Asia Pacific Journal of Information Systems
Vol. 22, No. 1, March 2012

The Behavioral Attitude of Financial Firms' Employees on the Customer Information Security in Korea*

Woo-Jin Jung**, Yuhyung Shin***, Sang-Yong Tom Lee****

Financial firms, especially large scaled firms such as KB bank, NH bank, Samsung Card, Hana SK Card, Hyundai Capital, Shinhan Card, etc. should be securely dealing with the personal financial information. Indeed, people have tended to believe that those big financial companies are relatively safer in terms of information security than typical small and medium sized firms in other industries. However, the recent incidents of personal information privacy invasion showed that this may not be true.

Financial firms have increased the investment of information protection and security, and they are trying to prevent the information privacy invasion accidents by doing all the necessary efforts. This paper studies how effectively a financial firm will be able to avoid personal financial information privacy invasion that may be deliberately caused by internal staffs. Although there are several literatures relating to information security, to our knowledge, this is the first study to focus on the behavior of internal staffs. The big financial firms are doing variety of information security activities to protect personal information. This study is to confirm what types of such activities actually work well.

The primary research model of this paper is based on Theory of Planned Behavior (TPB) that describes the rational choice of human behavior. Also, a variety of activities to protect the personal information of financial firms, especially credit card companies with the most customer information, were modeled by the four-step process Security Action Cycle (SAC) that Straub and Welke (1998) claimed.

Through this proposed conceptual research model, we study whether information security activities of each step could suppress personal information abuse. Also, by measuring the morality of internal staffs, we checked whether the act of information privacy invasion caused by internal staff is in fact a serious criminal behavior or just a kind of unethical behavior. In addition, we also checked whether there was the cognition difference of the moral level between internal staffs and the customers. Research subjects were customer call center

* This work was supported by the research fund of Hanyang University(HY-2009-N).
** MS Student, School of Business, Hanyang University
*** Assistant Professor, School of Business, Hanyang University
**** Corresponding Author, Professor, School of Business, Hanyang University

operators in one of the big credit card company. We have used multiple regression analysis.

Our results showed that the punishment of the remedy activities, among the firm's information security activities, had the most obvious effects of preventing the information abuse (or privacy invasion) by internal staff. Somewhat effective tools were the prevention activities that limited the physical accessibility of non-authorities to the system of customers' personal information database. Some examples of the prevention activities are to make the procedure of access rights complex and to enhance security instrument. We also found that 'the unnecessary information searches out of work' as the behavior of information abuse occurred frequently by internal staffs. They perceived these behaviors somewhat minor criminal or just unethical action rather than a serious criminal behavior. Also, there existed the big cognition difference of the moral level between internal staffs and the public (customers).

Based on the findings of our research, we should expect that this paper help practically to prevent privacy invasion and to protect personal information properly by raising the effectiveness of information security activities of finance firms. Also, we expect that our suggestions can be utilized to effectively improve personnel management and to cope with internal security threats in the overall information security management system.

Keywords : IS Management, Information Security, Information Privacy, Deterrence Theory, Security Action Cycle

금융회사의 고객정보보호에 대한 내부직원의 태도 연구

정 우 진, 신 유 형, 이 상 용

Ⅰ. 서 론

최근 보도에 따르면 기획재정부가 한국의 2012년 정보보호예산을 금년보다 30% 늘어난 규모로 책정하고 그 예산의 대부분을 개인정보 유출 및 오남용 방지, 정보보호 인프라 구축 등에 주로 사용할 것으로 밝히고 있다[아이뉴스, 2011]. 이 같은 정부의 예산편성은 특히나 올해에 유난히 많았던 개인정보와 관련한 사건사고가 많았기 때문으로 풀이된다. 정부는 물론이고 대기업 중소기업 가릴 것 없이 개인정보 유출 또는 오남용 등이 심심치 않게 신문이나 방송을 통해 보도되고 있으며, 특히 금융정보를 다루기 때문에 안전해야 하고 다른 업종보다 상대적으로 안전하다고 믿었던 금융회사들(국민, 농협, 삼성카드, 하나SK카드, 현대캐피탈, 신한캐피탈 등)의 연이은 사고는 이러한 개인정보유출의 심각성을 단적으로 보여주고 있다. 과거 수많은 기업의 정보유출 사건들을 비추어 볼 때, 사고와 관련된 해당 기업들은 앞으로 기업 이미지 손실과 같은 무형적 손실은 물론, 금전적인 배상에 이르는 유형적 손실도 겪을 것이 자명하다. 이와 같은 이유로 기업들은 정보를 보호하기 위해 금전적인 투자는 물론 그 외에 필요한 모든 노력들을 기울이는데 주저하지 않는 것이다.

기업이 보유한 정보에는 기밀, 직원의 인적 사항, 재무정보 등 다양한 정보들이 있는데, 본 연구에서는 앞서 언급한 사건들에서 알 수 있듯이 최근 사회적 이슈가 되고 있는 고객의 개인정보를 중심으로 연구하고자 한다. '개인정보'가 무엇인지 사전적으로 명확히 정의된 의미는 없으며, 단지 다양한 형태로 통용되는 논문들이나 국가별 판례에

따른 법률적 해석이 있을 뿐이다. 이러한 해석들을 참고로 종합해 볼 때 특징적인 개인정보의 의미는 '한 사람 그 자체가 다른 사람과 식별이 가능한 중요한 정보' 정도로 해석할 수가 있을 것이다. 이러한 의미의 개인정보는 지식 정보화 사회의 발전에 따라 유형적 가치는 물론 무형적 가치 또한 증대되고 있으며 현재 사회의 실질적인 핵심가치로써 평가 받고 있다[권영관, 염홍렬, 2009].

그렇다면 현 시대의 개인정보의 가치는 얼마나 되는가 하는 의문이 생기게 된다. 하지만 이와 관련한 연구들은 진행 중일 뿐 명확한 기준은 없다. 다만 법학적 방법론으로써 관행주의, 법 실용주의, Integrity로써의 법 등 크게 3가지 관점에 연구가 이루어지고 있는데 과거 판례들과 관련해서는 보통 법 실용주의 측면에서 접근하는 것이 바람직하다는 의견이 있다[허성욱, 2009]. 이러한 주장을 바탕으로 과거 소송사례에 비추어 측정해 보면, 옥션, GS칼텍스, 하나로텔레콤을 상대로 한 개인정보유출관련 소송의 경우 소송인 20만 여명에 총 청구액이 2,100억 원대에 달하는데 이 때 개인정보 1인의 금전적 가치에 대해 간접적으로 남아 측정이 가능이다. 물론 이것은 어디까지나 법 실용주의 측면에서 측정한 것으로 절대적 가치는 아니다. 또한, 기업의 입장에서는 개인정보 유출로 인한 금전적인 보상액이 기업의 생존을 위협할 만큼 크기 때문에 기업의 정보보호 활동은 이제 간과할 수 없는 기업운영의 중요한 핵심요소가 되었다[이상준, 2008].

정보보호와 관련한 다양한 논의들이 존재하지만 본 연구의 초점은 비록 학문적 연구를 바탕으로 연구된 논문일지라도 연구결과가 기업의 정보보호활동에 실질적으로 도움이 되고자 하는 데서 출발한다. 따라서 다음 제시되는 사례를 통해 본 논문 연구 범위를 좀 더 구체화 하고자 한다. 2010년 8월 한 국내 모 시중은행에서 일하는 은행원이 수백억 원을 예치한 고객의 금융거래 정보를 누설한 혐의로 경찰에 체포된 사건이 있었다. 그 은행원은 3일 금융거래 정보를 조회한 뒤 지인에게 그 금융정보를 넘긴 혐의(금융실명거래 및 비밀보장에 관한 법률위반 등)로 불구속 입건되었다[매일경제신문, 2010]. 이 사례의 초점은 첫째, 정보유출경로가 상대적으로 어려운 해킹이나 침입자에 의한 외부로부터가 아닌 마음만 먹으면 정보유출경로가 단순한 내부로부터 유출되었다는 것이다. 둘째, 정보유출이 기업의 정보보호활동과는 무관하게 통제하기가 어려운 실수가 아닌 체계적인 정보보호 활동으로 통제가 가능한 고의에 의해 발생되었다는 것이다. 셋째, 현재도 많은 기술적 연구가 진행되고 있으며 상대적으로 체계적 관리하기가 쉬운 시스템 아닌 체계적 관리보다는 심리학적 관리가 필요한 사람에 의해 유출되었다는 것이다. 마지막으로 넷째, 이 사례에서 은행원(내부직원)이 넘긴 한 고객정보는 내부직원이면 매일 아주 쉽게 조회가 가능하고 활용도 가능하며 수백억의 금전적 가치가 될 수도 있을 만큼 민감한 개인의 금융정보라는 것이다. 이러한 4가지 특징을 종합해 볼 때 본 연구는 "내부직원으로부터 발생될 수도 있는 고의적인 개인금융정보의 유출을 어떻게 하면 효과적으로 방지할 수 있을 것인가"에 대한 질문에 해결방안을 모색해 보는 것이다.

현재 많은 기업들이 정보유출을 방지하기 위해 자율적인 정보보호 활동을 강화하면서 안전한 관리기준을 제공할 목적으로 표준화된 정보보호 관리체계를 도입하고 있는데 이러한 정보보호 관리체계의 국제표준은 ISO 27001이고 국내에서는 한국인터넷진흥원에서 인증하는 ISMS (Information Security Management System) 인증을 따르고 있다. 개인정보보호와 관련해서는 국제표준은 따로 없고 다만 국내에서 ISMS와 마찬가지로 한국인터넷진흥원에서 인증하는 PIMS(Personal Information Management System) 인증을 권장하고 있다. 이러한 표준들은 각 기준에 따라서 여러 형태의 정보보호 관리영역이 존재하는데 이것은 결국 정보유출의 채널이 다양하다는 것을 반증하기도 한다. 하지만 기술적이든

물리적이든 다양한 정보유출 채널에도 불구하고 결국 정보유출의 주체는 사람이기 때문에 사회적, 조직적인 이슈가 더욱 중요하다고 할 수 있다[Dhillon and Backhouse, 2000]. 다시 말해, 조직이 조직구성원(사람)의 행동을 적절하게 통제한다면 조직 내의 정보유출을 방지하는데 있어서 기술적인 접근 보다 좀 더 효과적일 수도 있다는 뜻을 내포한다[Straub, 1990].

그렇다면 기업들은 사람(내부직원)에 의해 발생되는 정보유출을 방지하기 위해 어떠한 노력을 해야 하는가? 내부직원에 의한 정보유출은 그 직원이 정보습득이 가능하다는 전제에서 가능하다. 내부직원이 정보를 습득할 수 있는 방법은 정보를 조회할 수 있는 접근권한이 있어야 한다. 반대로 정보에 접근을 못하거나 정보조회를 하지 않으면 유출할 정보도 없게 된다. 하지만 본 연구의 조사 대상인 금융회사의 경우 고객의 개인정보는 그 회사의 핵심정보이기 때문에 고객정보의 조회나 접근권한 없이 필요한 업무를 수행하는 것은 불가능하다. 반드시 고객정보조회가 가능한 물리적 시스템에 대한 접근권한이 있어야 하고 고객 정보조회를 위한 시스템 조회권한도 있어야 한다. 물론 습득한 정보의 활용도 가능해야 한다. 따라서 금융회사는 업무특성상 내부직원을 고객정보로부터 완벽하게 통제하는 것은 불가능하다. 하지만 물리적으로 정보조회가 가능한 시스템 접근을 제한하거나 정보조회 시스템을 통한 업무 이외에 불필요한 정보조회를 제한할 수 있다면 정보유출의 전제가능성을 최소화할 수 있다. 즉, 기업의 입장에서 현실적으로 불가능하고 아직 실현하지도 않은 내부직원의 정보유출행위를 제한하기 보다는 정보남용과 관련한 업무 이외에 불필요한 정보조회를 제한함으로써 정보유출의 시발점을 통제하고 고객의 프라이버시 침해를 최소화할 수 있는 효과를 볼 수 있을 것이다. 따라서 본 연구의 구체적인 연구목적은 금융회사의 내부 직원으로부터 업무 이외에 불필요한 고객정보조회를 통제하기 위한 효과적인 기업정보보호 활동들을 파악해 보는 것이다.

본 연구의 구성은 다음과 같다. 다음 단락에서는 연구배경이 되는 금융회사의 정보보호 체계와 계획된 행위이론, 억제이론과 보안주기활동, 그리고 도덕발달이론을 다룰 것이다. 이러한 이론 및 체계를 바탕으로 연구가설과 연구모형을 Section 3에서 제시할 것이다. Section 4에서는 연구방법에 대하여 논의하고, Section 5에서는 연구결과에 대한 심도 깊은 토론을 행할 것이다. 마지막으로 본 논문을 요약하고 결론을 도출할 것이다.

Ⅱ. 연구 배경

2.1 금융회사의 정보보호체계

정보보호란 정보의 입력, 처리, 저장, 출력, 전송 등의 모든 단계에 걸쳐서 시스템을 보호하는 것을 말한다. 미국에서는 정보보호를 시스템 및 정보를 고의 혹은 실수에 의한 공개, 변조, 파괴 및 지체로부터 보호하는 활동이라고 정의하였고, 유럽에서는 전자적인 형태의 정보를 처리하거나 저장하는 모든 단계에 걸쳐서 정보를 보호하는 활동으로 정의하고 있다[박태완, 1997].

정보보호의 개념은 좀 더 폭넓게 국내에서 '정보보안'으로 불리며 다양한 내적 또는 외적인 위협들로부터 조직의 손실을 최소화하고 이익을 극대화하는 것을 의미하기도 한다[Finne, 1998]. 또한, 국제표준 ISO 27001[2007]의 따르면 정보보안은 기밀성, 무결성, 가용성이 강구되어 정보를 보호하는 일체의 행위라고 정의하고 있으며, 국정원에서는 정보시스템 및 통신망을 통해 수집, 가공, 저장, 검색하거나 소수인 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 물리적, 기술적 일체의 행위로 정의하고 있다[이철원, 2001].

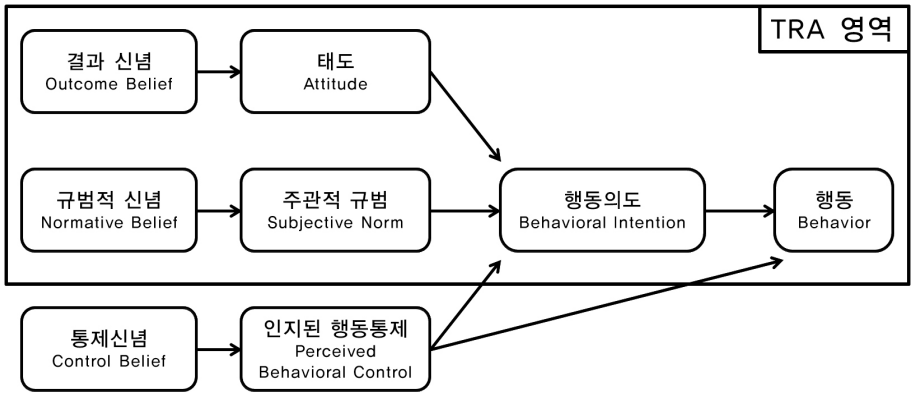
앞서 언급했듯이 금융회사에서 보호해야 할 주요한 핵심정보는 고객정보이다. 이러한 고객정보의 종류로는 성명, 주소, 주민등록번호, 성별, 국적 등 거래 주체를 식별할 수 있는 정보 및 금

융거래정보, 대출 등 여신에 관련된 정보, 채무/납세실적 등 신용도의 판단을 위해 필요한 정보, 유가증권 매매계좌에 예탁한 금전 또는 유가증권에 관한 정보 중 금융지주회사법에서 정의하는 증권총액정보 등이 있다. 이러한 금융회사의 고객정보를 취급하는 방침인 '금융지주회사법 제48조의 2'은 각 금융회사마다 내부방침을 따로 정해 엄격한 절차와 관리감독이 이루어지도록 하고 있다. 따라서, 각 금융회사에서 수집한 내부방침 문건과 최근 연이은 고객정보유출사고로 각 금융회사에서 보내 온 고객정보 취급방침에 관한 안내 이메일을 토대로 각 금융회사의 공통적인 내부방침을 종합해 보면, 고객정보의 제공 및 이용은 영업상의 목적으로만 가능하게 하였고 고객정보의 요청 및 제공 시 고객정보관리인의 결재를 득한 후 공식문서에 의하도록 하였으며 만약 피해를 입게 된 고객을 위한 적절한 보상 및 처리가 이루어지도록 민원사항에 대한 안내 및 상담, 처리, 그리고 결과 통지 등 민원관련 일체의 업무를 수행할 소관부서(주로 고객 서비스팀)를 지정하도록 하였다.

하지만 금융회사가 파악하고 있는 일선의 내부직원에 의한 실제 고객정보의 취급상태는 이와는 다소 차이가 있는 것으로 나타났다. 우선, 내부직원에 의한 고객정보의 주된 유출경로는 외부 협력사 소속인 채권관리사 등의 요청에 의한 타사 유출이나, 회사내부 문건을 통신망을 통해 유출시키거나 복사 또는 인쇄를 통해 문서화하여 유출하는 등의 것이다. 또한 금융회사는 정보남용 성격의 임의적인 정보조회에 대해서도 문제의식을 가지고 있으며, 이와 관련한 주요한 사례로 내부직원의 불필요한 정보조회나 정보조회 시스템 접근을 위한 내부직원 간의 접근권한공유 등을 제시하고 있다. 이러한 사고경로를 토대로 금융회사는 실제 대량의 고객정보취급부서이며 많은 내부직원을 관리해야 하는 고객서비스팀에 대한 정보보호활동에 좀 더 주의를 기울이는 것으로 파악되었다. 실제로 금융회사에서 수행되고 있는 감시활동은 감시시스템에 의한 24시간 감시와 정기적으로 년 1회 이상 감시팀에 의해 공식적인 감시점검이 이루어지고 있다. 또한 감시인으로서 각 부서의 팀장급 임원들에 의해 보안 환경에 대한 점검활동도 수시로 이루어지고 있다.

이와 함께 금융회사는 정보유출이나 정보남용을 예방하기 위한 정보보호 활동도 하고 있는데, 우선 물리적 환경으로는 CCTV, 경비실, 출입보안장치(비밀번호, 지문인식) 등을 설치운영하고 있으며 비인가 장비(개인노트북, 무선공유기, 이동단말기, USB 등)에 대한 반입/반출 엄격히 금지하고 있다. 반면, 정보조회를 위한 시스템 접속환경으로는 내부직원의 업무PC의 접속ID/PW설정, 조회 시스템 접속ID/PW설정, 사설메신저나 비업무 사이트 접속금지, 표준설치환경에서 임의적인 변경을 금지하는 등의 활동들을 하고 있다. 간혹 물리적으로 시스템 접근권한이 없는 동료의 업무PC나 전산센터 시스템 등에 접속하여 정보조회를 해야 할 경우가 있는데 그것은 정보보호센터의 절차에 따라 정보조회 권한에 대한 승인을 받은 후 접속이 가능하다.

하지만 정보유출 및 정보남용 사례에서 알 수 있듯이 정식절차에 따라 정보조회를 권한을 얻어 시스템에 접속하는 과정은 실제업무환경에서 적용하기 어렵고 보통은 접속권한이 있는 해당 PC의 동료나 상사의 ID/PW를 도용해서 사용하고 있는 것으로 파악되었다. 이와 같은 금융회사의 많은 정보보호활동 노력에도 불구하고 내부직원이 정보를 유출했다면 회사는 징계규정에 따라 해고 및 고발조치를 할 수 있도록 하였으나, 정보남용으로 인한 제재로서 경고조치나 실적평가반영 이외에 정보남용으로 인한 실질적인 피해결과가 발생하지 않는 한 특별한 징계규정은 없는 것으로 파악되었다. 즉, 정보남용에 대한 사실이 문제가 될 소지가 없거나 들어나지 않는다면 처벌할 근거가 없는 것이다. 또한 이러한 문제를 실제로 파악할 수 있는 수단에도 한계가 있는 것으로 나타났다.



<그림 1> 계획된 행위 이론(TPB) 모형

2.2 계획된 행위이론(Theory of Planned Behavior)

인간의 합리적 선택에 의한 행동을 설명한 연구 모형 중에는 Ajzen and Fishbein[1980]과 Fishbein and Ajzen[1975]의 합리적 행동이론(Theory of Reasoned Action; TRA)이 있다. TRA는 행동을 예측하기 위한 가장 좋은 예측 변수로 행동의도(Behavioral Intention; BI)를 제시하는데, 이러한 BI는 개인이 특정행동에 대해 갖는 태도(Attitude)와 개인이 특정 행동에 대해 다른 사람들이 어떻게 인지할 것인가에 관한 개인이 갖는 주관적인 규범(Subjective Norm; SN)에 의해 결정된다. 하지만, TRA는 의지적(Volitional)이며 자발적(Voluntary) 행동을 예측하는데 국한되며, 행동목적에 대한 통제가 완전하지 않을 경우 행동을 충분히 예측해 주지 못하기 때문에, 개인이 특정 행동을 할 때 통제를 수행할 수 있는 새로운 변수가 요구되었다. Ajzen[1985; 1991]은 완벽한 의지적 행동이 아닌 경우, TRA의 모형에 인지된 행동통제(Perceived Behavioral Control; PBC)의 필요성을 주장하며 <그림 1>의 계획된 행동통제(Theory of Planned Behavior; TPB)를 제안하였다. 결론적으로 개인의 의지에 의해 완전한 통제가 어려운 행동을 예측하기 위해서는 TPB로 예측하여야 설명력이 증가한다.

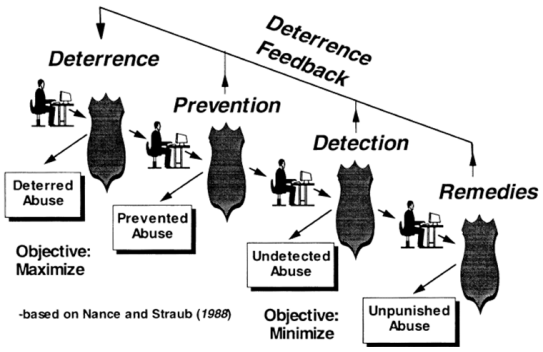
PBC는 앞으로 있을 행동에 대해 편의성, 용이성 또는 반대로 난해성, 복잡성 등의 개인의 인지 정도를 말하는 것으로 인지수준은 과거의 경험이나 그 행동을 실행하는데 기대되는 장애물, 난관 등에 의해 반영된다. 이렇게 행동에 제약을 주는 장애물이나 난관은 실제 기업에서 시스템이나 인증절차와 같은 물리적, 기술적 환경을 말한다[Triandis, 1979]. 이러한 PBC는 개인이 특정행동을 실행하기 위해 필요하다고 생각하는 자원이나 기회를 갖고 있을 가능성에 대한 믿음(통제신념; control belief)에 의해 결정되는데 즉, 개인이 자원이나 기회를 충분히 가지고 있다고 생각할수록, 그리고 행동하는데 있어서 장애물이 덜 예상된다고 생각할수록 행동에 대한 통제 인지수준이 증가하게 되는 것이다[Ajzen, 1985; 1991]. PBC는 Attitude와 SN과 더불어 BI를 결정하게 되는데 여기서 말하는 BI는 단지 행위자 자신들의 행동에 대한 통제 인지수준이 높을 때만 실제 행동으로 이어질 수 있다는 것이다. 다시 말해, 행동의도를 갖고 있더라도 PBC가 낮다면 실제로 행동을 하지 않는다는 것이다(Doll and Ajzen, 1992).

2.3 억제이론(Deterrence Theory)과 보안 주기활동(Security Action Cycle)

억제이론(Deterrence Theory)은 범죄학에서 주로

통용되는 이론으로 바람직하지 않거나 정당하지 못한 행동(범죄적 행동)을 하려는 행위자로 하여금 행동의 손해가 이익보다 많다는 것을 제시한 이론이다. 즉, 범죄로 얻는 이익보다 범죄를 저지른 후에 입는 손해가 더 크다는 것이다[Lebow and Stein, 1990]. 이러한 범죄적 행동을 예방하기 위해 억제는 상대방이 특정 행동을 하지 못하도록 하는 소극적인 영향력을 행사하는 것으로 심리적인 부분에 크게 작용하는데, 이러한 억제는 인간의 마음속에서 생겨나는 것이며, 객관적 진실보다는 상대방이 무엇을 믿는가 하는 점이 더 중요하다[Kissinger, 1974]. 범죄적 행동으로 인한 손익은 객관적으로 측정될 수 있는 부분이 아니고 인지적으로 결정되기 때문에 행동을 선택하는 당사자의 성향 내지는 특성에 따라서 달라질 수가 있다[Williams and Hawkins, 1986]. 다시 말해, 억제이론은 어떠한 생물학적, 심리학적, 사회학적 특성이 행위자로 하여금 범죄적 행동을 선택하게 하는지에 대한 답을 제공하지는 못한다. 단지 모든 유형의 사람들에게 공통적으로 적용되는 범죄적 행동의 발생 원인에 대한 설명일 뿐 범죄 행위자의 특성을 설명하지는 못한다는 것이다. 따라서 억제이론은 합리성을 가정하여 행위자의 다양한 특성에 따라 분류하지 않고 모든 행위자들은 모든 특성에서 동일하다는 전제를 한다[신동준, 2009].

Straub and Welke[1998]는 <그림 2>에서 보듯이 억제이론을 바탕으로 억제(Deterrence), 예방(Prevention), 탐지(Detection), 교정(Remedy)의 4단계의 과정을 나타내는 보안활동주기(Security Action Cycle; SAC)를 제시하였다. SAC은 각 단계마다 정보의 남용이 나타날 수 있고 이를 방지하지 하기 위한 정보보호활동도 반복적으로 이루어진다는 것을 설명한 것이다. 이렇게 정보보호활동이 이루어지는 가운데 나타나는 정보남용은 순차적으로 일어날 수도 있고 개별적으로 일어날 수도 있으며 어떤 행위자의 범죄적 행동이 있을 경우 이를 억제할 수 있는 기능도 가져야



<그림 2> 보안활동주기(Security Action Cycle)

한다[Theoharidou *et al*., 2005; p. 475].

구체적으로, 1단계 억제활동은 보안정책, 가이드라인 같은 수동적인 조치를 의미[Straub and Welke, 1998]하는 것으로 조직 내에서 정보보안 임무를 수행하기 위한 최상위에 보안요구사항이다[정보통신부, 2006]. Wiant[2005]는 억제이론을 활용하여 정보보호와 관련된 요소 중에서 정책에 대한 부분에 초점을 맞추어 개인의 인식과의 관계를 연구하였는데 이 연구에서 정보보안정책은 개인이 조직에서 발생하는 보안사고(정보유출이나 정보남용)를 인식하는데 영향을 준다고 설명하였다. 즉, 이러한 기업의 정보보안정책은 정보보안교육이나 지침을 통해 직원에게 전달되는데[Karyda *et al*., 2005] 이렇게 전달된 정보보안정책을 인지한 직원들은 기업에서 발생하는 보안사고에 대한 인식에 영향을 받게 된다는 것이다. 이러한 논리를 바탕으로 다음 장에 소개되는 가설 1과 가설 2를 세웠다.

2단계 예방활동은 조직 내의 물리적 시스템 보안, 특화된 보안 소프트웨어 설치, 시스템 접속 ID/PW 관리 등과 같은 정보접근과정 상의 통제를 통해 범죄적 행동을 제한하려는 노력을 의미[Straub and Welke, 1998]하는 것으로 전반적인 정보접근을 위한 물리적/기술적 통제활동을 나타낸다. 앞에서 언급했듯이 실제로 금융회사에 고객정보를 습득하기 위해서는 우선 물리적 시스템에 접근하기 위한 접근권한이 필요하며 그 시스템을

통해 필요한 정보를 조회할 수 있는 정보조회권한이 필요하다. 정보조회의 권한의 경우, 내부직원의 직위, 부서, 업무 등에 따라 약간의 차이가 있지만 기본적인 정보조회 권한은 모든 내부직원에게 공통적으로 부여되고 있다. 따라서 금융회사에서 내부직원이 고객정보를 습득하기 위해서는 물리적인 시스템 접근권한 그리고 정보조회 시스템의 접속권한 2가지 권한이 모두 충족되어야 가능하다. 물리적 시스템의 경우는 보통 내부직원마다 접근권한이 이미 부여된 업무PC가 제공되며 접근권한이 부여되어 있지 않은 외부 시스템(전산실 서버, 동료의 PC, 감시 시스템 등)의 이용을 원한다면 회사내규의 절차를 통해 해당 시스템의 접근권한을 부여 받아야 한다[인터넷진흥원, 2008]. 결과적으로 내부직원은 본인의 업무 PC보다 외부 시스템에서의 정보 습득이 상대적으로 복잡하고 어려운 환경이 되는 것이다. 이와 같이 복잡하고 까다로운 정도를 나타내는 복잡성(Complexity)은 새로운 기술을 배우고 이해하고 사용하는 것이 상대적으로 어려운 정도를 나타낸다[Rogers, 1983]. 반면 정보조회를 위한 시스템 접속권한은 직급이나 부서에 따라 정보조회 범위의 한계가 있을 뿐 직원 개개인에게 부여되는 고유 ID/PW가 각각 있다. 다만 부여된 직원 개인의 ID/PW로 시스템 내의 접속은 가능하겠지만 정보조회 시스템 자체가 워낙 방대하고 전문적이어서 직원 개인의 특성이나 역량에 따라 고객정보 수집에 차이를 보일 것이다. 이러한 논리를 바탕으로 다음 장에 소개되는 가설 3과 가설 4를 세웠다.

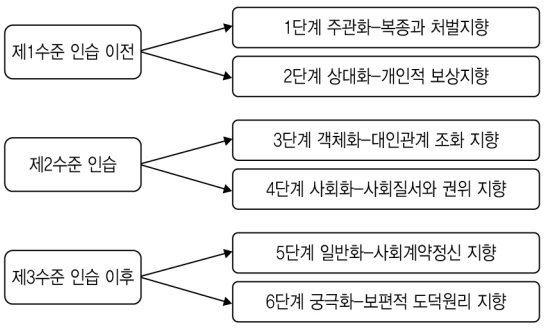
3단계 탐지활동은 보안을 위협하는 의심 행동을 스캐닝 하거나 감시 또는 바이러스 조사 등과 같은 모니터링을 의미한다[Straub and Welke, 1998]. 이러한 탐지활동의 대상은 내부직원이 될 수도 있고 외부침입자가 될 수도 있다. 하지만 이와 상관없이 실제로 기업에서 수행하는 탐지활동은 크게 두 가지로 구분할 수 있는데 하나는 사람(감시자)에 의한 감시활동이고 다른 하나는 시스템에 의한 감시활동이다[인터넷진흥원, 2008]. 이러한 기업의 감시활동들은 기술적인 정보접근은 물론 물리적인 정보접근까지 정보유출 대한 잠재적 위험성에 영향을 주고 있다[Bhimani, 1996]. 이러한 논리를 바탕으로 다음 장에 소개되는 가설 5와 가설 6을 세웠다.

마지막 4단계 교정활동은 조직에서 실시하는 보상이나 처벌 등을 의미하는데[Straub and Welke, 1998], 실제로 기업의 정보보호 관리체계에서 교정활동은 처벌에 국한되는 기업사례가 많은 편이다[인터넷진흥원, 2008]. 처벌은 규범적 요소에 영향을 받는데 인간은 합리적이긴 하지만 이러한 규범과 가치의 틀 안에서 합리적일 뿐 백지상태의 합리성을 가정하는 것은 비현실적이다. 대부분의 사람들은 규범과 가치의 틀 안에서 '합리적인 계산'을 하기 때문에 범죄 행동을 하지 않는 것이다. 범죄는 기본적으로 규범을 어기는 행위이므로 규범적 요소를 배제하고 범죄행동의 선택에 대해서 논하는 것은 적절치 않다. 따라서 처벌효과를 이야기할 때에도 완벽한 합리성을 가정하기보다 사회의 규범과 가치를 실제 경험하고 있는 사람들에게 처벌 효과가 어떻게 미치는지에 주목해야 한다[Tyler, 2006; p. 24]. 이러한 처벌효과는 처벌의 엄격성과 확실성에 의해 설명할 수 있는데, 사람들(내부직원들)은 이러한 처벌의 엄격성과 확실성을 통해 개인의 인식에 영향을 받게 된다[Tittle, 1980]. 하지만, 사람에 따라 처벌효과가 다르게 나타날 수 있다는 것은 이미 많은 연구자들이 지적한 사항이다. 이것은 무엇보다도 객관적인 처벌의 엄격성이나 확실성보다는 그에 대한 주관적인 인지가 행동선택을 위한 합리적 계산에서 실제로 고려된다는 사실에 근거한다. 그리고 범죄적 행동으로 인한 손익 계산은 정보처리 과정을 수반하기 때문에, 그러한 주관적 인지가 정보처리를 하는 주체의 성향이나 특징에 따라 달라질 수가 있다[신동준, 2009]. 이러한 논리를 바탕으로 다음 장의 가설 7과 가설 8을 수립하였다.

2.4 도덕발달이론(Moral Development)

도덕성은 주어진 구체적 사태를 도덕적으로 해석하여 어떤 행동이 옳고 그른지를 가려보고, 그 결과로써 특정행동을 하기로 선택하는 심리적, 이성적 판단과정을 말한다[Blasi, 1980]. 이러한 도덕성이 지적 특성인가 정의적 특성인가에 대한 의문은 지금도 논의되고 있는 이슈이다. 도덕성은 '도덕적 성향'을 말하며 도덕적 성향은 올바른 행동, 사회적으로 용인되는 행동, 서로에게 이로운 행동을 하는데 작용하는 인간의 성질을 말한다. 따라서 그 성질은 매우 복잡하다. 그래서 단지 지적 또는 정의적 특성 하나로 도덕성을 국한하는 것은 부적절하다. 이것은 마치 생각과 마음을 이원화 시키는 것과 같다. 본 연구에서는 도덕성을 '도덕 판단' 능력으로 정의하고 지적 특성과 정의적 특성이 결합된 통합적 특정으로 고려하였다. 즉, 도덕성이란 도덕적 행위를 결정하는 선행요인으로써 상황 판단력 혹은 다양한 선택지 중에서 어느 것을 선택하는 경향으로 정의하였다[손충기, 김영태, 2006].

콜버그[Kolhberg, 1927~1987]는 이러한 '도덕판단'의 기준을 <그림 3>과 같이 도덕발달단계로써 3수준 6단계로 구분하였다. 콜버그가 주장하는 고도로 성숙된 도덕성은 자기 자신을 다른 사람들과 동일시하고, 다른 사람들에게 배려하며, 무엇보다도 '정의와 휴머니즘' 원리에 입각해 행동할 수 있는 능력을 갖는 것이다. 도덕성의 이러한 단계들은 도덕성 진화의 일반적 방향을 반영하는데 콜버그는 도덕적 의식의 보편적 형식들(원리, 표준, 가치)은 모든 시대에 존재하는 것이지만 그것의 성숙도에는 차이가 있다고 주장하였다[문용린, 2000].



<그림 3> 콜버그의 도덕발달단계

제 1수준인 인습이전 수준은 도덕적 선악의 개념은 있지만 단순히 보상이나 처벌을 가져다주는 행위결과나 외적인 권위에 비추어 해석한다. 구체적으로 제 1수준에 포함된 1단계 주관화는 특정 행위의 결과가 지니는 가치나 의미를 도외시한 채 그 행위가 가져다주는 물리적 결과가 선악판단의 기준이 된다. 이 단계에서는 처벌과 같은 외적 규제를 피하거나 또는 권위에 무조건 복종하는 수준의 도덕성을 보인다. 또한 2단계 상대화는 자신이나 때로는 타인에게 이익이 되거나 필요를 충족시켜주는 행위는 선이라고 판단하는 단계로 이 단계에서는 서로 이익을 주고받는 일종의 교환관계로써 인간관계를 이해하는 상대적 쾌락주의에 지배 받게 된다.

제 2수준인 인습 수준은 타율적인 도덕성 수준으로 가정이나 사회 등 집단의 기대를 따르는 것이 그 결과와는 상관없이 가치를 지니는 것이라고 판단하며, 단순히 사회의 정서에 피동적으로 동화하는 것이 아니라 적극적으로 질서를 유지하고 정당화하는 것은 물론 힘 있는 사람과 동일시하려는 경향을 보인다. 또한 다른 사람의 상호작용을 고려한 사회 지향적 가치기준을 가지게 된다. 구체적으로 제 2수준에 포함된 3단계 객체화에서 올바른 행위란 다른 사람을 기쁘게 하고 도와주고 다른 사람은 그 행위를 인정하는 것으로 대인 관계 및 타인의 승인을 중시한다. 콜버그는 이를 착한 소년/소녀 지향이라고도 하였으며 이 단계에 비로소 행위자의 의도나 내적특성을 고려하게 된다. 4단계 사회화는 법과 질서를 준수하고 사회 속에서 개인의 의무를 다한다. 이 단계에서 올바른 행동이란 자신의 의무와 책임을

수행하고, 합법적 권위를 존중함으로써 사회적 질서를 유지하는 행동이다. 그러나 아직 소수의 권리에 대한 예리한 감각은 없으며 가장 성숙한 측면이 탈 인습적 측면으로 도덕적 관습이 이해되는 단계이다.

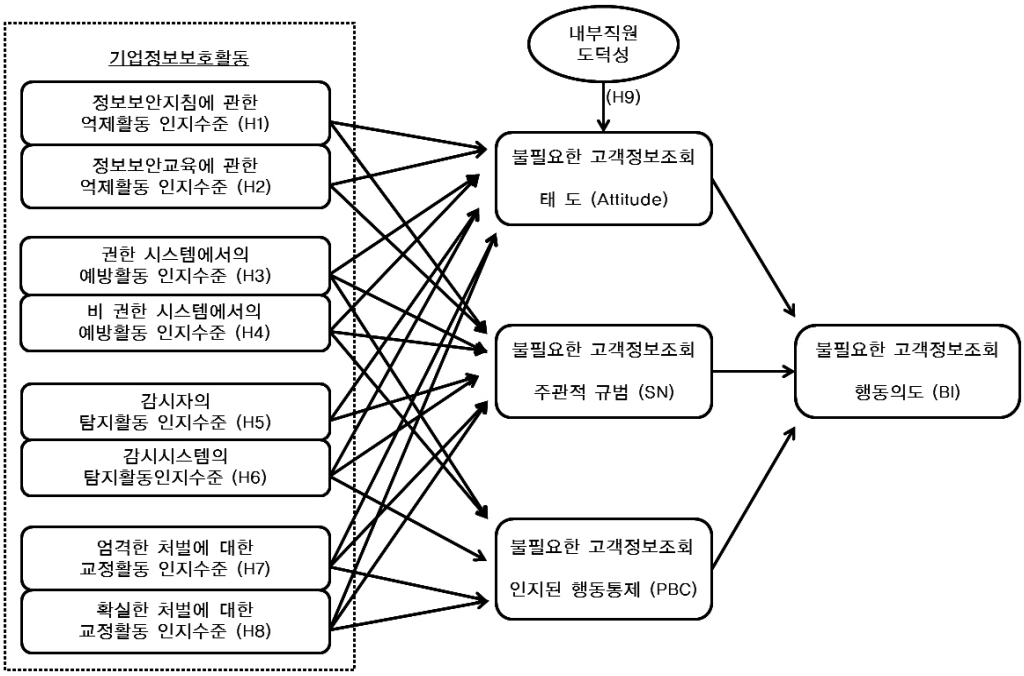
제 3수준인 인습 이후 수준은 자율적인 도덕성 수준으로 자신의 가치관과 도덕적 원리원칙이 자신이 속한 집단과 별개임을 깨닫게 되면서 개인의 양심에 근거하여 행위를 하게 된다. 구체적으로 제 3수준에 포함된 5단계 일반화는 인간으로서의 기본원리에 따라 행동하며 사회적 책임으로써의 공리주의, 가치기준의 일반화를 추구한다. 이 단계의 사람들은 신념이 서로 다른 사람들의 상호 유익한 합의를 시도한다. 그러므로 소수까지 포함된 모든 개인의 권리가 인정되는 것이 모두의 관심거리가 된다. 이 단계에서 올바른 행동은 개인의 기본권리와 사회 전체가 합의에 도달한 도덕기준에 비추어 규정된다. 사회적 합의로서의 법과 제도가 중요시되지만 사회적 유용성이나 합리성에 따라 법과 제도가 바뀔 수도 있다는 사실 또한 중요시하게 된다. 즉, 자유, 정의, 행복추구 등의 제도적 가치가 법보다 상위에 있음을 약간 인식하는 단계이다. 6단계 궁극화는 사회적 질서에 대한 것이 아니라, 모든 사회와 모든 사람을 결속시키는 도덕적 원칙에 대한 존중이 극에 달하게 되는 단계로 법이나 관습 이전에 인간 생명이 관여된 문제로 생명의 가치를 무엇보다도 우선하며 보편적 도덕원리를 지향한다. 따라서 스스로 선택한 도덕 원리, 양심의 결단에 따르는 특징을 보인다. 이 단계에서 올바른 행위는 스스로 선택한 도덕원리에 따르는 것으로 정의되는데 여기서 도덕원리란 공정성, 정의, 인간권리의 상호성과 평등성, 인간 존엄성에 대한 존중을 포함한다.

이러한 콜버그의 도덕발달단계의 특징은 각 발달단계가 순서대로 진행된다고 가정하며 일단 한 사람이 도덕적 발달의 상위단계에 도달하면 결코 전 단계로 퇴행하지 않는다는 것이다. 극단적으로 신체적, 정신적, 손상을 입은 경우를 제외하고 사람은 반드시 순서에 따라 각 단계를 거쳐간다. 다시 말해서 도덕발달은 다른 모든 발달처럼 일정한 원칙을 가지고 진행되므로 하룻밤 사이에 도덕군자로 변신할 수 없다는 것이다. 도덕발달의 또 다른 특징은 계층적 통합을 이루고 있다는 것이다. 낮은 단계는 높은 단계의 도덕적 추론을 이해하지 못하지만, 높은 단계는 낮은 단계의 도덕적 추론을 포괄하고 이해한다. 단계의 이동은 도덕적 추론을 구성하고 있는 일련의 인지적 구조가 재조정되는 것을 의미한다. 도덕적 난관에 부딪혔을 때 그것을 해결하려는 인지적 판단이 서지 못한 상태를 불균형이라 하는데 이러한 딜레마적 상황에서 현재의 인지적 판단으로 해결하지 못하는 경우 새로운 인지적 구조로 전환하여 해결해 나가는 것을 의미한다. 콜버그는 도덕발달이 멈추거나 한 단계에 고착되는 이유는 개인이 현재 수준의 도덕적 추론방식을 반성할 충분한 기회가 없었기 때문이라고 주장한다[문용린, 2000].

이러한 도덕발달이론을 토대로 볼 때, 금융회사의 내부직원이 업무 이외에 불필요한 고객정보조회를 하는데 있어 직원 개인의 도덕수준이 영향을 줄 것이다. 즉, 도덕수준이 높은 내부직원은 그냥 범죄적 행동 자체가 옳지 않다고 믿기 때문에 불필요한 고객정보조회를 하지 않을 것이다[Akers and Sellers, 2005; pp. 50-51]. 이러한 논리를 검증하기 위해 다음 장의 가설 9를 세웠다.

Ⅲ. 연구 모형과 가설

앞 부분에서 논의된 연구 배경을 바탕으로 우리는 <그림 4>와 같은 연구 모형을 제시하였다. 어떠한 가설이 어떤 이론에 근거하였는지는 앞의 장에서 설명한 바와 같다.



<그림 4> 연구모형

H1a: 정보보안지침은 불필요한 고객정보조회에 대한 내부직원의 태도에 (-)영향을 미칠 것이다.

H1b: 정보보안지침은 불필요한 고객정보조회에 대한 내부직원의 주관적 규범에 (-)영향을 미칠 것이다.

H2a: 정보보안교육은 불필요한 고객정보조회에 대한 내부직원의 태도에 (-)영향을 미칠 것이다.

H2b: 정보보안교육은 불필요한 고객정보조회에 대한 내부직원의 주관적 규범에 (-)영향을 미칠 것이다.

H3a: 접근이 가능한 시스템에서 고객정보조회가 복잡할수록 불필요한 정보조회에 대한 내부직원의 태도에 (-)영향을 미칠 것이다.

H3b: 접근이 가능한 시스템에서 고객정보조회가 복잡할수록 불필요한 정보조회에 대한 내부직원의 주관적 규범에 (-)영향을 미칠 것이다.

H3c: 접근이 가능한 시스템에서 고객정보조회가 복잡할수록 불필요한 정보조회에 대한 내부직원의 인지된 행동통제에 (-)영향을 미칠 것이다.

H4a: 물리적으로 시스템 접근이 복잡할수록 불필요한 정보조회에 대한 내부직원의 태도에 (-)영향을 미칠 것이다.

H4b: 물리적으로 시스템 접근이 복잡할수록 불필요한 정보조회에 대한 내부직원의 주관적 규범에 (-)영향을 미칠 것이다.

H4c: 물리적으로 시스템 접근이 복잡할수록 불필요한 정보조회에 대한 내부직원의 인지된 행동통제에 (-)영향을 미칠 것이다.

H5a: 감시자의 감시활동은 불필요한 정보조회에 대한 내부직원의 태도에 (-)영향을 미칠 것이다.

H5b: 감시자의 감시활동은 불필요한 정보조회에 대한 내부직원의 주관적 규범에 (-)영향을 미칠 것이다.

H6a: 감시 시스템의 감시활동은 불필요한 정보조회에 대한 내부직원의 태도에 (-)영향을 미칠 것이다.

H6b: 감시 시스템의 감시활동은 불필요한 정보조회에 대한 내부직원의 주관적 규범에 (-)영향을 미칠 것이다.

H6c: 감시 시스템의 감시활동은 불필요한 정보조회에 대한 내부직원의 인지된 행동통제에 (-)영향을 미칠 것이다.

H7a: 처벌의 엄격성은 불필요한 정보조회에 대한 내부직원의 태도에 (-)영향을 미칠 것이다.

H7b: 처벌의 엄격성은 불필요한 정보조회에 대한 내부직원의 주관적 규범에 (-)영향을 미칠 것이다.

H7c: 처벌의 엄격성은 불필요한 정보조회에 대한 내부직원의 인지된 행동통제에 (-)영향을 미칠 것이다.

H8a: 처벌의 확실성은 불필요한 정보조회에 대한 내부직원의 태도에 (-)영향을 미칠 것이다.

H8b: 처벌의 확실성은 불필요한 정보조회에 대한 내부직원의 주관적 규범에 (-)영향을 미칠 것이다.

H8c: 처벌의 확실성은 불필요한 정보조회에 대한 내부직원의 인지된 행동통제에 (-)영향을 미칠 것이다.

H9: 내부직원의 도덕성은 불필요한 정보조회에 대한 내부직원의 태도에 (-)영향을 미칠 것이다.

Ⅳ. 연구방법 및 설계

금융회사는 개인정보 중에서도 금융정보를 다루기 때문에 보안에 민감하고 그 정보의 가치는 상대적으로 중요하다. 이러한 금융회사의 특성을 고려하여 연구 분석의 질을 높이고자 금융회사 중에서 상대적으로 고객정보 보유량이 많은 카드회사들을 조사대상 기업으로 하였고(이기현, 서의진, 2011; p. 24) 모집단인 내부직원의 표본은 다량의 개인정보 접근이 용이하고 활용도 빈번하여 그 만큼 잠재적 개인정보유출 가능성이 높은 고객접점의 콜센터 상담원들을 대상으로 하였다. 조사방법은 미리 준비된 설문지를 익명의 자기기입식 질문지법으로 2011년 7월 중 배포하였으며 160개를 수거, 그 중 무효한 설문지 26개를 제외한 134개 설문지를 분석대상으로 하였다. 설문조사의 내용이 내부직원이 아닌 일반인이 상식적으로 생각하기에 범죄적 행동으로 인식할 수도 있는 질문으로 구성되었기 때문에 조사 대상기업의 회사가 노출되지 않는다는 조건으로 관리자의 승인을 받아 설문조사를 실시하였고 조사 대상자인 상담원들의 신상조사는 최소화하여 설문응답의 부담을 줄이는데 노력하였다. 또한 상담원들의 성의 있는 응답을 유도하기 위해 1:1 면접방식에 의해 설문을 작성하도록 하였고 이러한 설문작성에 대한 소정의 보상금도 지불하였다.

수집된 설문자료들은 타당도 검증을 위한 탐색적 요인분석을 실시하여 일부 항목을 제거하였다. 모든 측정변수는 구성요인을 추출하기 위해 주성분 분석을 사용하였으며 요인적재치의 단순화를 위해 직교회전 방식을 채택 하였다. 총 49문항 중 8문항이 이론 구조에 맞지 않게 적재되어 제거하였고 최종적으로 41개 문항을 분석에 이용하였다. 요인분석결과 변수들 간의 상관관계가 다른 변수에 의해 잘 설명되는 정도를 나타내는 KMO는 0.792로 나타났으며 나머지 측정치는 <표 1>에 제시하였다.

H1, H2에 해당하는 억제활동을 측정하기 위해서는 행위자인 내부직원이 해당기업의 정보보안 정책에 대해 얼마나 인지하고 있는지를 측정해야 하지만 실제로 내부직원의 정보보안정책 인지수준을 측정할 수 있는 객관화된 척도는 찾을 수 없었기 때문에 정보보안 정책 전달 수단인 정보보안 지침과 정보보안 교육의 유용성을 측정하여 간접적으로 억제활동에 대한 내부직원의 인지수준을 측정하였다. 따라서 억제활동의 척도는 기술수용이론(Technology Acceptance Model: TAM)의 인지된

<표 1> 요인 분석

개념	요인	고유 값	분산설명력
기업정보 보호활동	억제활동	6.311	12.879
	교정활동	5.396	11.012
	예방활동(비 권한 접근)	4.465	9.113
	예방활동(권한 접근)	4.063	8.293
	탐지활동(감시인)	3.520	7.183
	탐지활동(감시시스템)	3.333	6.803
	도덕성	2.785	5.683
계획된 행동이론 (TBP)	태도(Attitude)	2.763	5.640
	행동의도(BI)	2.268	4.628
	주관적 규범(SN)	1.878	3.832
	인지된 행동통제(PBC)	1.826	3.727

유용성 척도를 이용하여[Davis, 1989] '정보보안 지침의 인지된 유용성'과 '정보보안교육의 인지된 유용성'을 억제활동을 측정하는 변수로 사용하려고 하였다. 하지만 요인분석에서 이 두 변수는 같은 요인으로 추출되었기 되었기 때문에 실제 분석에서는 이 두 변수를 결합한 '억제활동의 인지된 유용성'을 실제 측정변수로 이용하였다. 이와 같이 두 변수가 같은 요인으로 추출된 이유는 조사대상인 상담원들이 실제 업무에서 정보보안지침과 정보보안교육에 대한 경험이 부족해 서로 구분하지 못하고 동일하게 인식하기 때문으로 풀이된다. 또 다른 가능성은 조사대상이 실제 업무에서 정보보안지침과 정보보안교육을 동시에 수행함으로써 상담원들의 인식에 혼란을 주었을 가능성도 배제할 수 없다.

H3, H4에 해당하는 예방활동을 측정하기 위해서는 행위자인 내부직원이 정보조회의 결과를 추출(정보습득)하기까지 얼마나 어려운가 또는 복잡한가에 대한 인지수준을 측정해야 한다. 구체적으로 기업이 취하는 예방활동은 내부직원이 정보를 습득하기까지 쉽게 그 해당정보를 습득을 할 수 없도록 하기 위한 조치로 난관이나 방해물들을 설치하는 것이다. 이렇게 난관이나 방해물은 정보조회를 위한 시스템 내의 처리는 동일하지만 물리적인 환경에 접근권한 유무에 따라서는 차이를 나타낼 것이다[Triandis, 1979]. 예방 활동의 척도는 TPB with belief decomposition의 인지된 복잡성 척도를 이용하여[Taylor and Todd, 1995] '권한 시스템의 인지된 복잡성'과 '비권한 시스템의 인지된 복잡성'을 예방활동을 측정하는 변수로 이용하였다.

H5, H6에 해당하는 감시활동을 측정하기 위해서는 행위자인 내부직원이 해당기업으로부터 받는 감시수준을 얼마나 인지하고 있는지를 측정해야 한다. 측정방법은 우선 ISMS를 참고하여 사람(감시인)과 시스템(감시 시스템)으로 구분하고 이미 조사대상기업의 탐색조사와 관리자의 인터뷰 통해 얻는 실제 감시체계를 적용하여 내부직원이 기업의 실제 감시체계를 얼마나 인지하고 있는지를 측정하였다. 감시활동의 척도는 이러한 실제 감시체계로부터 내부직원이 받는 인지수준을 적용하여 '감시인에 대한 인지수준'과 '감시 시스템에 대한 인지수준'을 탐지활동을 측정하는 변수로 이용하였다.

H7, H8에 해당하는 교정활동을 측정하기 위해서는 행위자인 내부직원이 해당기업의 처벌수준을 얼마나 인지하고 있는지를 측정해야 한다. 교정활동의 척도는 억제이론의 처벌효과의 척도인 '처벌의 엄격성'과 '처벌의 확실성'을 교정활동을 측정하는 변수로 이용하였다[Tittle, 1980]. 하지만 요인분석에서 이 두 변수는 같은 요인으로 추출되었기 때문에 실제 분석에서는 이 두 요인을 결합하여 '교정활동의 인지수준'을 실제 교정활동을 측정하는 변수로 이용하였다. 이와 같은 결과는 조사대상인 상담원들이 '처벌의 엄격성'과 '처벌

의 확실성'에 대한 개념을 구분하지 못하고 동일하게 인식하거나 두 변수의 중요성을 동일하게 인식하고 있기 때문으로 추정된다. 마지막으로 H9에 해당하는 내부직원의 도덕성 측정은 설문조사의 시간적 공간적 제약조건을 고려하여 Rest의 DIT의 전체단계 중 6단계의 척도만을 이용하여 도덕성 수준을 측정하였다.

지금까지의 모든 변수는 Likert 5점 척도로 구성하였고 분석방법은 SPSS 회귀분석을 통해 인과관계를 측정하여 제시하였다. <표 2>와 같이 인구통계학적 특성을 통제 변수로 이용하여 연구의 타당성을 고려하였다. 특징적인 것은 상담원이 정규사원(2년 이상)이냐 파견사원(2년 미만)이냐에 따라 측정결과에 영향을 미칠 수 있기 때문에 재직기간을 통제변수로 활용하였고 금융회사의 경우는 S사와 ABC사 두 카드회사를 대상으로 조사하였는데 <표 2>에 제시된 ABC사를 세분화한 이유는 같은 회사이지만 업무가 다른 부서나 팀에 따라 연구에 영향을 줄 수 있다고 판단하여 표본을 팀별로 구분하여 통제변수로 활용하였다.

<표 2> 인구통계학적 특성

구 분		빈도수(명)	구성비율(%)
성별	여자	78	58.2
	남자	56	41.8
나이	25세 이하	33	24.6
	26~30세	53	39.6
	31세 이상	48	35.8
학력	고졸 이하	43	32.1
	초대(재)졸	48	35.8
	대(재)졸 이상	43	32.1
재직기간	3개월 미만	29	21.6
	3~6개월	31	23.1
	6~12개월	23	17.2
	1~2년	13	9.7
	2년 이상	38	28.4
금융회사	S사	11	8.2
	A사	54	40.3
	B사	43	32.1
	C사	26	19.4

Ⅴ. 분석 및 결과

앞서 제시된 가설들을 검증하기 위해서는 우선 기본연구 모형인 TPB 모형의 영향관계가 유의미하게 나와야 하는데 이러한 결과는 <표 3>에 잘 나타나 있다. 불필요한 정보조회에 대한 내부직원의 태도, 주관적 규범, 인지된 행동통제가 각각 0.000, 0.016, 0.000으로 통계적 유의수준 하에서 불필요한 정보조회의 행동의도에 (+)의 영향을 미치는 것으로 나타나 선행연구의 TPB의 기본가설을 증명하였다. 따라서 본 연구의 TPB 모형은 가설을 검증하는데 적합한 기반을 제공하는 것으로 나타났다.

<표 3> TPB 모형 회귀분석

종속변수	독립변수	통제변수			모델		
		SE	β	t값(유의도)	SE	β	t값(유의도)
행동의도	상수	0.332		7.067(0.000)	0.355		0.563(0.574)
	금융회사	0.300	-0.185	-2.010(0.047)	0.240	-0.070	-0.946(0.346)
	성별	0.160	0.084	0.958(0.340)	0.131	-0.043	-0.595(0.553)
	나이	0.170	0.071	0.782(0.436)	0.136	0.062	0.854(0.395)
	학력	0.166	-0.038	-0.438(0.662)	0.131	0.004	0.060(0.952)
	재직기간	0.054	0.105	1.124(0.263)	0.043	-0.009	-0.121(0.604)
	태도				**0.069**	**0.289**	**3.765(0.000)**
	주관적 규범				**0.078**	**0.195**	**2.449(0.016)**
	인지된 행동통제				**0.067**	**0.373**	**4.952(0.000)**
	통계량	R^2 = 0.060, 수정된 R^2 = 0.023 F = 1.627, p = 0.158			R^2 = 0.436, 수정된 R^2 = 0.400 F = 12.069, p = 0.000 Durbin-Watson = 1.956		

아래 제시된 <표 4> ~ <표 6>는 독립변수인 기업의 정보보호활동이 불필요한 정보조회에 대한 내부직원의 태도, 주관적 규범, 인지된 행동통제에 미치는 영향을 다중회귀 분석한 결과표이다. 결과에 따르면 억제활동과 관련한 모든 종속변수들과의 인과관계에서 유의미하지 않게 나타나 H1, H2는 모두 기각되었다. 이것은 억제활동과 관련한 해당기업의 정보보안정책이 내부직원이 불필요한 정보조회를 하는데 있어서 별다른 영향을 주지 못했거나 정보보안 지침이나 정보보안교육이 내부직원에게 정보보안 정책을 제대로 전달하지 못하는 데서 그 원인을 찾을 수 있다. 어떠한 원인이든 금융회사는 고객의 개인정보보호가 의무사항으로 이러한 의무사항을 내부직원

<표 4> 종속변수가 태도인 회귀분석

종속변수	독립변수	통제변수			모델		
		SE	β	t값(유의도)	SE	β	t값(유의도)
태도	상수	0.354		6.612(0.000)	0.729		6.008(0.000)
	금융회사	0.319	-0.082	-0.919(0.360)	0.326	-0.065	-0.0720(0.473)
	성별	0.170	-0.291	3.433(0.001)	0.176	0.217	2.466(0.015)
	나이	0.181	-0.002	0.026(0.979)	0.182	-0.052	-0.584(0.560)
	학력	0.177	-0.105	-1.257(0.211)	0.76	-0.153	-1.833(0.069)
	재직기간	0.058	0.159	1.780(0.078)	0.061	0.184	1.963(0.052)
	억제활동				**0.148**	**-0.116**	**-1.254(0.212)**
	예방(권한접근)				**0.120**	**0.192**	**1.910(0.058)**
	예방(비 권한접근)				0.110	-0.169	-1.726(0.087)
	탐지(감시인)				0.122	0.127	-1.255(0.212)
	탐지(감시 시스템)				0.135	0.051	0.460(0.646)
	교정(처벌)				**0.118**	**-0.216**	**-2.322(0.022)**
	통계량	R^2 = 0.128, 수정된 R^2 = 0.094 F = 3.772, p = 0.003			R^2 = 0.233, 수정된 R^2 = 0.164 F = 3.372, p = 0.001 Durbin-Watson = 1.914		

<표 5> 종속변수가 주관적 규범인 회귀분석

종속변수	독립변수	통제변수			모델		
		SE	β	t값(유의도)	SE	β	t값(유의도)
SN	상수	0.339		8.853(0.000)	0.689		7.445(0.000)
	금융회사	0.306	-0.196	-2.135(0.035)	0.308	-0.123	-1.336(0.184)
	성별	0.163	0.107	1.222(0.224)	0.167	0.079	-0.880(0.381)
	나이	0.174	-0.115	-1.266(0.208)	0.172	-0.112	-1.241(0.217)
	학력	0.169	-0.018	-0.209(0.835)	0.167	-0.020	-0.235(0.814)
	재직기간	0.056	0.171	1.843(0.068)	0.057	0.118	1.241(0.217)
	억제활동				0.140	0.001	0.010(0.992)
	예방(권한접근)				0.114	-0.151	-1.470(0.144)
	예방(비 권한접근)				0.104	-0.069	-0.692(0.490)
	탐지(감시인)				0.116	-0.038	-0.366(0.715)
	탐지(감시 시스템)				0.127	-0.046	-0.411(0.682)
	교정활동				**0.111**	**-0.248**	**-2.613(0.010)**
	통계량	R^2 = 0.068, 수정된 R^2 = 0.032 F = 1.866, p = 0.105			R^2 = 0.203, 수정된 R^2 = 0.131 F = 2.829, p = 0.003 Durbin-Watson = 1.772		

<표 6> 종속변수가 인지적 행동통제인 회귀분석

종속변수	독립변수	통제변수			모델		
		SE	β	t값(유의도)	SE	β	t값(유의도)
PBC	상수	0.380		7.712(0.000)	0.639		9.236(0.000)
	금융회사	0.343	-0.144	-1.547(0.124)	0.313	-0.059	-0.698(0.486)
	성별	0.183	0.060	-0.672(0.503)	0.174	0.016	-0.191(0.849)
	나이	0.195	0.083	0.903(0.368)	0.181	0.113	1.316(0.190)
	학력	0.190	0.022	-0.253(0.801)	0.173	-0.019	-0.234(0.815)
	재직기간	0.062	0.092	0.976(0.331)	0.060	-0.007	-0.075(0.940)
	예방(권한접근)				**0.115**	**-0.248**	**-2.645(0.009)**
	예방(비 권한 접근)				0.108	-0.136	-1.443(0.151)
	탐지(감시 시스템)				0.116	-0.045	-0.483(0.630)
	교정활동				**0.116**	**-0.268**	**-3.008(0.003)**
	통계량	R^2 = 0.042, 수정된 R^2 = 0.004 F = 1.118, p = 0.354			R^2 = 0.260, 수정된 R^2 = 0.206 F = 4.845, p = 0.000 Durbin-Watson = 1.951		

이 반드시 인지할 수 있도록 해야 함에도 불구하고 해당기업의 억제활동은 내부직원에게 별다른 영향을 주지 못하는 것으로 나타났다. 물론 이직률이 높은 상담원의 직업적 특성 때문에 장기적이고 전략적인 계획이 필요할 수도 있는 억제활동의 영향이 미미할 수도 있겠으나 기업은 그 직업적 특성에 맞추어 내부직원이 회사의 정보보안 정책을 인지할 수 있도록 억제활동을 재구성해야 필요가 있다고 판단된다.

예방활동과 관련한 모든 종속변수들과의 인과관계에서 H3a, H3b와 H4b, H4c는 기각되었지만 H3c(-2.645), H4a(-1.726)은 채택되어 내부직원의 불필요한 정보조회에 대해 예방활동은 부분적으로 효과가 있는 것으로 분석되었다. 하지만 H3a의 경우 가설의 의도와는 반대로 (-)영향이 (+1.910)영향으로 유의미하게 나타나 불필요한 정보조회를 하는 내부직원의 태도에는 오히려 긍정적 영향을 주는 것으로 분석되었다. 이것은 측정척도인 복잡성의 특성으로 기인한 것으로 풀이된다. 인지복잡성 이론에 따르면 어떤 대상이 체계적인 복잡성을 가질 때 개인은 좀 더 관심을 가지고 구체적으로 평가하려고 하는 성향을 보이지만 개인의 인지능력 한계이상으로 복잡성을 가질 경우 일반화시키기 위한 통제 신념이 작용하게 된다[Rauterberg, 1996]. 즉, 사전에 접근권한을 가지고 있는 시스템에서 상담원들은 실제업무인 정보조회가 복잡하고 어려울수록 호기심을 가지게 되고 그 가치를 평가하는 개인의 성향으로 인해 그 상담원의 태도에는 긍정적 영향을 나타냈으나 그 복잡하고 어려운 한계를 넘으면 통제를 할 수 있는 영역을 벗어나기 때문에 이를 일반화시키기 위한 노력이 작용하게 되어 상담원들의 행동통제에는 부정적 영향을 미치는 딜레마적 분석결과가 나타나게 된 것으로 판단된다. 결국 분석결과를 종합해보면, 금융회사는 딜레마적 성격이 나타나는 접근권한을 가진 시스템의 경우는 예방활동의 수준을 조절할 필요가 있으며 사전에 접근권한이 없었던 외부시스템으로부터의 예방활동은 강화시킬 필요가 있을 것으로 판단된다. 즉, 시스템 내의 정보조회에 대한 예방활동 보다는 물리적인 시스템 접근성을 엄격하고 복잡하게 하는 것이 좀 더 효과적인 정보보호활동으로 판단해 볼 수 있다.

감시활동과 관련한 모든 종속변수들과의 인과관계에서 H5, H6은 모두 기각되었다. 이러한 결과는 실제 업무환경에서 상담원들이 기업의 비밀스러운 감시활동을 인지하지 못하고 있거나 감시활동을 설사 인지한다 하더라도 초기에는 다소 효과를 보일 뿐 지속적인 감시활동으로 인해 시간이

<표 7> 도덕성과 태도의 회귀분석

종속변수	독립변수	통제변수			모델		
		SE	β	t값(유의도)	SE	β	t값(유의도)
태도	상수	0.354		6.612(0.000)	0.495		3.277(0.001)
	금융회사	0.319	-0.082	-0.919(0.360)	0.315	-0.081	-0.921(0.359)
	성별	0.170	0.291	3.433(0.001)	0.174	0.246	2.836(0.005)
	나이	0.181	0.002	0.026(0.979)	0.179	0.000	-0.003(0.997)
	학력	0.177	-0.105	-1.257(0.211)	0.178	-0.073	-0.864(0.389)
	재직기간	0.058	0.159	1.780(0.078)	0.057	0.164	1.858(0.066)
	도덕성				**0.112**	**0.177**	**2.050(0.042)**
	통계량	R^2 = 0.128, 수정된 R^2 = 0.094 F = 3.772, p = 0.003			R^2 = 0.156, 수정된 R^2 = 0.116 F = 3.922, p = 0.001		

지나면서 차츰 익숙해지고 무감각해지는 현상에서 추정할 수 있다. 따라서 기업이 정보보호를 위한 감시활동의 효과를 보기 위해서는 상담원들이 감시 대상자로서 감시활동을 인지할 수 있도록 하는 노출된 감시활동을 하거나 감시활동으로 적발된 경우의 징계사항을 사전에 고지함으로써 감시활동의 지각을 높이는 노력이 필요할 것으로 판단된다.

교정활동과 관련한 모든 종속변수들과의 인과관계에서 H7, H8가 모두 채택되었다. H7과 H8은 요인분석에서 하나의 변수로 정제하여 분석하였기 때문에 하나의 분석결과로 도출하였다. 우선 유의수준을 가늠할 수 있는 t값과 p값은 전체적으로 모두 유의한 결과를 나타냈다. H7과 H8은 각 a(-2.322), b(-2.613), c(-3.008)로 지지되었다. 이와 같은 결과는 앞서 제시된 다른 어떠한 정보보호활동보다도 교정활동의 인지수준이 내부직원의 불필요한 정보조회에 대해 가장 강력한 억제효과를 나타내고 있음을 증명하고 있다.

내부직원의 개인적 특성인 도덕성과 관련된 H9은 부정적 영향을 미쳐야 할 가설검증이 긍정적으로 유의미하게 나타나면서 기각되었다. 이와 같은 결과는 상담원들이 쉽게 저지를 수 있는 '업무 이외의 불필요한 정보조회'가 일반인들에게는 확실한 문제행동으로 인식하는 반면에 실제업무 환경에서의 상담원들은 문제행동으로 인식하기에는 다소 무리가 있다고 판단하는 것으로 풀이된다. 이와 같은 결과를 해석하기 위해서는 우선 '문제행동'의 개념을 알 필요가 있다. 문제행동은 비행, 일탈행동, 부적응 행동, 비윤리적 행동 등 다양한 용어들로 혼용되고 있는데 범죄행동보다는 비교적 강도가 약하고 가벼운 행동을 일컫는다[정문성, 구정화, 1991]. 문제행동의 개념은 '사회체제 속에서 정당화된 것으로 인식되고 공유되는 제도화된 기제들을 위반하는 것[Cohen, 1959; p. 462]', '사회 속에서 사람들을 위해 마련된 규준에서 현저하게 벗어난 행동[Merton, 1961; pp. 723-724]', '지역사회의 인내한계를 충분히 초과하는 정도의 행동으로써 동의 받지 못하는 방향으로 행해진 행동[Clinard, 1963; p. 22]' 등으로 학자에 따라 다양하게 정의되고 있으나 이들의 개념들을 포괄하는 개념이 Docking[1989; pp. 6-8]의 '좋은 행동'의 개념이다. Docking은 좋은 행동을 '사회적으로 허용되는 행동', '자기 통제적인 행동', '책임 있는 행동'으로 규정하였는데 이와 반대되는 행동이 '사회적으로 허용되지 않는 행동', '자기 통제가 안 되는 행동', '무책임한 행동'을 문제행동으로 정의할 수 있을 것이다[정문성, 구정화, 1991].

그렇다면 상담원들은 과연 불필요한 정보조회를 어떠한 행동으로 인식하고 있는지를 확인해 볼 필요가 있다. 이러한 의문을 해결하기 위해서는 상담원의 업무특성을 우선 파악할 필요가 있다. 우선 조사대상 기업이 요구하는 최고의 상담원은 전화로 인입된 고객의 성향을 잘 파악하여 신속하고 정확하게 고객의 요구를 해결하고 고객이 미처

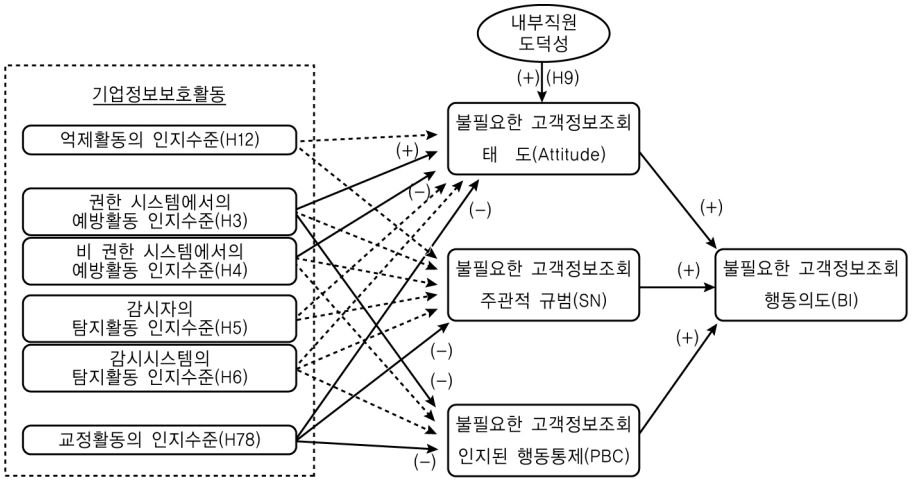
생각하지 못한 부분까지 배려함으로써 고객감동을 실천하는 인재상이라고 한다. 특히, VIP 고객, Black List 고객의 경우 그 고객의 개인정보를 알고 싶지 않아도 알 수밖에 없는 업무환경에 있으며 미리 알아야만 그 고객의 요구 사항에 적절하게 응대할 수가 있다고 한다. 이와 더불어 상담원들은 회사에서 요구하는 사항을 처리하기 위해 고객의 개인정보가 수시로 필요할 경우도 있다고 한다. 그렇다면 이렇게 지속적으로 다량의 고객정보를 조회하고 활용하는 직원의 업무환경에서 어디까지가 업무에 필요한 정보조회이고 어디까지가 업무 이외의 불필요한 정보조회인지를 상담원들이 과연 구분할 수 있을 것인가에 의문을 가지게 된다. 앞서 감시활동의 결과에 대한 해석과 마찬가지로 처음에는 상담원들도 불필요한 정보조회가 문제행동으로 인식할 수도 있었을 것이다. 하지만 다량의 정보조회를 지속적으로 하다 보면 익숙해지고 이것이 불필요한 정보조회이든 아니든 문제행동으로 인식하면서 행동하는 것에 무감각해질 가능성이 있다고 판단된다.

<표 8>에서 보듯이 실제 설문에서 조사대상인 상담원들이 불필요한 정보조회에 대해 행동의도를 제외한 나머지 태도, 주관적 규범, 인지된 행동통제 대해 평균이상으로 긍정적 응답한 사람이 더 많다. 또한 불필요한 정보조회에 대한 행동의도가 있다고 응답한 사람도 36명 이상이다. 이렇게 응답한 상담원들이 모두 불필요한 정보조회가 문제행동으로 인식하면서 설문에 응답했다고 하기는 다소 무리가 있어 보인다. 빈번하게 고객정보를 조회하고 활용해야 하는 상담원들이 업무상 불필요하다고 정보조회를 문제행동으로 인식하기는 어려울 수 있다고 생각한다. 결과적으로 불필요한 정보조회에 대한 일반인의 인식과 일선의 내부직원의 인식에는 다소 차이가 있는 것으로 나타났다.

<표 8> 불필요한 정보조회에 대한 빈도분석

구 분		빈도수	평균
불필요한 정보조회 직원의 행동의도	2.5 미만	98	2.09
	2.5 이상	36	
불필요한 정보조회 직원의 태도	2.5 미만	53	2.65
	2.5 이상	81	
불필요한 정보조회 직원의 주관적 규범	2.5 미만	43	2.74
	2.5 이상	91	
불필요한 정보조회 직원의 인지적 행동통제	2.5 미만	48	2.75
	2.5 이상	86	

<그림 5>는 지금까지 분석한 종합적인 결과를 제시한 연구모형이다.



<그림 5> 연구 결과

Ⅵ. 결 론

위 연구결과에 따르면 금융회사의 내부직원에 의한 불필요한 고객정보조회를 가장 효과적으로 억제시키기 위한 방법은 처벌이 엄격하고 확실하게 적용될 것이라는 인식을 심어주는 것이다. 이와 같은 결과는 과거 많은 논문에서 이미 처벌효과에 대한 많은 연구결과로써 증명한 바 있다. 이러한 교정활동과 관련한 처벌효과 외에도 예방활동으로서 물리적인 시스템의 접근을 엄격하고 복잡하게 프로세스 한다면 내부직원에 의한 불필요한 고객정보조회를 억제시키는데 다소 효과가 있는 것으로 나타났다. 구체적인 방법으로 사전 접근권한이 없었던 시스템을 접근하기 위한 접근권한의 허가절차를 보다 엄격하고 까다롭게 하거나 그 외부 시스템에 접근하기까지의 물리적 보안장치(출입통제 보안장치, 경비시스템)를 좀 더 강화시키는 것도 효과적일 수 있을 것이다.

한편, 내부직원의 도덕성을 측정하여 분석함으로써 내부직원의 불필요한 정보조회에 대해 일반인의 인식과 일선의 내부직원의 인식에는 다소 차이가 있다는 것을 알았다. 하지만 이 같은 분석결과에는 다소 측정상의 한계가 있었다. 이론적 배경에서 밝힌 도덕발단 전 단계를 모두 측정할 경우 측정문항 과대로 인한 측정의 오류가 있을 수 있을 것을 우려하여 6단계의 도덕성여부 판단하였다. 이러한 한계로 정확한 도덕성 수준을 측정했다고 보기는 어렵다고 생각되며 도덕성과 문제행동 간의 관계도 선행연구마다 달라 명확한 이론적 배경을 설명하기에는 한계가 있음을 인정한다. 또한, 콜버그의 도덕성 발달이론은 자유주의적, 개인주의적인 서구문화를 바탕으로 한 것이라는 점에서 모든 문화에 보편적으로 적용하기에는 한계가 있다. 즉, 본 연구에서 정의한 콜버그의 도덕 판단력이 도덕적 행위와 일치하는가에 대해서는 앞으로 좀 더 많은 연구가 필요하다고 생각한다. 향 후 연구에서는 미흡했던 도덕성에 관한 자세한 연구를 할 것이며, 만약 이러한 연구를 통해 도덕발달 단계를 전부 측정함으로써 유의미한 결과가 나타난다면 금융회사에서 직원채용 시 도덕성 검사를 활용하는데 있어서 중요한 근거로 제시될 수 있다고 생각한다.

본 연구의 또 다른 한계점이라면 연구목적의 특성과 조사대상의 제약으로 많은 표본을 수집할 수가 없었다는 것이다. 따라서 이렇게 제한된 표본으로 분석된 결과를 일반화 할 수 있을지는 본인도 자신할 수는 없다. PIMS 인증을 받은 금융회사들은 표면적인 보안환경에 있어서는 큰 차이를 보이지는 않는다[인터넷진흥원, 2008]. 다만 기업에 따라, 부서에 따라, 업무에 따라 그 기업의 내부직원이 인지수준에는 영향을 미칠 수 있다고 생각한다. 이러한 인지 정도의 차이가 분석결과에 차이를 나타낼 가능성이 있다. 따라서 향 후 추가적인 표본의 수를 늘린다면 좀 더 타당성 있는 연구가 될 수 있을 것으로 기대한다.

한편, 본 연구의 연구모형에서 행동(Behavior) 변수는 측정하지 않았다. 사실 합리적 행동이론(TRA)에서 행동의도와 행동 사이에는 상당히 강력한 상관관계가 존재한다. 특히, 행동이 의지적 통제 하에 있을 경우에 상관관계가 좀 더 높게 나타난다[Ajzen and Fishbein, 1980]. 하지만 행동의도와 행동 사이의 관계를 설명하는데 있어서 행동의도가 행동을 예측하는 것이 충분한지에 대한 논란이 있다. 즉, 행동의도를 매개하지 않고 행동에 영향을 주는 다른 요인이 있을 수 있다는 것이다. 이러한 추가적인 요인으로는 행동기대[Behavioral Expectation: Warshaw and Davis, 1985], 통제 위치와 가치[Saltzer, 1981] 등이 있다. 이 같이 행동의도와 행동 간에는 실제 괴리가 나타날 수 있는데 이러한 논리를 바탕으로 본 논문에서 행동을 측정하지 않은 이유는 크게 3가지이다. 첫째, 연구는 의지적으로만 행동하기는 통제요인이 많은 범죄적 행동에 대한 측정으로 조사대상자의 솔직한 행동측정이 어렵다고 판단하였다. 둘째, 합리적 행동이론(TRA)에서 행동에 유

일한 영향을 주는 행동의도 이외에도 추가적인 요인들이 있을 수 있기 때문에 전반적으로 다량의 측정에서 오는 측정오류나 조사 대상자의 측정거부 등을 고려하였다. 마지막으로 행동은 연구목적을 달성하는데 반드시 필요한 측정 요인이 아니기 때문에 행동에 대한 측정을 제외시켰다.

많은 기업들이 정보보호를 위해 정보보안체계를 구축하고 다양한 정보보안정책을 마련하여 내부직원들의 보안의식을 고취시키기 위한 정보보호활동을 수행하고 있다. 이러한 기업의 노력들은 직원들에게 지침이나 교육을 통해 전달하고 있으나 현실적으로는 직원 개개인의 보안의식 부족으로 인해 정보남용이나 정보유출로 나타나는 것이 오늘 날의 현실이다. 이러한 현실적 어려움에 본 논문이 도움이 되길 기대한다. 구체적으로, 본 논문은 기업 핵심기술정보, 국가기밀과 같은 보안에 상당한 정성과 비용을 들여 접근이 어려운 기밀정보가 아니라 다량의 개인정보를 다루는 조직의 내부구성원으로부터 접근이 용이한 고객정보나 데이터들 또는 그들 스스로 중요한 정보라고 인식하지 못할 수도 있는 정보들을 다루는 연구로서 정보를 어떻게 관리하고 통제해야 할지에 대한 방향을 제시하고 정보유출 시 개인의 재산과 프라이버시 침해를 방지하기 위한 금융회사의 정보보호활동의 효과를 높이는데 실용적인 도움이 될 수 있기를 기대한다. 그리고 본 논문은 인간을 심리적으로 고찰한 연구로서 정보보호 관리체계의 인원보안 관리수준에 향상과 내부 보안위협을 대응하는데 효과적으로 활용될 수 있기를 기대한다.

마지막으로, 금융회사의 정보보호체계에 대한 자세한 서술내용의 출처를 밝히지 않은 점에 양해를 바란다. 이와 같이 출처를 밝히지 않은 이유는 조사대상 기업에서 자료를 이용하고 표본조사를 허가한 것에 대한 요구조건으로서, 본 논문을 읽었을 때 조사대상 기업을 유추할 수 없도록 작성할 것을 요구 받았기 때문이다. 다소 출처 불분명한 부분에 대해서는 향 후 추가적인 연구를 통해 본 연구에서 부족했던 부분을 개선하여 제시할 것이며 이와 같은 연구를 해외 금융회사를 대상으로 비교 연구한다면 본 연구의 타당성을 높이는데 도움이 될 것으로 기대하고 있다.

〈References〉

[1] Ajzen, I., *From Intentions to Actions: A Theory of Planned Behavior,* Action Control: From Cognition to Bahavior, New York: Springer-Verlag, 1985, pp. 11-39.

[2] Ajzen, I., *The Theory of Planned Behavior*, Organizational Behavior and Human Decision Processes, Vol. 50, 1991, pp. 179-211.

[3] Ajzen, I. and Fishbein M., *Understanding Attitudes and Predicting Social Behavior,* NJ: Prentice-gall, 1980.

[4] Akers, R.L. and C.S. Sellers, *Criminological Theories*, OxfordUSA, 2005.

[5] Bhimani, A., "Securing the Commercial Internet," *Communications of the ACM*, Vol. 39-6, 1996, pp. 29-35.

[6] Blasi, A., *Bridging Moral Cognition and Moral Action; Critical Review of Literature,* Psychological Bulletin, Vol. 88, No. 1, 1980.

[7] Clinard, M.B., *Sociology of Deviant Behavior*, N.Y.: Holt Rinehart and Winston, 1963.

[8] Cohen, A.K., *The Study of Social Disorganization and Deviant Behavior*, Sociology Today: Problems and Prospects, N.Y.: Basic Books, 1959.

[9] Davis, F. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly*, 1989, pp. 319-340.

[10] Dhillon, G. and Backhouse, J., "Information System Security Management in the New Millennium," *Communications of the ACM*, Vol. 43, 2000, pp. 125-128.

[11] Docking, J., *Elton's Four Question: Some General Consideration*, School Management and Pupil Behavior, The Falmer Press, 1989.

[12] Doll and Ajzen, I., "Accessibility and Stability of Predictors in the Theory of Planned Behavior," *Journal of Personality and Social Psychology*, Vol. 63, 1992, pp. 754-765.

[13] Finne, T., "A conceptual framework for information security management," *Computers and Security*, Vol. 17, 1998, pp. 303-307.

[14] Fishbein, M. and Ajzen, I., *Belief, Attitude, Intention, and Behavior: An Interoduction to Theory and Research*, Reading, MA: Addison-Wesley, 1975.

[15] Heo, Seong-Wook, "Current state and Legal task of Personal information disclosure litigation," *Korean Legal Center*, 2009.

[16] Jung, Moon-Sung and Jung-Hwa Ku, "The Relationship between Youth's Moral Thinking and Moral Behaviors," *National Youth Policy Institute*, No. 6, 1991.

[17] Karyda, M., Kiountouzis, E., and KoKolakis, S., "Information System Security Policies: A Contextual Perspective," *Computers and Security*, Vol. 24, 2005, pp. 246-260.

[18] Kissinger, H., *American Foreign Policy,* New York: W.W. Norton and Co., 1974, p. 15.

[19] Kwon, Young-Kwan and Heung-Youl Youm, "Security Management Model for Protecting Personal Information for the Customer Contact Center," *Journal of the Korea Institute Security and Cryptology,* Vol. 19, No. 2, 2009.

[20] Lebow, R.N. and Stein, J.G., *Deterrence: The Elusive Dependent Variable*, Cambridge University Press, Vol. 42, No. 3, Apr. 1990.

[21] Lee, Cheolwon, Jongki Kim, Dongho Lee, and Choonshik Park, *The Study on Information Security Evaluation Methods, Korea Institute of Information security,* Vol. 11, No. 3, 2001.

[22] Lee, Gee-Hyun and Ui-Jin Seo, *Real condition of Collecting and Providing Personal Information Management and Investigation results of improvement remedy,* Korea Consumer Agency, 2011.

[23] Lee, Sang-Jun, *Information Security is Strategic investment reviving a company*, Boannews, Vol. 25, 2008.

[24] Merton, R.K., "Social Problems and Sociological Theory," *Contemporary Social Problems*, N.Y.: Harcout, Brace and World, 1961.

[25] Ministry of information and Communication, *National Information Security White Paper*, 2006.

[26] Moon, Yong-lin, *Theory of moral development,* Ahkanet, 2000.

[27] National Information Society Agency, *Overview of Information Security Management System*, 2008.

[28] Park, Tae-Wan, *Information System Security Inspection*, National Information Society Agency, 1997.

[29] Rauterberg, M., "How to Measure Cognitive Complexity in Human-Computer Interaction," *Austrian Society for Cybernetic Studies*, 1996.

[30] Rogers, E.M., *Diffusion of Innovations*, Free Press, New York, NY, 1983.

[31] Saltzer, E.B., "Cognitive Moderators of the Relationship between Behavioral Intentions and Behavior," *Journal of Personality and Social Psychology*, Vol. 41, 1981, pp. 260-71.

[32] Shaji, Sam, *ISO 27001,* Information Security Management Standard (ISMS), 2007.

[33] Shin, Dong-Joon, *The Effect of Punishment: A*

Critique of Deterrence Theory, Criminal Policy, Vol. 21, No. 2, 2009.

[34] Son, Chung-Ki and Young-Tae Kim, "A Study on Possibility Inquiry of Development of a New Defining Issues Test for Middle School Students in Korea," *Korea Society for Educational Evaluation*, Vol. 19, No. 2, 2006, pp. 41-65.

[35] Straub, D.W., "Effective IS Security: An Empirical Study," *Information Systems Research*, Vol. 1, 1990, pp. 255-276.

[36] Straub, D.W. and Welke, R.J., "Coping With Systems Risk: Security Planning Models for Management Decision Making," *MIS Quarterly*, Vol. 22, 1998, pp. 441-469.

[37] Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E., "The insider threat to information systems and the effectiveness of ISO17799," *Computers and Security*, Vol. 24, 2005, pp. 472-484.

[38] Taylor, S. and Todd, P., "Decomposition and crossover effects in the theory of planned behavior: a study of consumer adoption intentions," *International Journal of Research in Marketing*, Vol. 12, 1995, pp. 137-55.

[39] Triandis, H.C., *Values, attitudes, and interpersonal behavior*, Nebraska Symposium on Motivation, Belief, Attitudes, and Values, University of Nebraska Press, Lincoln, NE, 1979, pp. 195-259.

[40] Tittle, C.R., "*Sanctions and Social Deviance: The Question of Deterrence,*" NY: Praeger, 1980.

[41] Tyler, T.R., *Why People Obey the Law,* Princeton; Princeton University Press, 2006.

[42] Warshaw, P.R. and Davis, F.D., "Disentangling Behavioral Intention and Behavioral Expectation," *Journal of Experimental Social Psychology*, Vol. 21, 1985, pp. 213-228.

[43] Wiant, T.L., "Information security policy's impact on reporting security incidents," *Computers and Security*, Vol. 24, 2005, pp. 448-459.

[44] Williams, K.R. and Hawkins, R., *Perceptual Research on General Deterrence: A Critical Review*, Law and Society Review, Vol. 20, No. 4, 1986, pp. 545-572.

〈Appendix〉 설문 문항

* 억제활동에 관한 측정문항

회사의 정보보안지침이 업무 이외의 불필요한 고객정보접근 및 조회를 통제하는데 유용한가?
1. 회사의 정보보안지침은 불필요한 고객정보접근 및 조회를 통제하는데 효과가 있다.
2. 회사의 정보보안지침은 불필요한 고객정보접근 및 조회를 통제하는데 비교적 유용하다.
3. 회사의 정보보안지침은 불필요한 고객정보접근 및 조회를 개선하는데 도움을 준다.
4. 회사의 정보보안지침은 내가 생각했던 불필요한 고객정보접근 및 조회 행위를 통제방법을 포함하고 있다.
5. 회사의 정보보안지침은 불필요한 고객정보접근 및 조회를 통제하는데 있어서 내가 알고 있는 통제 방법보다 효과적이다.

회사의 정보보안교육이 업무 이외의 불필요한 고객정보접근 및 조회를 통제하는데 유용한가?
1. 회사의 정보보안교육은 불필요한 고객정보접근 및 조회를 통제하는데 효과가 있다.
2. 회사의 정보보안교육은 불필요한 고객정보접근 및 조회를 통제하는데 비교적 유용하다.
3. 회사의 정보보안교육은 불필요한 고객정보접근 및 조회를 개선하는데 도움을 준다.
4. 회사의 정보보안교육은 불필요한 고객정보접근 및 조회 행위를 통제하기 위한 유익한 내용을 포함하고 있다.
5. 회사의 정보보안교육은 불필요한 고객정보접근 및 조회를 통제하는 방법을 배우는데 있어 적합한 방식이라고 생각한다.

* 예방활동에 관한 측정문항

본인의 업무PC에서 업무 이외의 불필요한 고객정보접근 및 조회가 얼마나 복잡한가?
1. 내 PC에서 불필요한 고객정보접근 및 조회방법을 배우는 것은 어렵다.
2. 내 PC에서 불필요한 고객정보접근 및 조회를 하는 것은 기술적으로 복잡하다.
3. 내 PC에서 불필요한 고객정보접근 및 조회를 능숙하게 하는 것은 어렵다.
4. 내 PC에서 불필요한 고객정보접근 및 조회를 하기 위해서는 업무절차가 복잡하다.
5. 내 PC에서 불필요한 고객정보접근 및 조회가 어렵다는 것은 나는 잘 알고 있다.

본인의 업무PC 이외의 시스템(동료PC, 전산실 등)에서 업무 이외의 불필요한 고객정보접근 및 조회가 얼마나 복잡한가?
1. 내 PC 이외의 시스템에서 불필요한 고객정보접근 및 조회 방법을 배우는 것은 어렵다.
2. 내 PC 이외의 시스템에서 불필요한 고객정보접근 및 조회를 하는 것은 기술적으로 복잡하다.
3. 내 PC 이외의 시스템에서 고객정보에 접근하는 자체가 물리적으로 어렵다.
4. 내 PC 이외의 시스템에서 고객정보에 접근하기 위한 업무절차가 까다롭다.
5. 내 PC 이외의 시스템에서 고객정보에 접근하는 것이 어렵다는 것은 나는 잘 알고 있다.

* 탐지활동에 관한 측정문항

본인이 인지하고 있는 상사나 감시자 등 사람에 의한 보안감시 수준은?
1. 회사 내 CCTV를 통해 나의 행동이 보안직원들로부터 실시간 감시되고 있다는 것을 알고 있다.
2. 직속상사가 자주 내 업무자리를 보안점검하고 있다는 것을 알고 있다.
3. 직속상사가 자주 내 업무기록 및 히스토리를 점검하고 있다는 것을 알고 있다.
4. 감시부서에서 주기적으로 내 업무자리를 보안점검하고 있다는 것을 알고 있다.
5. 감시부서에서 주기적으로 내 업무기록 및 히스토리를 점검하고 있다는 것을 알고 있다.

본인이 인지하고 있는 보안시스템에 의한 보안감시 수준은?
1. 회사 내 CCTV를 통해 나의 대부분의 행동이 보안시스템에 의해 녹화, 저장되고 있다는 것을 알고 있다.
2. 내 ID로 로그인된 시스템에서 발생되는 모든 업무는 중앙시스템에 기록, 저장되고 있다는 것을 알고 있다.
3. 내 ID로 로그인된 시스템에서 발생되는 모든 업무는 보안시스템에 의해 감시하고 있다는 것을 알고 있다.
4. 내 업무PC에는 고객정보 수집을 감시하는 보안프로그램이 설치되어 있다는 것을 알고 있다.
5. 내 업무PC에서 일어나는 모든 행위가 보안시스템에 의해 원격으로 감시되고 있다는 것을 알고 있다.

* 교정활동에 관한 측정문항

업무 이외의 불필요한 고객정보접근 및 조회 시 받게 되는 처벌의 엄격성은?
1. 내가 만약 불필요한 고객정보접근 및 조회로 인해 처벌을 받는다면 아마도 높은 수준의 처벌을 받게 될 것이다.
2. 내가 만약 불필요한 고객정보접근 및 조회로 인해 처벌을 받는다면 엄격하게 받게 될 것이다.
3. 내가 만약 불필요한 고객정보접근 및 조회로 인해 처벌을 받는다면 퇴사도 각오해야 할 것이다.

업무 이외의 불필요한 고객정보접근 및 조회 시 받게 되는 처벌의 확실성은?
1. 내가 만약 불필요한 고객정보접근 및 조회를 한다면 처벌을 피할 수 없을 것이다.
2. 내가 만약 불필요한 고객정보접근 및 조회를 한다면 아마도 처벌을 받게 될 것이다.
3. 내가 만약 불필요한 고객정보접근 및 조회를 한다면 처벌을 받을 가능성이 상당히 높다.

◆ About the Authors ◆

Woo-Jin Jung

Woo-Jin Jung received his MS degree in MIS from Hanyang University, Seoul, Korea. His research interests are in the area of information security management.

Yuhyung Shin

Yuhyung Shin received her Ph.D. in organizational psychology from Columbia University in 2005. She is an assistant professor of organizational behavior at the School of Business, Hanyang University, Seoul, Korea. Her current research interests include social and emotional aspects of virtual teams, team processes, person-organization fit, and organizational citizenship behavior.

Sang-Yong Tom Lee

Sang-Yong Tom Lee is a Professor in School of Business, Hanyang University, Seoul, Korea. He was on the faculty of Department of Information Systems, National University of Singapore before joining Hanyang University. He received his PhD degree from Texas A&M University (1999). His research interests include economics of information systems, online information privacy, and value of IT. His papers have been published in Management Science, MIS Quarterly, Journal of Management Information Systems, Communications of the ACM, IEEE Transactions on Engineering Management, Information & Management, and others.

Submitted : December 7, 2011 Accepted : March 16, 2012
1st revision : March 11, 2012