.050	6
		Response	0.691	0.217	2
Risk	0.603	Compliance with Laws	0.342	0.206	3
		Security	0.383	0.230	1
		Occurrence of Lesion	0.168	0.101	4
		Occurrence of Error	0.107	0.064	5

Table 17. Weight of Standard Alternatives about Group 3

Top Rating	Lower Rating	Final Weight	Handm-ade	Self-Devlo-pment	Solution
Cost	Purchase	0.024	0.016	0.010	0.002
	Mainte-nance	0.013	0.009	0.005	0.001
	Labor	0.044	0.004	0.016	0.029
Cost Total		0.081	0.029	0.031	0.032
Effici-ency	Process-ing speed	0.047	0.003	0.013	0.031
	Operat-ing Conven-ience	0.050	0.033	0.020	0.006
	Response	0.217	0.144	0.043	0.017
Efficiency Total		0.314	0.180	0.076	0.054
Risk	Compli-ance with Laws	0.206	0.014	0.056	0.136
	Security	0.230	0.017	0.058	0.153
	Occurr-ence of Lesion	0.101	0.067	0.017	0.007
	Occurr-ence of Error	0.064	0.006	0.023	0.043
Risk Total		0.601	0.104	0.154	0.339
Alternatively final weight			0.314	0.261	0.425
Alternatively the final priorities			2	3	1

4.5 4단계 : Privilege 계정 운영방식 선정을 위한 공식 도출

Table 18.의 공식은 3단계에서 도출된 그룹3의 상위평가 요인 가중치와(Table 16.), 대안별 가중치(Table 17.)를 바탕으로 Expert Choice 2000 프로그램의 민감도 분석 기능을 이용하여 비용, 업무효율성, 위험의 상수 값을 도출한다. 이 상수 값을 이용하여 서버 Privilege 계정 운영방식 선정을 위한 공식을 도출한다.

Table 19.는 그룹3 상위평가 요인 가중치(0.082, 0.315, 0.603)와 그룹3 기준 대안별 가중치(31.4%, 26.1%, 42.5%)를 바탕으로 Table 18.의 공식에 적용하여, Privilege 계정 운영방식 산정에 대한 공식을 검증하였다.

Table 18. Selection Criteria Formula of Privilege Account Operations

Operating	Formula
Handmade	$M = (31.5 \times C) + (58.3 \times E) + (17.3 \times R)$
Self-Dev-elopment	$D = (33.7 \times C) + (24.0 \times E) + (26.1 \times R)$
Solution	$S = (35.2 \times C) + (17.5 \times E) + (56.7 \times R)$

M : Weight of Handmade
D : Weight of Self-Development
S : Weight of Solution
C : Weight of Cost
E : Weight of Business Efficiency
R : Weight of Risk

4.6 사례를 통한 의사결정 모델과 공식 검증

본 연구에서는 A금융회사의 사례를 통해 의사결정 모델과 공식을 적용하여 검증한다.

Privilege 계정 의사결정은 Table 20.과 같이 3단계 과정을 통해 검증된다.

Table 19. Group3. Verification Formula using Result Value

Operant-ing	Cost		Business Efficiency		Risk		Total	Priorities	Operanting
	Consta nt	Weight	Con-s tant	Weight	Con-st ant	Weight			
Handm-ade	31.5	0.082	58.3	0.315	17.3	0.603	31.4%	2	Solution
Self-De-elopment	33.7		24.0		26.1		26.1%	3	
Solution	35.2		17.5		56.7		42.5%	1	

Table 20. 3-Steps of Privilege Account Decision Making

[Step 1] Calculate importance factor Importance calculation is from 1 to 9 points on 10 kind of factors in Table 11. [Step 2] Calculate weight of top standard Calculate weight of importance factors (Cost, Business Efficiency, Risk) using Step 1. [Step 3] Calculate alternative weight use Formula Calculation of weight each operations applying Formula(Table 18.)

1단계는 Table 21.과 같이 10개의 평가 요인의 중요도를 Table 22. 기준으로 1점~9점 평가한다. 2단계는 Table 21.의 중요도 평가 데이터를 사용하여 Table 23.과 같이 비용, 업무효율성, 위험 평균값 계산 후 가중치를 산정한다. A금융회사는 위험의 가중치가 가장 높았다. 3단계 산정된 가중치를 Table 18.의 운영방식별 공식을 적용하여 Table 24.와 같이 솔루션 운영방식이 37.1%로 가중치가 도출되었다.

A금융회사는 수작업 방식으로 Privilege 계정 운영을 하고 있지만 이 결과를 참고하여 Privilege 계정 운영방식에 대한 변경을 고려하고 있다.

본 연구에서 제시한 의사결정 모델과 공식을 적용하면 각 금융회사의 상황에 적합한 서버 Privilege 계정 운영방식 선정을 합리적으로 할 수 있다.

Table 21. Importance Rating of Privilege Account about "A" Financial Company Privilege

Top Rating	Lower Rating	Importance(1~9)								
		1	2	3	4	5	6	7	8	9
Cost	Purchase				√					
	Maintenance				√					
	Labor						√			
Efficiency	Processing speed							√		
	Operating Convenience									√
	Response									√
Risk	Compliance with Laws									√
	Security									√
	Occurrence of Lesion								√	
	Occurrence of Error									√

Table 22. Measure the Relative Importance

Measure	Definition
1	Not Important
3	Some Important
5	Important
7	Very Important
9	The Most Important
2, 4, 6, 8	Median of Determine the 2 Adjacent

Table 23. Top calculation based on weight about "A" Financial Company

Cost		Efficiency		Risk	
Average	Weight	Average	Weight	Average	Weight
4.67	0.215	8.33	0.383	8.75	0.402

Table 24. Result of Operating Privilege Account Applying the Formula at "A" Financial Company

Operanting	Cost		Efficiency		Risk		Total	Priorities
	Constant	Weight	Constant	Weight	Constant	Weight		
Handmade	31.5	0.22	58.3	0.38	17.3	0.40	36.1	2
Self-Devlopment	33.7		24.0		26.1		26.9	3
Solution	35.2		17.5		56.7		37.1	1

V. 결 론

2011년 4월 농협 전산망 해킹 사고 이후 서버 Privilege 계정의 중요성이 제고되었고, 감독기관의 규제가 강화되었다. 그러나 2014년 4월 농협 전산망 해킹 사고 이후의 서버 Privilege 운영방식 현황을 분석한 결과, 법규 미준수 등의 4가지 문제점이 도출되었다. 도출된 문제점에 대해 전자금융감독규정 및 정보보호관리체계(ISMS)인증 통제항목에서 명시하고 있는 Privilege 계정관리 직무분리, Privilege 계정 공유 금지, Privilege 계정 사용 시 승인 후 개인별 사용내

역을 기록·관리 및 Windows Privilege 계정 관리강화의 4가지 개선방안을 제시하였다. 이러한 개선방안 적용은 법규준수 및 Privilege 계정 운영 미흡으로 발생할 수 있는 보안사고를 사전에 예방할 수 있다.

또한, 운영방식을 합리적으로 선택 할 수 있도록 금융회사 서버 Privilege 운영방식 현황 조사를 통해 서버 Privilege 운영방식 선정을 위한 10개의 평가 요인을 선정하였다. 선정된 요인을 AHP를 사용하여 비용, 업무효율성, 위험의 3가지 상위기준으로 분류하여 합리적으로 운영방식을 선택 할 수 있는 서버 Privilege 계정 의사결정 모델을 제시하고, 이를 기반으로 공식을 도출하였다. 실제 A금융회사 사례를 바탕으로 제시된 의사결정 모델과 공식은 Privilege 계정 의사결정 3단계 과정을 통해서 검증하였다. Privilege 계정관리가 중요함에도 불구하고 현재까지 Privilege 계정 운영방식을 결정하기 위한 연구나 가이드가 제시되고 있지 않다. 따라서 본 연구에서 제시한 모델과 공식은 서버 Privilege 계정 운영방식을 변경 또는 현 운영방식의 적정성을 검토하고 있는 금융회사에 유용하게 활용될 수 있다. 구매비용, 유지보수 비용, 인건비, 업무처리속도, 운영편의, 장애대응, 법률준수, 보안성, 장애발생 및 오류발생의 10가지 평가기준을 바탕으로 회사 및 조직이 추구하는 중요도에 맞는 적합한 Privilege 계정 운영방식을 결정할 수 있다.

또한, 본 연구에서 제시한 Privilege 계정 운영방식의 4가지 개선안과 Privilege 의사결정 모델 및 공식 활용은 금융회사 뿐만 아니라 대규모 서버를 운영하는 일반기업에도 유용하게 활용될 수 있다.

References

[1] Ye Jin, Jang, "Overview of NH Bank Cyber Attack ", AP. "http://ne-ws.donga.com/3/all/20110503/36898474/1#," 3. Mar. 2011.

[2] Sang Jin, Jang, "NH Bank Computer Network Password Was '1' and '0000'. ", The Cho-sun Ilbo, "http://news.cho-sun.com/site/data/html_dir/2011/04/20/2011042002347.html," 20 .April. 2011.

[3] Financial Services Commission, "Enfor-cement Bylaws of Regulation On Supe-rvision of Electronic Financial Activiti-es," Sep. 2009.

[4] Financial Services Commission, "Regu-lation On Supervision of Electronic Fi-nancial Activities," June. 2010.

[5] Sang-hyun Lee, "Identity and Access management of information systems r-esearch on how to strengthen," Dongg-uk University , Aug. 2012

[6] Byung-eon Park, "An integrated appro-ach for identity and access manageme-nt for efficient administrative work," *Jonornal of The Korea Institute of inf-ormation Security & Cryptology*, v.25, no.1, pp.165-172, Feb. 2015

[7] Young-seok Cho, "A Study on Decision Making Process of System Access Ma-nagement," *Jonornal of The Korea Ins-titute of information Security & Cryp-tology*, v.25, no.1, pp.225-235, Feb. 2015.

[8] Yang-hyun, Kwon, "Study on access control model for the environment of smart grid sys-tem," Pusan National University, Feb. 2013.

[9] Sang-Pil Shin, "An analytic hierarchy process (AHP) approach to selection of implementation mode of mobile office system," Seoul National Univetsity of Science and Technology, July. 2013.

[10] Seokung Yoon, "Factor analysis of VoIP Security Checklists using AHP," *Jonornal of The K-orea Institute of information Security & Cry-ptology*, v.22, no.5, pp.1115-1122, OCT. 2010.

[11] Dong-wook Kim, "A Study on Informa-tion Security Policy in the era of Sma-rt Society," *Jonornal of The Korea Ins-titute of information Security & Cryp-tology*, v.22, no.4, pp.883-899, Aug. 2012.

[12] Kihoon Sung, "A Study on Threat fact-ors of Information Security in Social Network Service by Analytic Hierarchy Process," *Jonornal of The Korea Instit-ute of information Security & Cryptol-ogy*, v.20,

no.6, pp.261-270, Dec. 2010.
〔13〕 Yong-Wook Chung, "The weight analysis research in developing a similarity classification problem of malicious code based on attributes," *Jonornal of The Korea Institute of information Security & Cryptology*, v.23, no.3, pp.501-514, June. 2013.
〔14〕 Young-Jin Shin, "A Study of Priority or Policy Implement of Personal Info-mation Security in Public Sector: Foc-sed on Personal Information Security Index," *Jonornal of The Korea Institut of information Security & Cryptology*, v.22, no.2, pp.379-390, Apr. 2012.
〔15〕 Saaty T. L., "The Analytic Hierarchy ro-cess," McGraw-Hill, New York, 1980.
〔16〕 Hodong Kim , "A Study on Password Management for Improving Efficiency about Information Security Check Ser-ice," Konkuk University, Jan. 2009.
〔17〕 Gwansik Yoon, "Design and implemenatio-n of an access control system in martwor-k environment," Ajou University, Jan, 2013.
〔18〕 Yonghan Lee, "A flexible access control model for complex business applicatio-ns," Korea University, Jun. 2012.
〔19〕 Sunho Jo, "A Study on the Selection Method of Water Supply System in Apartment House in using AHP", Dong-Eui University, Feb, 2014

〈저자소개〉

이 석 원 (Suk-Won Lee) 정회원
2006년 2월: 인하대학교 정보통신학과 졸업
2014년 3월 ~ 현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 정보보호 정책, 위험관리

이 경 호 (Kyung-Ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사 졸업
2009년 8월: 고려대학교 정보경영대학원 박사 졸업
1994년 2월 ~ 2013년 12월 : 삼성그룹, 네이버(주), 시큐베이스 등 근무
2011년 9월 ~ 현재 : 고려대학교 정보보호대학원 조교수, 부교수
〈관심분야〉 위험관리, 정보보호 컨설팅, 정보보호 및 개인정보보호정책