Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.6, Dec. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.6.1437

개인정보 오남용 예방을 위한 정보보호정책 개선에 관한 연구 : 금융회사의 개인정보 오남용 모니터링 결과 중심으로

김 영 호,† 김 인 석‡
고려대학교 정보보호대학원

A Study on the Improvement of Information Protection Policy to Prevent the Misuse of Personal Information : Based on the Results of the Monitoring Personal Information Misuse in Financial Companies

Young-ho Kim,† In-seok Kim‡
Graduate School of Information Security, Korea University

요 약

각종 개인정보 유출사고를 계기로 정부에서는 강화된 개인정보보호 대책을 시행하였고, 금융회사들은 정부 대책에 의거 개인정보 오남용 여부를 주기적으로 점검하는 등 노력을 기울이고 있지만 개인정보 오남용 문제는 여전히 개선되지 않고 있는 실정이다. 본 연구는 금융회사 직원을 대상으로 개인정보 오남용 모니터링 시스템을 이용한 현장실험 결과를 분석하여 오남용 문제 개선방안을 제시하고자 한다. 특별억제이론에 기반하여 오남용 행위자를 조치 하는 방법에 따른 오남용 방지 효과를 확인하고, 오남용 행위자들의 담당업무 및 근속연수와 오남용 행위 간의 관련성을 분석하였다. 분석결과를 바탕으로 제시하는 개선방안들이 실효성 있는 정책수립에 활용되기를 기대한다.

ABSTRACT

As a result of various personal information leakage incidents, the government implemented enhanced privacy protection measures, and financial companies are making efforts to periodically check whether personal information is misused according to government measures, but the problem of misuse of personal information is still not improved. The purpose of this study is to analyze the results of field experiments using the monitoring system for misuse of personal information and to suggest ways to improve the misuse problem. Based on the specific deterrence theory, this study examined the effects of misuse prevention according to the method of dealing with misusers, and analyzed the relationship between the duties of misusers and their years of service and misuse. It is expected that the analysis results of this study will be used for effective policy establishment.

Keywords: Privacy, personal information misuse monitoring, performance of information protection, deterrence theory, information protection policies

Received(09. 16. 2019), Modified(11. 05. 2019), Accepted(11. 05. 2019)

† 주저자, capella005@gmail.com
‡ 교신저자, iskim11@korea.ac.kr(Corresponding author)

I. 서 론

2014년 1월 신용카드 3사의 대규모 개인정보 유출 사고를 계기로 정부에서는 관계부처 합동으로 “금융분야 개인정보 유출 재발방지 종합대책”을 마련하였고, 개인정보 보호 관련 법과 정책들이 보완되거나 새로 도입되었다[1]. “금융분야 개인정보 유출 재발방지 종합대책(관계부처 합동)”은 개인정보의 수집부터 파기까지 단계별 정보보호 강화, 자기정보결정권 등 신용정보 주체의 권리보장 강화, 임원책임 확대 및 엄정한 제재 등 금융회사 책임 강화, 금융권 사이버 안전 대책 강화 등 정보보호·보안 강화와 예방조치 강화 등을 주요 내용으로 한다. 또한, 신용정보의 이용 및 보호에 관한 법률 및 신용정보업감독규정은 신용정보관리·보호인이 신용정보 유출 등을 방지하기 위한 내부통제시스템을 구축하고 운영하도록 하고 있으며, 이에 따라 각 금융회사들은 개인신용정보의 유출 및 오남용 여부에 대한 점검을 수행하여야 한다.

카드 3사의 대형 유출사고 이후 개인정보의 유출 사고는 감소 추세이긴 하지만, 개인정보침해신고센터를 통하여 접수되는 유형을 보면 개인정보의 오남용에 해당하는 ‘개인정보의 목적 외 이용’ 및 ‘주민등록번호 등 다른 사람 정보의 훼손·침해·도용’ 은 지속적으로 큰 비중을 차지하고 있는 것으로 나타나 개인정보의 오남용 문제는 여전히 개선되지 않고 있음을 알 수 있다[2]. 최근 금융 감독당국에서는 개인정보의 유출 및 오남용 관련하여 점검이나 관리를 소홀히 한 금융회사에 대해 중징계 조치하는 등 감독을 강화하고 있는 추세이다. 이에 따라 각 금융회사들도 자체 점검을 더욱 강화할 것으로 보이며, 개인정보 오남용을 모니터링 할 수 있는 시스템의 구축과 운영에도 더욱 관심을 가질 것으로 예상된다.

본 연구에서는 개인정보 오남용 모니터링이라는 기술적 수단을 통한 개인정보 오남용 행위 억제효과를 살펴보고, 조직 구성원들의 인적 · 업무적 요인들과 개인정보 오남용 행위 간의 연관성을 확인한다. 모니터링 결과에 대한 분석을 통해 개인정보 오남용 문제를 개선하기 위한 방안을 제언하고자 한다.

II. 관련연구

개인정보 유출 및 오남용을 탐지하기 위한 효율적인 수단인 모니터링 시스템에 대한 연구는 그 동안 기술적으로 정밀한 모니터링 방법을 찾기 위한 방향으로 진행되어 왔다. 다양한 보안 솔루션에서 생성되는 로그들을 효율적으로 분석할 수 있는 단일 및 복합 시나리오를 통한 시스템 구성방법이나[3], 육하원칙(5W1H) 중 Why를 제외한 4W1H에 의거한 위협요소 분류 및 탐지 건에 대한 소명 프로세스 모듈 등은 본 연구에서 사용된 모니터링 시스템에도 반영되어 있는 요소들이다[4].

그러나, 대부분의 개인정보 오남용 모니터링 시스템에 대한 선행 연구들은 로그 데이터 수집방법이나 시스템 구성 방법, 시나리오 설계 방법 등 시스템을 구축 운영하기 위한 기술적 방법 연구에 그쳤다는 한계가 있으며, 모니터링 시스템을 구축하는 근본 목적인 개인정보 오남용 억제 효과를 체계적으로 분석한 연구자료는 찾을 수 없었다.

2.1 억제이론(Deterrence Theory)

개인정보 오남용 여부를 모니터링하고 오남용 행위자를 조치함으로써 조직 구성원들의 개인정보 오남용 행위를 방지 할 수 있을 것이라는 것은 억제이론으로 설명된다. 억제이론은 인간은 합리적이면서 경제적인 선택을 하는 존재라는 것을 전제로 범죄에 의한 이익이 처벌에 따른 고통보다 클 경우에 범죄가 발생하며 처벌의 고통이 범죄로 얻게되는 이익보다 클 경우에는 범죄가 일어나지 않는다는 이론이다.

이러한 억제이론은 주로 범죄예방 관련으로 연구되어 왔다. 연성진(2003)은 전국 13개 교도소의 수형자 943명을 대상으로 설문조사를 실시하여 처벌이 범죄억제에 미치는 영향을 연구하였는데, 억제이론을 배경으로 범죄자 처벌이 실제로 범죄억제라는 목적을 달성하고 있는지를 연구하였다[5]. 정철우, 장명순(2011)은 억제이론을 바탕으로 음주운전과 교통안전교육의 관계를 연구하였다[6]. 교통안전교육에 따른 음주운전 재범 억제효과를 분석하여 교통안전 교육이 음주운전을 억제시키는 요인으로 작용하고 있으며, 강의식 교육보다는 토론 및 체험식 교육이 효과적이라는 결론을 도출하였다[6].

정보보호 분야에서도 억제이론을 배경으로 한 다수의 연구가 진행된 바 있다. 안중호, 박준형, 성기문, 이재홍(2010)은 정보보안 예방방법으로서 윤리교육과 처벌이 조직유형에 따라 어떤 영향을 미치는가를 연구함으로써 정보보안을 추구하기 위한 조직구성원의 행위 변화와 자기통제를 이끌어내는 방법을 찾고자 하였다[7]. 이도연(2017)은 특정 조직의 직

원들을 대상으로 스팸메일 모의훈련 시스템을 이용한 현장실험 연구를 수행하였는데, 교육의 억제효과와 처벌의 특별 억제효과를 실증적으로 연구하여, 조직 유형과 직급이 정보보호 교육과 처벌의 효과에 영향을 미친다는 것을 확인 하였다[8].

억제이론은 각종 정보보호 정책(교육, 처벌 등)이 정보보호 준수 의도나 행동에 미치는 영향에 관한 연구들의 대표적인 이론적 배경이며[9], 본 연구에서 사용한 개인정보 오남용 모니터링도 개인정보를 업무 목적 외로 이용하여서는 안 된다는 정보보호 정책을 위반한 직원을 억제하는 수단에 해당한다. 억제이론은 일반억제와 특별억제로 나누어 볼 수 있는데 일반억제는 다른 사람이 처벌받는 것을 보고 동일한 범죄 발생이 억제되는 것이고, 특별억제는 본인의 처벌경험을 통해 향후 범죄의 재발을 억제하는 것이다. 개인정보 오남용 행위를 탐지할 수 있는 모니터링 시스템으로 오남용 행위를 신속하게 발견하고 행위자에 대한 적절한 조치를 취한다면, 오남용 행위자가 오남용 행위를 반복하지 못하도록 하는 특별 억제효과를 가지게 된다.

본 연구에서는 개인정보 오남용 모니터링이 얼마나 조직 구성원들의 오남용 행위 억제에 영향을 미쳤는가를 실제 행동 변화를 측정함으로써 모니터링의 특별 억제효과를 확인하고자 한다. 특별억제효과를 연구하는 방법에 있어서 그 동안 주로 사용되었던 스팸메일 모의훈련이나 정보보호교육이 아닌 개인정보 오남용 모니터링을 도입하였기 때문에 특별 억제이론에 대한 새로운 연구방법론을 제시하였다는 점에서 학술적 가치를 지닌다.

III. 연구설계

3.1 가설설정 및 연구모형

3.1.1 오남용 행위자 조치

연성진(2003)은 범죄에 대한 확실하고(certain) 엄격한(severe) 처벌은 개인에게 범죄를 저지르지 않도록 하는 억제효과가 있다고 하였다[5]. 처벌의 확실성(certainty)과 엄격성(severity)에 따라 범죄발생 억제효과가 달라질 수 있다는 것은 모니터링에 있어서도 오남용 행위자를 조치하는 방법에 따라 오남용 행위의 재발을 방지하는 모니터링 효과가 달라질 수 있다는 의미와 같다. 본 논문에서 개인정보 오남용 모니터링의 특별 억제효과를 간략히 '모니터링 효과'라 하기로 한다.

오남용 행위자를 조치하는 방법으로 본 연구에서는 모니터링 시스템의 알림처리와 소명처리 기능을 사용한다. 알림처리는 오남용으로 탐지된 직원에게 주의조치 차원의 경고 메시지를 보내는 것이고, 소명처리는 해당 직원에게 오남용 행위가 발생한 경위 및 재발방지 확약 등이 포함된 내용을 작성토록 하는 것이다. 소명처리가 징계와 같은 처벌 수단은 아니지만, 단순 알림처리보다는 엄격한(severe) 수단이기 때문에 오남용 행위 재발방지에 더욱 효과적일 것이라 예상할 수 있다. 엄격성의 차이에 따른 특별 억제효과를 확인하기 위한 다음의 가설을 수립하였다.

가설1(H1) : 오남용 행위자를 조치하는 방식에 따라 모니터링 효과가 다르게 나타날 것이다.

3.1.2 근속연수

근속연수는 근로자가 동일 기업에서 계속하여 근무한 연수를 뜻한다. 박오원, 차종석(2019)은 근속연수와 직무성과의 관계를 설명할 수 있는 인적자본이론(human capital theory)을 배경으로 근속연수가 개인들의 성과와 태도에 미치는 효과를 규명하는 연구를 수행하였다[10]. 근속연수에 따라 개인적 변화 및 조직 환경에서의 변화가 발생하기 때문에 근속연수가 미치는 영향을 살펴보는 것은 시사하는 바가 크다. 개인적 변화로는 일반적으로 근속연수가 나이와 비례하는데, 근속연수가 길어지고 나이가 많아질수록 업무지식과 경험은 축적되지만 과거부터 행하여 온 익숙한 업무패턴이나 습관들을 바꾸거나 새로운 상황에 적응하는 것에는 어려움을 느낀다. 조직에서의 변화로는 근속연수가 길어질수록 직급이 높아지고 직급이 높아지면 업무수행에 있어서 권한이나 자율성도 함께 증가된다. 미국과 한국 문화전반에 걸쳐 억제모델을 연구한 Anat Hovav, John D`Arcy(2012)가 언급한 것처럼 한국에서는 나이가 많을수록 높은 사회적 지위를 가지는 경향이 있다[11]. 이처럼 근속연수를 통하여 확인할 수 있는 변화들이 많으므로, 본 연구에서는 정보보호 측면으로 접근하여 근속연수의 차이가 개인정보 오남용 행위에 미치는 영향을 확인하기 위한 다음의 가설을 수립하였다.

가설2(H2) : 조직 내 구성원의 근속연수에 따라 모니터링 효과가 다르게 나타날 것이다.

3.1.3 담당업무

이혜정, 유규창, 명순영(2019)에 따르면 인사관리의 기준은 크게 '사람'과 '일'로 구분할 수 있으며[12], 앞서 언급한 근속연수는 사람의 특성인 성별, 학력, 나이 등과 같이 '사람' 중심의 요소이다. 연공을 중시하였던 과거와 달리 오늘날에는 '일' 중심 요소인 직무중심의 인사관리 필요성과 관심이 증대되고 있어, 해당 연구에서는 기업의 직무중심의 인사관리가 구성원의 태도에 미치는 영향을 연구하였다[12]. 직무는 직책이나 직업상에서 책임을 지고 담당하여 맡은 사무로 정의되며, '담당업무'로 표현할 수 있다.

직급, 나이 등은 기존 연구에서 변수로 사용된 바 있지만, 담당업무를 변수로 하는 정보보호 관련 연구들은 찾기 어렵다. 그나마 최동근(2015)이 정보보호 담당자의 역할이 조직의 정보보호수준에 미치는 영향을 연구하기 위하여 정보보호담당자의 직급, 부서, 주업무, 보안업무 비중 등을 다루었는데[13], 정보보호는 담당자 혼자서 하는 것이 아니라 조직 내 모든 구성원들이 준수하여야 하는 것임을 감안할 때 정보보호담당자가 아닌 일반직원들을 대상으로 한 연구가 더 많이 진행될 필요가 있다. 이에, 본 연구에서는 일반 직원들의 담당업무와 오남용 행위와의 연관성을 살펴보기 위한 다음의 가설을 수립하였다.

가설3(H3) : 조직 내 구성원의 담당업무에 따라 모니터링 효과가 다르게 나타날 것이다.

3.1.4 연구모형

설정된 가설에 따른 연구모형은 Fig.1.과 같다. 종속변수는 특별억제 효과인 '모니터링 효과'이며, 독립변수는 특별억제요소 중 엄격성에 해당하는 '오남용 행위자 조치방법'(H1), 사람중심 요소인 '근속연수'(H2), 일 중심요소인 '담당업무'(H3)가 된다.

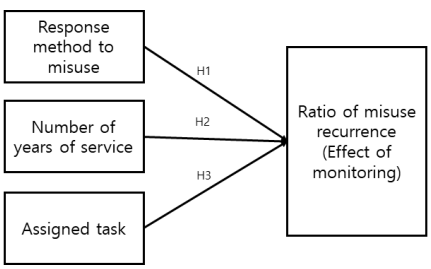

Fig. 1. Research model

3.2 모니터링 효과 측정방법

모니터링 효과를 어떠한 기준으로 볼 것이냐에 따라 측정방법은 달라질 수 있다. 개인정보 오남용 모니터링 효과에 대한 선행연구가 없기 때문에 본 연구에서는 특별억제이론에 근거하여 모니터링의 효과를 정량적으로 측정할 수 있는 모델을 Fig.2.와 같이 제시한다. 특별억제는 처벌의 경험을 통하여 범죄자가 범죄를 반복하는 것을 억제할 수 있다는 것이므로, '모니터링 효과'는 오남용 행위로 조치받은 직원이 이후 오남용 행위를 반복하는지 여부로 측정한다. 모니터링이 효과가 있다면 오남용 행위가 반복 되지 않을 것이며, 효과가 없다면 반복될 것이다.

Fig.2.의 절차 및 모니터링 효과는 아래와 같다.

① 오남용 행위를 한 직원들이 모니터링 되고, (A)

② 해당 직원에 대한 대응조치를 한다.(Fig.2.에서는 소명처리를 의미)

③ 오남용 행위가 반복된 직원을 확인한다. (B)

모니터링 효과 = (1-B/A)×100 (%)

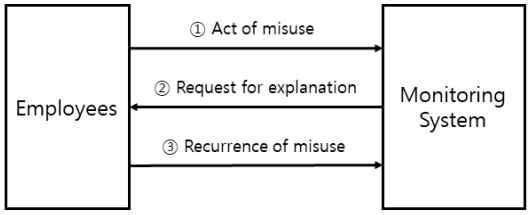

Fig. 2. Effect of monitoring measurement model

3.3 모니터링 구성

본 연구에 사용된 개인정보 오남용 모니터링 시스템은 크게 세 가지 기능으로 구성되어 있다. 각종 보안 솔루션 및 업무시스템으로부터 로그를 수집하는 기능, 수집된 로그들을 분석하고 탐지하는 탐지기능, 탐지된 내용에 대한 소명처리 등의 조치를 하는 대응기능이 있다. 어플리케이션, 서버, DB, DW 등으로부터 원천데이터 로그가 수집되면, 미리 설정된 시나리오에 의한 분석 과정을 거치게 되고, 보안담당자가 대시보드 등을 통하여 현황을 파악하고 탐지된 건에 대한 대응조치 하는 프로세스로 진행된다.

본 논문은 시스템을 구축하는 기술적 방법에 대한 연구가 아니므로 시스템 구성이나 로그수집 기능에 대해서는 별도로 언급하지 않는다. 탐지기능은 탐지 시나리오와 관련된 것이며, 대응기능은 오남용 행위

자에 대한 조치방법에 대한 것인데, 연구목적을 달성하기 위하여 다음과 같이 설계하였다.

3.3.1 탐지 시나리오 및 조치방법

오남용 의심행위를 탐지하는 시나리오를 구현하기 위하여 업무 담당자 인터뷰를 통해 비즈니스 프로세스를 파악하고, 개인정보 처리행위 주체, 행위 발생 시간, 오남용 대상, 행위 위치, 위협 요인을 4W1H 기준(WHO, WHEN, WHAT, WHERE, HOW)으로 분석하여 시나리오 구성요소를 도출하였다. 도출된 구성요소를 바탕으로 시나리오 구현의 적용성 검토 과정을 거친 후 총 41개의 탐지 시나리오를 생성하였는데, Table 1.은 개인정보 오남용 발생 가능 영역별 분류에 따른 시나리오 현황을 보여준다.

Table 1. Scenario classification

Domain	Classification	scenario count
Excessive inquiry	Peer employees information	9
	per office	1
	Retirement scheduled employees	2
	Other Office Customers	2
Inappropriate inquiry	Intensive inquiry of specific customer	2
	Out-of-business hours	1
	Not normal screen usage pattern	10
	Peer employees information	2
	Unauthorized system access	1
	Self information	1
	Customer information	5
Print	Excessive print of documents	1
Retention	Excessive retention of documents	1
Send	Excessive sending of documents	1
Move	Excessive move of documents	1
Decryption	Excessive decryption of documents	1
Total		41

모니터링으로 탐지된 직원들에 대해서는 알림처리와 소명처리의 두 가지 방법으로 대응한다. 3.1.1 오남용 행위자 조치에서 이미 설명한 바와 같이 본 연구에서는 알림처리와 소명처리의 엄격성의 차이에 따른 모니터링 효과를 확인할 것이다.

3.3.2 제한사항

본 연구를 위한 시나리오 적용과 대상자 선정에 있어서는 다음의 제한사항이 존재한다. 탐지 시나리오들 중에서 금융회사 내 모든 직원들에게 동등하게 적용될 수 있는 시나리오만을 선택하여야 했다. 일부 시나리오들은 관련 업무를 수행하는 특정 그룹에서만 주로 탐지되어, 전체 직원을 대상으로 연구를 진행하는 취지에 부합하지 않았기 때문이다.

연구 대상자 선정에 있어서는, 가설설정 단계에서 언급한 바와 같이 금융회사 내 '일반직원'을 대상으로 한다. 여기서 '일반직원' 이라 함은 전자금융감독규정에서 정한 정보보호교육 의무 이수시간이 6시간에 해당하는 직원을 의미한다. 개인정보를 주로 취급하는 일반직원들을 대상으로 하여야 가치있는 연구가 되기 때문에 일반직원으로 제한하였으며, 이들은 모두 6시간의 정보보호교육 이수 대상자들이므로 동일한 교육 조건하에서 실험을 수행할 수 있게 되었다.

금융회사의 일반직원들을 대상으로 한 본 연구에서는 IT 및 정보보호담당자를 제외함으로써 실제 모니터링 대상자는 약 1만 5천명이 되었고, 금융회사 본연의 업무를 수행하는 직원들을 대상으로 한 의미있는 결과가 도출될 수 있도록 설계하였다.

IV. 연구결과

모니터링 시스템으로 수집된 1년간의 모니터링 결과 데이터를 분석하기 위한 도구로 IBM의 SPSS Statistics v25 통계패키지를 이용하였다. 가설(H1, H2, H3)을 검증하기 위한 검증방법으로는 두 가지 이상의 명목형 변수들이 상호독립적인지 관련성이 있는지를 밝힐 수 있는 카이제곱(χ^2) 독립성 검정을 실시한다. 만약, 명목형 변수들이 독립적이라는 귀무가설이 기각되면 Cramer's V 값을 통하여 변수들이 어느 정도의 강한 연관성을 갖는지도 확인해 볼 것이다.

4.1 표본현황

Table 2.는 특별 억제효과를 확인할 수 있는 오남용 행위자 조치방법별 수집 데이터 표본이다. 이와 별개로, 구성원의 근속연수 및 담당업무별 모니터링 효과를 분석하는 데에는 Table 3.과 같이 총 786명의 소명처리 표본이 사용되었다. 참고로, 금융회사에서는 고객에게 다양한 서비스를 제공하기 위해 한명의 직원이 여러 업무를 동시에 수행하는 경우가 많기 때문에 본 연구에서는 직원이 복수의 업무를 수행할 경우 주 업무를 기준으로 분류하였다.

Table 2. Sample Status

Categories		Frequency	Ratio (%)
Response method to misuse	Request for explanation	601	34.1
	Notification	1,163	65.9
Total		1,764	100

Table 3. Demographic characteristics

Categories		Frequency	Ratio (%)
Number of years of service	Less than 10	191	24.3
	11~20	112	14.3
	21~30	336	42.7
	More than 31	147	18.7
Assigned task	General manager	125	15.9
	Deposit	363	46.2
	Loan	225	28.6
	Etc	73	9.3
Total		786	100

4.2 검증결과

4.2.1 조치방법과 모니터링 효과

오남용 행위자 조치방법별 오남용 행위 발생 결과는 Table 4.와 같다. 오남용 행위자에 대한 초기 조치방법으로 소명처리를 한 경우는 오남용 행위를 반복하지 않은 직원 비율이 92.3%였으며, 반복한 직원은 7.7%로 나타났다. 반면, 알림처리를 한 직원들 중에서 오남용 행위를 반복하지 않은 직원 비율은 87.5%, 반복한 직원은 12.5%로 나타났다.

Table 4. Ratio of recurrence analyzed by response method to misuse

Response method to misuse	Unoccurred	Reoccurred	Total
Request for explanation	92.3%	7.7%	100%
Notification	87.5%	12.5%	100%

가설 1을 검증하기 위하여 조치방법과 오남용 행위 발생 간의 상관관계를 카이제곱검정으로 확인한 결과는 Table 5.와 같이 나타났다. 카이제곱(χ^2) 값은 9.510이고, 유의확률은 0.002($p<0.01$)로써 오남용 행위자 조치방법에 따라 모니터링 효과의 차이가 존재하는 것이 확인되어 가설 1이 채택되었다. 연관성 정도를 확인할 수 있는 Cramer's V 값은 Table 5.와 같이 0.073으로 나타났다.

Table 5. Analysis result by response method

	χ^2	V	p
Pearson Chi-square	9.510	-	.002
Cramer's V	-	.073	.002

4.2.2 근속연수와 모니터링 효과

근속연수에 따른 오남용 행위 발생 결과는 Table 6.과 같다. 근속연수 31년 이상인 직원들의 오남용 행위 재발률이 10.2%로 가장 높게 나타났는데, 전체적으로 근속연수가 길어질수록 재발률이 증가하고 있음을 알 수 있다. 가설 2를 검증하기 위한 근속연수와 오남용 행위 발생 간 상관관계를 카이제곱검정을 통해 확인한 결과는 Table 7.과 같다. 카이제곱(χ^2)값은 10.329, 유의확률은 0.016($p<0.05$)으로써, 근속연수에 따라 모니터링 효과의 차이가 존재하는 것이 확인되어 가설 2가 채택되었다. Cramer's V 로 확인되는 연관성 정도는 0.115로 나타났다.

Table 6. Ratio of recurrence analyzed by number of years of service

Number of years of service	Unoccurred	Reoccurred	Total
Less than 10	97.9%	2.1%	100%
11~20	94.6%	5.4%	100%
21~30	92.6%	7.4%	100%
More than 31	89.8%	10.2%	100%

Table 7. Analysis result by years of service

	χ^2	V	p
Pearson Chi-square	10.329	-	.016
Cramer's V	-	.115	.016

4.2.3 담당업무와 모니터링 효과

담당업무별 오남용 행위 발생 결과는 Table 8.과 같다. 담당업무가 업무총괄인 경우 오남용 행위가 재발된 직원 비율이 12.8%로 가장 높았는데, 업무총괄을 제외한 일반 업무담당자들의 오남용 재발 비율은 4.1%~6.7% 수준을 보이고 있다.

가설 3을 검증하기 위한 담당업무와 오남용 행위 발생 간 상관관계를 카이제곱검정을 통해 확인한 결과는 Table 9.와 같다. 카이제곱(χ^2) 값은 11.858이고, 유의확률은 0.008 ($p<0.01$)로써 담당업무에 따라 모니터링 효과의 차이가 존재하는 것이 확인되어 가설 3이 채택되었으며 Cramer's V 값은 0.123으로 나타났다.

Table 8. Ratio of recurrence analyzed by assigned task

Assigned task	Unoccurred	Reoccurred	Total
General manager	87.2%	12.8%	100%
Deposit	95.9%	4.1%	100%
Loan	93.3%	6.7%	100%
Etc	94.5%	5.5%	100%

Table 9. Analysis result by assigned task

	χ^2	V	p
Pearson Chi-square	11.858	-	.008
Cramer's V	-	.123	.008

V. 결 론

5.1 연구의 의의 및 결과 요약

본 연구는 학술적 의의와 실무적 가치를 균형있게 갖추고 있다. 특별 억제이론을 적용한 개인정보 오남용 모니터링 효과 측정 모델을 제시하였고, 스팸메일 발송실험에 편중되어 있던 기존의 현장실험 연구방법을 개인정보 오남용 모니터링이라는 새로운 영역으로 확장하였다는 점에서 학술적 가치를 지닌다. 억제이론을 배경으로 조직 구성원들의 정보보호 정책 준수에 미치는 영향을 연구함에 있어서 기존에는 주로 설문조사에 의존하였는데, 설문조사는 실제 행동과 일치하지 않을 수 있다는 한계가 있다[14]. 한계를 보완하기 위한 현장실험은 스팸메일을 이용한 연구방법이 주를 이루어 왔으며, 본 연구를 계기로 다양한 연구방법을 동원한 현장실험이 촉진될 수 있을 것으로 기대할 수 있다. 실무적으로는 그 동안 연구되지 않았던 개인정보 오남용 모니터링 결과를 다루고 모니터링 효과를 측정하였다는 점에서 모니터링 시스템을 운영하거나 향후 구축에 관심있는 조직의 의사결정에 참고자료가 될 수 있다.

연구결과를 보면, 오남용 행위자를 조치하는 방법에 따라서 소명처리가 92.3%, 알림처리가 87.5%의 오남용 재발방지 효과(특별 억제효과, 모니터링 효과)를 가지는 것으로 확인되었다. 오남용 행위자를 조치하는 엄격성의 차이에 따라 모니터링 효과가 다르다는 것이 검증된 것이다(H1). 또한, 오남용 행위자의 근속연수 및 담당업무와 모니터링 효과 간 상호관련성이 있는 것으로 확인되어 가설(H2, H3)이 모두 채택되었다. 구체적으로는 조직 내에서 근속연수가 31년 이상 된 직원들과 업무총괄의 위치에 있는 직원들에게서 오남용 행위 반복 비율이 높게 나타나 모니터링 효과가 가장 낮았다. 연구결과를 통해 근속연수가 길거나 조직 내에서 위치가 높은 직원이 개인정보 오남용 관점에서는 취약한 것을 확인할 수 있으며, 이에 대한 보완 대책이 필요하다.

5.2 정보보호 정책개선 제언

첫째, 연구결과를 통해 알림조치 만으로도 오남용 행위가 대폭 감소하였지만 소명처리보다는 효과가 적게 나타났음을 확인하였다. 개인정보 오남용 재발방지를 위해서는 조치방법의 엄격성이 긍정적인 영향을 미쳤다는 것을 참고하여, 엄격한 기준을 수립할 필요가 있다. 오남용 행위자에 대한 엄격한 조치 기준을 마련하기 위해서는, 본 논문에서 제시한 모니터링 효과 측정 모델을 활용하여 조치방법 별 효과를 정량적으로 측정 가능하여야 최선의 방안을 선택할 수 있을 것으로 판단된다.

둘째, 오남용 행위를 반복하였던 직원 중 근속연수가 긴 직원들을 대상으로 인터뷰 한 결과, 과거의 업무처리 패턴을 습관적으로 반복한 직원들이 많았다. 주로 개인정보 관련 사고가 크게 발생하기 이전에 입사하여 정보보호에 대한 인식이 낮은 그룹이었

는데, 이들에 대해서는 무의식적으로 발생되는 행위를 차단하기 위한 시스템적 개선이 수반되어야 한다. 김보라(2018)는 스팸메일 현장실험 연구를 통해 메일을 열람하기 전에 위험성을 알리는 보안서비스를 제공하였을 때 스팸메일 열람률이 크게 개선되는 것을 확인한 바 있다[15]. 개인정보 오남용에 있어서도 조직 구성원들의 의도하지 않은 개인정보 조회나 실수에 의한 조회를 방지하기 위해서 시스템을 통한 사전 경고 팝업 등을 제공함으로써 오남용 발생률을 감소시킬 필요가 있다. 그렇지만, 박철주(2012)가 언급하였듯이 기술적 통제는 억제수단으로써 필요조건에 해당될 뿐 예방적 수단으로써의 충분조건으로 보기는 힘들다[16]. 따라서 이들에 대해서는 지속적이고 반복적인 재교육이 반드시 필요하다.

셋째, 업무총괄의 위치에 있는 직원들이 취약한 것으로 나타났듯이, 내부통제로부터 사각지대에 위치한 직원의 존재 가능성 등 취약한 내부통제 프로세스에 대한 보완 대책을 마련하여야 한다. 구체적 실행방안으로는, (1)업무총괄자도 개인정보의 오남용과 관련하여서는 다른 직원들과 동등하게 통제 받을 수 있는 프로세스를 마련하여 사각지대를 제거 (2)실무를 담당하지 않는 업무총괄자에게는 개인정보 접근권한에 제한을 두어 불필요한 접근을 차단 (3)업무총괄자를 대상으로 정기적인 교육 실시 및 업무총괄자가 오남용 행위로 적발되는 경우 타 직원보다 처벌수위를 강화하는 방안 등이 있다.

마지막으로, 정보보호 인식 자체가 미흡한 직원들에게서는 여전히 개인정보를 오남용 하는 행위가 발생 가능하기 때문에, 정보보호교육 정책의 근본적인 개선이 필요하다. 근속연수, 나이와 같은 개인적 요인이나 담당업무, 직위와 같은 업무적 요인 외에도 정보보호 인식 수준이나 습득 능력의 차이로 인해 현실적으로는 모든 직원에게 같은 교육을 하더라도 동일한 교육효과를 기대할 수 없다. 따라서, 교육정책이 기존의 '교육시간' 중심에서 '교육 프로세스'의 적정성을 강조하는 방향으로 바뀌어야 한다. 조직에서 구성원들의 정보보호정책 준수 정도를 자체적으로 분석하여, 부족한 구성원들에게는 교육을 강화하고 우수한 구성원들에게는 불필요한 교육시간을 면제해 줄 수 있는 차별화된 교육 프로세스를 수립하고 운영할 수 있도록 유도하는 정책이 필요하다. 이러한 정책은 조직이 구성원들의 정보보호정책 준수 수준을 측정할 수 있는 프로세스를 마련하게 하고, 구성원들이 정책을 능동적으로 준수하게 하여 조직 전체의 정보보호 수준을 실질적으로 향상시키는 선순환 구조를 구축하게 한다. 감독기관 입장에서도 교육 프로세스의 적정운영 여부를 살펴봄으로써 교육시간 이수여부와 같은 단편적이고 외면적 수치가 아닌 교육의 본질적 목적 달성여부를 확인하는 방향으로 접근할 수 있다.

5.3 한계 및 발전방향

본 연구의 한계점은 다음과 같다. 연구대상을 특정 금융회사로 한정하였기 때문에 연구결과를 금융업이 아닌 다른 업종에 적용할 경우 업종 간 차이가 있을 수 있고, 조직 문화와 특성에 따라서도 차이가 발생할 수 있다. 또한, 본 논문에서 언급하는 '오남용 행위'는 법률 위반행위를 지칭하는 것이 아니라 개인정보 오남용 모니터링 시스템의 탐지 시나리오가 탐지한 직원의 행동 패턴을 의미하기 때문에, 법적인 의미의 '오남용 행위'와는 다르다는 한계가 있다. 마지막으로, 본 연구에서는 오남용 행위자 조치방법, 근속연수, 담당업무를 독립변수로 설정하였는데, 행위자에 대한 더 많은 정보의 수집 및 활용이 가능하다면 보다 다양한 해석이 가능할 것으로 생각된다.

본 연구에서 개인정보 오남용 모니터링이라는 새로운 연구방법을 시도하였기 때문에 앞으로 많은 후속연구가 발생될 수 있을 것이다. 특히, 근속연수가 짧은 직원들은 소명처리만으로도 모니터링 효과가 높은 것으로 나타났지만, 근속연수가 짧았던 직원들이 시간이 흘러 근속연수가 길어지면 어떻게 변화될지에 대한 후속 연구도 진행되기를 기대한다.

References

[1] Related ministries joint, "Comprehensive measures to prevent the recurrence of personal information leakage in the financial sector," Mar. 2014.

[2] Ministry of the Interior and Safety, "Personal Information Inspection and Administrative Disposal Case Study," Apr. 2018

[3] Seung-tae Ryu, "A Study of Detection Measures about the Personal Information Leakage through Scenario-Based Integrated Security Log

Analysis," Master's Thesis, Korea University, Dec. 2015
[4] Hyung-bum Kim, "Internal Leakage of Personal Credit Information in Financial Institutions, Symptoms Monitoring Design Plan," Master's Thesis, Konkuk University, Dec. 2016
[5] Seong-jin Yeon, "The Deterrent Effect of Punishment on Crime," Korean Institute of Criminology, pp. 11-155, Dec. 2003
[6] Cheol-woo Jung and Myeong-soon Jang, "Analysis of Effectiveness of Traffic Safety Education on DWI(Driving While Intoxicated) Deterrence," Journal of Korean Society of Transportation, 29(3), June. 2011
[7] Joong-ho Ahn, Jun-hyung Park, Ki-moon Sung and Jae-hong Lee, "Impacts of Punishment and Ethics Training on Information Security Compliance: Focus on the Moderating Role of Organizational Type," Information Systems Review, 12(1), pp. 23-42, Apr. 2010
[8] Do-yeon Lee, "The effect of punishment and training on information security policy compliance behavior : the empirical analysis through field experiments," Master's Thesis, Yonsei University, Dec. 2017
[9] Jong-ki Kim and Da-woon Oh, "A Study on Security Policy Violations of Organization Members," Information policy, 25(3), pp. 95-115, 2018
[10] Ow-won Park and Jong-seok Cha, "Effects of Organizational Tenure of R&D Workforce on Creative Performance and Organizational Commitment : Focusing on Moderating Effect of Career Plateau," Korean Journal of Business Administration 32(2), pp. 327-345, Feb. 2019
[11] Anat Hovav and John D`Arcy, "Applying an extended model of deterrence across cultures : An investigation of information systems misuse in the U.S. and South Korea," Information & Management, vol.49, no.2, pp.99-110, 2012
[12] Hye-jeong Lee, Gyu-chang Yu and Soon-young Myung, "The impact of job-based HR on the attitude of employee," A Study on the Organization and Personnel Management, 43(3), pp. 149-176, Aug. 2019
[13] Dong-keun Choi, Mi-sun Song, Jong-in Im and Kyung-ho Lee, "Study the role of information security personnel have on an organization's information security level," Journal of the Korea Institute of Information Security and Cryptology, 25(1), pp. 197-209, Feb. 2015
[14] Paschal Sheeran, "Intention-behavior relations: A conceptual and empirical review," European review of social psychology, vol.12, no.1, pp. 1-36. 2002.
[15] Bo-ra Kim, Jong-won Lee and Beom-soo Kim, "Effect of Information Security Training and Services on Employees' Compliance to Security Policies," Journal of informatization policy, 25(1), pp. 99-114, Feb. 2018
[16] Chul-ju Park and Myung-seong Yim, "An Understanding of Impact of Security Countermeasures on Persistent Policy Compliance," Korean Studies Information Service System, 10(4), pp. 23-35, May. 2012

〈저자소개〉

김 영 호 (Young-ho Kim) 정회원
2008년 2월: 경북대학교 컴퓨터공학과 졸업(학사)
2018년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 개인정보보호, 정보보호관리체계, 정보보호정책

김 인 석 (In-seok Kim) 정회원
1973년 2월: 홍익대학교 전자계산학과 졸업(학사)
2003년 2월: 동국대학교 정보보호학과 졸업(석사)
2008년 2월: 고려대학교 정보경영공학과 졸업(박사)
2011년~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 전자금융보안, IT감사, 전자금융법규