「정보시스템연구」 제22권 제4호
한국정보시스템학회
2013년 12월, pp. 49~69

http://dx.doi.org/10.5859/KAIS.2013.22.4.49

고객정보 식별자 표시제한으로 인한 업무영향에 관한 연구
- 국내 증권 업무를 중심으로 -

신상철* · 이영재**

〈목 차〉

Ⅰ. 서 론

정보 사회는 정보기술(IT: information technology)을 기반으로 지속적으로 발달하였고, 이제는 IT가 사회 모든 분야에서 기본 인프라로 자리 잡았다. 정보기술은 경쟁력 확보와 비용 효율화를 위한 주요 추진 전략중의 하나이며, 기업의 IT 의존도는 증대되고 있다(이장형 외, 2010). 그러나 해킹, 바이러스, 사이버 테러, 개인정보 유출 등 정보화의 이면에 존재하는 역기능도 지속적으로 증가하고 있다.(박경아 외, 2012). 기업에서도 역기능에 대응하기 위하여 보안통제를 강화하고 있으며, 내부자에 의한 정보유출 예방 체계를 강화하고 있다.

국정 통계 지표를 발표하는『e-나라지표』를 보면 개인정보 침해로 인한 신고 상담이 지속적으로 증가함을 알 수 있다. 2012년도 개인정보 침해신고 상담건수는 총 166,801건으로 전년대

* 동국대학교 경영정보학과 박사과정, 제1저자, infsecpro@naver.com
** 동국대학교 경영정보학과 교수, 교신저자, yjlee@dgu.edu

비 약 26.7% 증가하였다. 개인정보 침해 유형은 주민등록번호 등 타인 정보 도용이 가장 많으며, 해킹 및 내부자에 의한 정보유출 보안사고도 지속 발생하고 있다.

국내 금융 분야에서도 개인정보보호를 위하여 『전자금융감독규정』(금융위원회), 『개인정보 안정성 확보 조치 기준』(안전행정부) 등에 근거하여 다양한 기술적 보호 조치를 적용하고 있으나, 인가된 내부 직원의 정보유출 보안 사고는 지속적으로 발생하고 있다. 최근 국내 금융 분야의 개인정보 유출 보안사고 사례를 보면 2013년 5월에 메리츠화재에서 내부자에 의한 16만여 건, 비슷한 시기에 한화손해보험에서는 해킹 보안사고로 12만여 건의 개인정보가 유출되었다.

기업에서는 외부자의 해킹으로 인한 침입 대응도 중요하지만, 내부자의 정보유출로 인한 보안 위협도 증대되고 있어 내부 네트워크 및 사용자 영역에서의 보안관리도 점점 중요해지고 있다(황기영 외, 2008). 따라서 내부 직원이 고객정보를 검색하고 획득할 수 있는 업무 정보시스템으로의 접근통제와 정보 노출 최소화가 필요하다.

그러나 기업의 보안통제 강화는 내부 사용자가 업무 정보시스템을 사용할 때 업무 수행이 어려워지게 되는 결과를 초래하게 된다(장덕성, 2003). 즉 보안통제가 강할수록 보안 수준은 높아질 수 있으나, 사용자는 업무 정보시스템 활용에 지장을 받게 된다. 따라서 보안통제와 업무효율이라는 이중적 구조에서 업무영향을 최소화하면서 적절한 보안통제 정책을 수립할 수 있는 다양한 분야의 연구가 필요하다. 정보보안의 기본 기능인 기밀성을 위하여 개인정보 표시제한 시에도 표시제한으로 인한 개인정보 사용이 업무에 미치는 영향을 고려하여 보안통제 정책을 수립하여야 한다.

반면 기존 개인정보보호 관련 연구는 개인정보보호 관리체계 수립, 기술 개발, 법·제도 개선, 지침 수립, 개인정보 영향평가, 개인정보보호 지표(수준 측정) 수립 등을 위주로 진행되었고, 보안통제가 업무 수행에 미치는 영향에 관한 국내 연구는 미흡한 실정이다.

본 연구는 고객정보 사용과 고객정보 식별자 표시제한으로 인한 업무지장과의 관련성을 분석하고, 관련성이 있을 경우 업무지장 정도를 측정하여 업무 영향을 실증 분석한다. 실증 분석 결과를 토대로 기업이 효과적인 표시제한 보안통제 정책을 수립할 수 있도록 보안통제와 업무영향간의 관계와 결과를 제시한다.

이를 통하여 학문적으로는 보안통제와 이분변수인 업무지장 영향과의 인과 관계 및 영향도를 통계적으로 분석할 수 있는 기법을 개발하고, 실무적으로는 기업이 보안통제를 적용할 때 업무영향을 고려한 효과적인 보안정책 수립에 기여하고자 한다.

연구 대상은 국내 금융업종 중 증권 업무를 중심으로 입출금, 주문, 상품 등 계정처리 업무 정보시스템을 사용하는 내부 직원으로 하였다. 연구 절차는 선행 연구(이론적 배경), 연구 설계, 실증 분석, 결론 순으로 진행하였다.

Ⅱ. 이론적 배경

2.1 개인정보의 정의 및 오·남용

개인정보 개념에 대한 정의는 개인정보보호

법을 대표적으로 들 수 있다 (노영희, 2012). 『개인정보보호법』 제2조에 '개인정보란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보를 말한다'로 정의하고 있다. OECD 가이드라인(1980)에서는 '개인정보를 식별할 수 있는 개인(데이터의 주체)에 관한 정보'라고 정의하고 있다.

개인정보 도용이란, 정보주체의 동의 없이 부정한 목적으로 타인에 의해 개인정보가 불법적으로 이용됨으로써 정보 주체의 인격적 침해 및 경제적 손실을 야기하는 경우를 의미한다(장은경 외, 2006). 정보통신망의 확대로 인하여 개인정보의 부정 유출, 오·남용, 수집 등의 문제가 증가하였으며, 국내·외 많은 나라에서 개인정보가 유출되고 오·남용 되는 것을 근절하기 위하여 『개인정보보호법』을 제정하였다(유한나 외, 2012).

개인정보는 중앙 집중방식으로 대량으로 수집·관리되어 데이터베이스화 되면 고의 또는 과실에 의해 언제라도 개인정보가 침해·누설될 수 있는 위험성이 존재하며(김희수 외, 2006), 정당한 사용자로 인증을 받았다고 할지라도 업무처리에 있어서 필요한 최소한의 권한만을 부여하는 것이 필요하다(정성민, 2008). 또한 금융회사는 고객 신용정보 조회 권한을 직급별·업무별로 차등 부여하여 내부통제를 강화하고, 내부직원의 고객 신용정보 오·남용을 방지하고 있다(개인 신용정보 관리·보호 모범규준, 2005).

이처럼 개인정보의 오·남용이 증가됨에 따라 국가에서는 개인정보보호법을 제정하였고, 금융 분야에서도 보호 기준을 수립하는 등 다양한 예방 활동이 필요함을 알 수 있다.

2.2 고객정보 사용 및 식별자

기업은 고객정보 식별자를 활용하여 데이터를 추출하여 분석하고, 이를 마케팅이나 고객관리, 고객 서비스를 위하여 사용한다.

즉 데이터베이스 등 정보기술을 이용하여 방대한 고객정보를 축적하고, 이를 통하여 고객에게 맞춤화된 서비스 및 상품을 제공한다(Pepard, J., 2009).

정보시스템 사용 형태에 대하여 김영희 등(2004)은 사용자가 할 수 있는 행위를 검색, 조회, 변경, 등록, 다운로드, 출력으로 파악하였고 이석형 등(2009)은 디지털 자료 활용 형태를 열람, 다운로드, 전송으로 분류하였다.

방대한 정보가 축적된 데이터베이스에서 특정 고객정보를 찾아내기 위하여 고객정보 식별자가 활용된다. 식별자란 정보의 효율적인 유통과 활용을 위해 유일한 코드를 부여하여 이를 관리해주는 체계로서(강상욱 외, 2007) 변하지 않고 지속적으로 유지되어야 하며, 관리 범위내에서 유일한 값이어야 한다(Priscilla, C. 외, 1999).

이민영(2004)은 국내에서 주민등록번호는 공공기관뿐만 아니라 민간분야에서도 광범위하게 사용되고 있으며 표준 통일 개인 식별번호로서 기능을 담당한다고 하였다. 이동훈(2004)은 주민등록번호는 정보사회가 진척되는 과정에서 데이터베이스내의 개인정보를 확인하기 위한 수단은 물론 여러 데이터베이스에 분산되어 있는 개인정보의 연동을 위해 이용되고 있다고 하였다.

2.3 보안통제

2.3.1 기밀성 및 접근통제

정보보안은 기밀성, 무결성, 가용성을 유지 보호하기 위한 제반 활동이며(이경근 외, 2010) 기밀성은 정보의 비밀이 유지되는 것을 의미한다(홍영란 외, 2012).

기밀성을 위하여 금융 어플리케이션은 개인정보 제공 시에는 최소 권한의 원칙을 만족해야 한다. 필요한 권한 보다 필요 이상의 권한을 허용하게 되면 최소 권한의 원칙을 위배하게 된다(나석현 외, 2006).

개인정보 노출 위협(privacy concern)은 향상된 정보 기술로 인해 정보 시스템의 개인정보 저장, 감시, 검색, 커뮤니케이션 등에 대해 이용자가 느끼는 위협이다(Culnan, M.J. 외, 2003).

개인정보 노출 최소화 및 내부 사용자의 보안 위협에 대응하기 위하여 접근통제가 필요하다. 접근통제는 컴퓨터나 통신시스템에서 비인가된 사용, 누설, 변경, 파괴 등 보안 위협을 막는 것이다(ISO /IEC, 1996). 접근통제는 행위자, 행위대상 및 행위내용에 대한 통제 프레임워크에 기반하며(Sandhu, R.S. 외, 1994), 고객 개인정보가 저장된 데이터베이스에서는 접속자 통제, 접속 범위 통제, 및 접속 후 행동 통제의 세 가지 통제 방안이 필요하다(Laudon,K. 외, 2012). 접속 후 행동 통제는 해당 이용자가 프로그램 등 수단과 데이터를 활용하여 할 수 있는 행동을 통제하는 것을 의미한다(이은곤, 2013).

즉 내부 업무 정보시스템의 접근통제는 내부 사용자의 업무 정보시스템 접속권리에 대한 통제, 접속하여 활용하는 데이터 범위에 대한 통제 그리고 조회, 다운로드, 인쇄 등 업무 정보시스템 내에서의 내부 사용자 행동에 대한 통제가 필요하다.

2.3.2 표시제한

기업은 정보유출과 정보 남용을 예방하기 위하여 불필요한 정보 조회를 제한함으로써 고객의 프라이버시 침해를 최소화할 수 있다(정우진 외, 2012).

해외에서도 개인정보 보안통제를 위하여 다양한 노력을 경주하고 있다. 2007년 19차 개정된 “The Social Security Finance Act”에서는 개인 의료 정보의 표시제한과 접근채널의 일원화 등 두 가지 기본 원칙을 제시하고 있다(Allaert. F.A. 외, 2009).

국내 법규 관련 기준들을 보면 “개인정보의 기술적·관리적 보호조치 기준”에서는 개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 개인정보를 표시제한할 것을 권고하고 있다(방송통신위원회 고시 제2012-50호, 2012). 국내 금융권 경우 “금융 감독 검사 매뉴얼”에는 전자금융 거래 시 비밀번호, 주민등록번호 등 주요 고객정보가 화면에 노출되는지에 대한 검사 항목을 반영하고 있다(금융감독원 IT검사매뉴얼, 2013).

2.4 보안통제와 업무영향

금융 회사는 업무 수행을 위하여 고객의 개인정보를 사용할 수 밖에 없으며 이는 기업 활동의 업무 효율성과 관계된다(박종찬, 2006). 반면 금융 회사는 정보화 역기능인 개인정보 침해 및 도용, 내부 사용자의 오·남용을 예방하기 위하여 내부 업무 정보시스템에 보안통제를 적용할 수

밖에 없다. 그러나 보안의 중요성 때문에 기업 구성원이 시스템을 사용함에 어려움이 있다면 정보 생성 등 업무 수행이 어려워지게 된다. 따라서 사용자 편의성을 고려한 보안시스템이 디자인 되어야 한다(장덕성, 2003).

정보보안 정책의 준수가 업무 생산성과 일부 상충관계에 있기 때문에 보안정책을 준수하도록 하는데 어려움이 있으며, 업무를 수행함에 불편함이 존재할 경우, 기업이 조직원들에게 보안정책을 준수하도록 하는데 장애가 될 수 있다(Chan,M. 외, 2005). 조직원은 보안정책을 준수하는데 불편함이 있으면 정보보안 정책을 제대로 준수하지 않게 되므로(Herath,T. 외, 2009), 보안정책은 실제로 이를 준수하는 사용자의 관점에서 접근하는 것이 중요하다(박철주 외, 2012).

보안기술이 효과를 발휘하기 위해서는 조직에서 사용하는 다른 정보기술과 충돌 없이 조화롭게 운영될 수 있도록 유연해야 하며, 조직의 고유한 상황에 적합해야 한다(Werlinger, R. 외, 2009). 정보보안 체계를 준수하는 것은 업무를 수행하는 개인에게 시간지체, 업무과중 등 비용을 발생시킨다. 이를 해결하기 위해서는 보안시스템을 사용자 중심적 관점에서 개발할 필요가 있다(정태석 외, 2012).

따라서 증권 기업의 내부 업무 정보시스템에 대한 표시제한도 보안통제 효과와 더불어 고객정보 사용자들의 불편함을 최소화하고, 업무 수행에 장애가 되지 않도록 업무 생산성을 고려한 효율적 표시제한 보안정책이 수립되어야 할 것이다.

이상 살펴본 선행 연구들을 정리하면 다음 <표 1>과 같다.

<표 1> 선행 연구 정리

구분	항목	주요내용	출처
개인정보의 정의 및 오·남용	개인정보 정의	살아 있는 개인에 관한 정보로써 성명, 주민등록번호, 영상 등을 통하여 개인을 알아볼 수 있는 정보	개인정보보호법
	개인정보 오·남용	정보통신망의 확대로 인하여 개인정보의 부정 유출, 오·남용, 수집 등의 문제 증가	유한나 외, 2012
고객정보 사용 및 식별자	고객정보 사용	정보시스템에서 사용자가 할 수 있는 행위를 검색, 조회, 변경, 등록, 다운로드, 출력으로 파악	김영희 외, 2004
		디지털 자료 활용 형태를 열람, 다운로드, 전송으로 분류	이석형 외, 2009
		금융 회사는 업무 수행을 위하여 고객의 개인정보를 사용할 수 밖에 없으며 이는 업무 효율성과 관계됨	박종찬, 2006
	식별자	정보의 효율적인 유통과 활용을 위해 유일한 코드를 부여하여 이를 관리해주는 체계	강상욱 외, 2007
		식별자는 변하지 않고 지속적으로 유지되어야 하며, 관리 범위 내에서 유일한 값이어야 한다	Priscilla,C. 외, 1999
		주민등록번호는 개인 식별번호로서 기능을 담당	이민영, 2004

구분	항목	주요내용	출처
보안통제	기밀성	정보의 비밀이 유지되는 것	홍영란 외, 2012
	접근통제	컴퓨터나 통신시스템에서 비 인가된 사용, 누설, 변경, 파괴 등 보안 위협을 막는 것	ISO/IEC, 1996
	표시제한	불필요한 정보 조회를 제한함으로써 고객의 프라이버시 침해를 최소화할 수 있다	정우진 외, 2012
		개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 표시제한을 권고	방통위 고시 제2012-50호, 2012
보안통제와 업무영향		보안의 중요성 때문에 기업 구성원이 시스템을 사용함에 어려움이 있다면 정보 생성 등 업무 수행이 어려워지게 됨	장덕성, 2003
		정보보안 정책의 준수는 업무 생산성과 일부 상충 관계에 있음	Chan,M. 외, 2005
		정보보안 체계를 준수하는 것은 업무를 수행하는 개인에게 시간지체, 업무과중 등 비용을 발생	정태석 외, 2012

Ⅲ. 연구 설계

3.1 연구 설계

기업은 효율적 업무처리 및 고객관리를 위하여 내부 업무 정보시스템을 구축하였고, 금융 업무 환경에서 고객정보 사용은 업무에 필수적 요소이다.

선행 연구를 통하여 개인정보의 도용 및 오·남용이 증가함을 알 수 있었고, 기업은 개인정보의 도용 및 오·남용을 예방하고, 고객정보의 비밀을 유지하고자 접근통제, 중요정보 표시제한 등 보안통제를 적용하고 있다.

그러나 보안통제는 내부 업무 정보시스템 사용자들에게 시간 지체, 업무 과중 등 업무 수행에 지장을 줄 수 있다. 따라서 내부 업무 정보시스템은 사용자 관점을 고려한 보안정책이 필요하다.

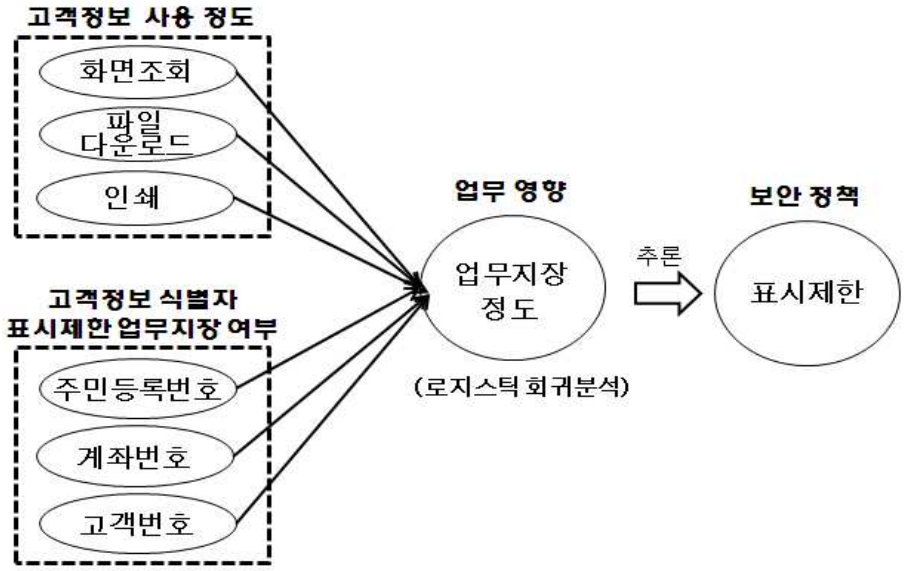
본 연구는 이러한 배경 하에서 증권 회사의 내부 업무 정보시스템에서 고객정보 사용 정도와 고객정보 식별자 표시제한으로 인한 업무지장 설문 데이터를 기반으로 업무지장 영향을 파악한다.

이를 통하여 효율적 업무처리를 위한 고객정보 식별자 표시제한 보안정책을 추론하는 연구를 설계하였다. 선행 연구와 전문가 설문을 통하여 고객정보 사용 유형은 화면 조회, 파일 다운로드, 인쇄 형태로 정의하였고, 고객정보 식별자는 주민등록번호, 계좌번호, 고객번호로 하였다. 기술적 연구(descriptive study)를 도식화하면 다음 <그림 1>과 같다.

3.2 변수 정의

3.2.1 고객정보 사용

금융 회사의 내부 업무 정보시스템 사용자들



<그림 1> 연구 설계

은 고객정보 식별자를 활용하여 고객정보를 조회 검색하고, 파일로 다운로드하며, 인쇄·출력하는 등 고객정보를 사용하고 있다.

김영희 등(2004)은 정보시스템에서 사용자의 행위를 검색, 조회, 변경, 다운로드, 출력으로 파악하였고, 이석형 등(2009)은 디지털 자료 활용 형태를 열람, 다운로드, 전송으로 분류하였다.

본 연구에서는 업무 정보시스템에서의 고객

<표 2> 증권 업무 전문가의 고객정보 사용

설문자	근무지	업무 경력	증권 업무 정보시스템의 고객정보 사용 유형			
			화면 조회	파일 다운로드	인쇄	기타
전문가 1	본사	19	사용	사용	사용	화면캡처
전문가 2	본사	20	사용	사용	사용	종이형태 고객정보
전문가 3	본사	10	사용	사용	사용	주민등록증 스캔정보
전문가 4	본사	19	사용	사용	사용	없음
전문가 5	본사	20	사용	사용	사용	화면캡처
전문가 6	지점	20	사용	사용	사용	없음
전문가 7	지점	11	사용	사용	사용	없음
전문가 8	지점	13	사용	사용	사용	없음
전문가 9	지점	12	사용	사용	미 사용	없음
전문가 10	지점	10	사용	사용	미 사용	없음
전문가 11	고객센터	10	사용	사용	사용	없음
전문가 12	고객센터	10	사용	사용	사용	없음

정보 사용을 보다 명확하게 정의하기 위하여 증권 업무 10년 이상 경험이 있고, 증권 계정처리 업무 정보시스템을 사용하는 본사, 지점, 고객센터에 근무하는 증권 업무 전문가를 대상으로 설문을 실시하였다. 설문 결과는 <표 2>와 같다.

<표 2>와 같이 증권 업무 정보시스템에서의 고객정보 사용은 '화면 조회', '파일 다운로드', '인쇄' 사용으로 조사되었다. 소수 의견으로 '화면 캡처', '종이형태 고객정보 사용', '주민등록증 스캔정보' 등이 있었으나, '화면 캡처'와 '주민등록증 스캔정보'는 '화면 조회' 사용과 유사하고, '종이형태 고객정보 사용'은 '인쇄' 사용과 유사하며 각각 소수 의견임에 따라 고객정보 사용 변수 정의에서 제외하였다.

고객정보 사용에 대한 선행 연구와 증권 업무 전문가의 설문 결과를 통하여 고객정보 사용 변수는 다음 <표 3>과 같이 정의하였다.

<표 3> 고객정보 사용의 조작적 정의

변수	조작적 정의	출처
화면 조회	업무 정보시스템 사용자가 고객정보를 화면에서 조회하는 사용	- 김영희 등(2004) : 정보시스템 사용자가 할 수 있는 행위를 검색, 조회, 변경, 등록, 다운로드, 출력으로 파악 - 이석형 등(2009) : 디지털 자료 활용 형태를 열람, 다운로드, 전송으로 분류 - 증권 업무 전문가 설문 결과
파일 다운로드	업무 정보시스템 사용자가 고객정보를 엑셀 등의 파일로 다운로드하는 사용	- 김영희 등(2004) : 정보시스템 사용자가 할 수 있는 행위를 검색, 조회, 변경, 등록, 다운로드, 출력으로 파악 - 이석형 등(2009) : 디지털 자료 활용 형태를 열람, 다운로드, 전송으로 분류 - 증권 업무 전문가 설문 결과
인쇄	업무 정보시스템 사용자가 고객정보를 종이 등으로 인쇄(출력)하는 사용	- 김영희 등(2004) : 정보시스템 사용자가 할 수 있는 행위를 검색, 조회, 변경, 등록, 다운로드, 출력으로 파악 - 증권 업무 전문가 설문 결과

3.2.2 고객정보 식별자 표시제한

식별자는 정보시스템에서 특정 정보를 구별하는 유일한 값으로서 변하지 않고, 지속되는 특성을 지니고 있다.

주민등록번호는 방대하게 고객정보가 저장되어 있는 데이터베이스에서 식별자는 개인을 식별하고 검색하는데 사용되며(이민영, 2004), 여러 데이터베이스에 분산되어 있는 개인정보의 연동을 위해서도 사용된다(이동훈, 2004).

또한 금융 증권 기업에서는 주민등록번호외에도 고객의 증권 계좌를 개설하면서 계좌번호를 생성하고, 고객 개인별로 고객번호를 부여하여 고객정보 식별자로 사용하고 있다.

본 연구에서는 증권 업무 정보시스템에서의 고객정보 식별자를 보다 명확히 정의하기 위하여 9년 이상의 경력을 보유한 증권 데이터베이스 전문가를 대상으로 설문을 실시하였으며, 결과는 아래 <표 4>와 같다.

<표 4> 증권 데이터베이스 전문가의 고객정보 식별자

설문자	담당업무	업무 경력	증권업무 정보시스템 고객정보 식별자 유형			
			주민등록번호	계좌번호	고객번호	기타
전문가 1	DB 관리운영	16	사용	사용	사용	없음
전문가 2	DB 관리운영	14	사용	사용	사용	성명(인덱스)
전문가 3	DB 관리운영	20	사용	사용	사용	카드번호(인덱스)
전문가 4	DB설계 컨설팅	15	사용	미사용	사용	없음
전문가 5	DB설계 컨설팅	14	사용	사용	사용	외국인 실명번호
전문가 6	DB설계 컨설팅	9	사용	사용	사용	없음

<표 4>와 같이 증권 업무 정보시스템의 고객정보 식별자는 '주민등록번호', '계좌번호', '고객번호' 로 조사되었다. 소수 의견으로 '성명', '카드번호' '외국인 실명번호'가 있었으나, '성명'과 '카드번호'는 식별자가 아닌 인덱스 형태로 제외하였고, '외국인 실명번호'는 증권 업무 정보시스템에서 범용적으로 사용되는 식별자가 아니므로 제외하였다.

표시제한은 '어떤 내용을 나타내는 것을 제한하는 것'으로 정보 노출을 방지하기 위하여 특정 정보 값을 드러내지 않도록 하는 것을 의미한다. 고객의 프라이버시 보호를 위하여 불필요한 정보 노출을 최소화하여 내부 정보유출 및 정보남용을 예방할 수 있다. 정보유출 관점에서도 개인정보 표시제한 처리 미흡으로 인한 정보유출 보안 위협이 대두되고 있으며, "개인정보의 기술적·관리적 보호조치 기준", "금융 감독 검사 매뉴얼" 등 국내 법규 기준들도 표시제한 보안통제를 강화하고 있다.

기업은 개인정보 침해 및 오·남용을 예방하기 위하여 내부 업무 정보시스템에 보안통제를 적용한다. 그러나 선행 연구에서 살펴보았듯이 보안통제로 인하여 정보시스템 사용자는 업무 수행이 어려워지게 되고, 정보 생성 등 업무지장을 받을 수 있다.

업무영향은 증권 업무 정보시스템 사용자가 고객정보를 사용함에 있어 고객정보 식별자 표시제한으로 인하여 시간 지체, 업무 과중 등 업무 생산성에 영향을 받는 업무지장의 정도로써, 로지스틱 회귀분석을 통하여 산출되는 오즈비(odds ratio)로 하였다.

선행 연구와 증권 데이터베이스 전문가의 설문 결과를 통하여 도출한 고객정보 식별자, 표시제한, 업무지장 변수에 대한 조작적 정의는 다음 <표 5>와 같다.

<표 5> 고객정보 식별자 표시제한 조작적 정의

변수		조작적 정의	출처
고객정보 식별자	주민등록번호	고객 개인이 보유하고 있는 주민등록번호	- 강상욱 등(2007) : 식별자란 정보의 효율적인 유통과 활용을 위해 유일한 코드를 부여하여 이를 관리해주는 체계임 - Priscilla, C. 등(1999) : 식별자는 변하지 않고 지속적으로 유지되어야 하며, 관리 범위 내에서 유일한 값이어야 함

			- 이민영(2004) : 주민등록번호는 데이터베이스에서 개인을 식별하고 검색하는데 사용 - 증권 데이터베이스 전문가 설문 결과
	계좌 번호	증권 고객이 계좌를 개설하고 발급받는 계좌 고유번호	- 강상욱 등(2007) : 식별자란 정보의 효율적인 유통과 활용을 위해 유일한 코드를 부여하여 이를 관리해주는 체계임 - Priscilla, C. 등(1999) : 식별자는 변하지 않고 지속적으로 유지되어야 하며, 관리 범위 내에서 유일한 값이어야 함 - 증권 데이터베이스 전문가 설문 결과
	고객 번호	증권 고객이 발급받는 고객 고유번호	- 강상욱 등(2007) : 식별자란 정보의 효율적인 유통과 활용을 위해 유일한 코드를 부여하여 이를 관리해주는 체계임 - Priscilla,C 등(1999) : 식별자는 변하지 않고 지속적으로 유지되어야 하며, 관리 범위내에서 유일한 값이어야 함 - 증권 데이터베이스 전문가 설문 결과
표시제한		업무 정보시스템에서 어떤 내용을 나타내는 것을 제한 하는 것	- 이기혁(2008) : 개인정보 표시제한 처리 미흡을 보안위협으로 정의 - 개인정보의 기술적·관리적 보호조치 기준(방송통신위원회,2012) : 개인정보를 조회, 출력 등 업무처리를 할 경우 표시제한 권고 - 금융 감독 검사 매뉴얼(금융감독원, 2013) : 전자금융거래시 비밀번호, 주민등록번호 등 주요 고객정보가 화면에 노출되는지에 대한 검사
업무지장		업무 정보시스템 사용자에게 시간 지체, 업무 과중 등 업무 생산성에 영향을 주는 장애	- Chan, M., Woon, I., Kankanhalli, A(2005) : 정보보안 정책의 준수가 업무 생산성과 일부 상충관계에 있음 - 장덕성(2003) : 보안통제로 인하여 사용자 업무수행이 어려워질 수 있음. - 정태석 등(2012) : 회사의 정보보안 체계를 준수하는 것은 업무를 수행하는 사용자에게 시간지체, 업무과중 등 비용을 발생시킴

3.3 표본구성 및 검증

3.3.1 표본구성

본 연구를 위한 연구 모집단은 국내 자산 규모가 상위 5위 이내인 증권 기업 중의 하나를 선정하였다.

표본 구성은 본 연구가 회사 차원의 표시제한 보안정책을 추론하는 것임에 따라 본사, 지점, 고객센터로 구분하고 본사와 지점 인구비를 고려하여 설문 대상을 무작위화하였다.

설문 결과가 특정 부서 또는 특정 업무자의 의견으로 치우치지 않도록 본사에서는 부서별로 구분하여 불특정 1인을 설문대상으로 선정하였으며, 지점은 전국 지역 분포를 고려하여 총 30개 지점을 선정하였다. 고객센터는 근무 인력 중 50명을 무작위로 선정하였다.

3.3.2 검증

본 연구의 설문 결과는 '로지스틱 회귀분석'으로 실증 분석한다. 로지스틱 회귀분석은 종속변수가 이 분형 값(명목척도)일 때 개개 관측치들이(설명변수) 어느 연구 관심결과의 집단으로 포함되는지를 분류할 수 있게 해주는 통계 기법이다.

로지스틱 회귀분석은 어떤 설명변수(독립변수)가 연구 관심결과(종속변수)와 관련성이 있는지(영향을 미치는지)를 파악할 수 있게 해주고, 관련성이 있는 경우, 영향도인 odds ratio(measure of effect size)를 산출하여 특정 설명변수가 연구 관심결과로 나타나게 될 확률을 계산할 수 있게 해준다(김윤용, 2011). 즉 연구 관심결과(종속변수)가 이분형 값인 명목 척도일 때 로지스틱 분석을 통하여 개개변수의 영향력의 정도를 파악할 수 있다(박용성, 2008).

본 연구는 등간 척도인 고객정보 사용과(설명변수) 이분형 값인 업무지장(종속 변수)간의 관련성 여부와 관련성이 있을 경우, 영향도(odds ratio)를 산출하기 위하여 로지스틱 회귀분석을 검증 방법으로 사용하였다.

Ⅳ. 실증 분석

4.1 자료 수집 및 분석 방법

4.1.1 자료 수집

선정된 연구 모집단을 대상으로 고객정보 사용 정도, 고객정보 식별자 표시제한으로 인한 업무지장, 설문자 기초 정보에 대한 설문을 실시하였다.

고객정보 사용 정도는 '고객정보 화면 조회 정도', '고객정보 파일 다운로드 정도', '고객정보 인쇄 정도'로 구성하고, 표시제한으로 인한 업무지장은 업무지장 여부에 대하여 '있다'와 '없다'로 구성하였다. 설문자 기초 정보로는 소속(부서명), 성명, 직급, 전화번호, 담당업무, 근무연수로 구성하였다.

설문 척도는 다음 <표 6>과 같이 고객정보 사용 정도는 등간척도로, 업무지장 여부는 명목척도로 구성하였다.

배포된 설문서 중 중복 답변, 결측 값(무 응답) 내포 설문을 배제하고 지점 및 본사 인구비 (6:4)를 고려하여 총 90개의 설문을 통계 검증 대상으로 사용하였다. 통계 검증 설문대상 중 10년

<표 6> 설문 척도

항목	설문 척도	데이터 전처리
고객정보 사용 정도	1) 없다, 2) 매일 3) 1주일에 2-3회 4) 1주일에 한번 5) 월간, 6) 분기 7) 반기, 8) 연간	- 리커드 7점 척도 사용 (매우낮음 - 낮음-약간낮음-중간 - 약간높음-높음-매우높음) - 고객정보 사용 정도의 '없다'와 '연간' 사용은 고객정보 사용이 거의 없으므로 측정값을 매우낮음으로 분류
업무지장	1) 지장 없다 2) 지장 있다 3) 고객정보 식별자 자체가 없다.	- '식별자 자체가 없다' 는 표시제한 대상이 없으므로 업무지장 '없다'로 분류

이상 업무 경력자는 전체의 40%이며, 5년 이상 업무 경력자는 77%이다.

지점에서는 전국적으로 총 30개의 지점에 설문서를 배포하였고, 20개 지점의 설문서를 회수하였다. 회수된 설문서 중 지점장 및 팀장은 관리 업무를 주로 수행하므로 고객정보를 주로 사용하는 내부 정보시스템 사용자의 실무와는 거리가 있어 통계 검증 대상에서 제외하였다. 또한 특정 지점의 설문 내용으로 치우치지 않도록 지점별로 회수 설문을 2개씩 무작위로 선정하여 총 40개를 통계검증 대상 설문으로 하였다.

본사에서는 부서별 1인을 무작위 선정하여 총 44명에게 설문서를 배포하였고, 설문대상 중 30명 설문을 회수하여 통계 검증으로 사용하였다.

고객센터에서는 고객센터 근무자를 대상으로 무작위 선정된 총 50명에게 설문서를 배포하였고, 설문 대상 중 20명의 설문을 회수하여 통계 검증으로 사용하였다.

4.1.2 분석 방법

자료 분석을 위한 통계 검증은 로지스틱 회귀분석을 사용하여 설명변수(독립변수)인 '고객정보 사용 정도'가 연구 관심결과(종속변수)인 표시제한으로 인한 '업무지장'과의 관련성 여부(영향을 미치는지?)를 분석하였다. 또한 관련성이 있을 경우는 odds ratio(OR 추정치)를 산출하여 설명변수가 연구 관심결과로 나타나는 확률(영향도)을 구하였다.

설명변수가 연구 관심결과와의 관련성 여부(영향을 미치는지?)는 'omnibus tests of model coefficients'로 검증하였다. 'omnibus tests of model coefficients' 의 model chi-square 검정 통계량값(sig)은 작을수록 좋다. 본 연구에서는 검정 통계량인 sig값(유의도)이 95%신뢰구간인 0.05이하일 경우에 유의한 결과로 측정하였다. 'omnibus tests of model coefficients' 결과표에서 sig(유의도)가 유의수준보다 작아서 검정결과가 유의하다면 설명변수(독립변수)는 연구 관심 결과(종속변수)와 관련이 있다는 것을 의미한다.

로지스틱 회귀 계수 추정치의 유의성 검정도 95% 신뢰구간인 0.05 이하일 경우에만 유의한 결과로 하였다. 즉 sig 값이 0.05이하의 값일 때에는 설명변수(고객정보 사용 정도)가 연구 관심결과(표시제한으로 인한 업무지장)에 유의한 영향을 미치며, 이때 영향을 미치는 정도값(영향도)인 OR 추정치인 '(Exp(B))'를 산출하였다. OR 추정치는 '설명변수가 1 증가할 때, 연구 관심결과의 증가율' 즉 설명변수가 연구 관심결과에 미치는 영향도를 의미한다.

로지스틱 회귀 모형을 통한 예측이 얼마나 정확한지 평가하는 예측 효율성(overall percentage)의 cutoff value는 0.5로 하였다. 즉 0.5보다 크면 '1'로 분류하여 업무지장이 '있다'로 분류하였고, 0.5보다 작으면 '0'으로 분류하여 업무지장이 '없다'로 분류하였다.

4.2 주민등록번호 표시제한

고객정보 식별자 중 주민등록번호에 대하여 주민등록번호 13자리 중 뒷부분의 7자리 표시제한으로 인한 업무지장 영향을 분석하였다. 표시제한은 증권 업무 정보시스템의 화면, 다운로드 파일, 인쇄물을 대상으로 하였으며 분석 결과는 다음 <표 7>과 같다.

<표 7> 주민등록번호 표시제한

고객정보 사용정도	고객정보 식별자 (주민등록번호) 표시제한		omnibus tests of model coefficients		로지스틱 회귀계수 추정치와 유의성 검증					예측 효율성
	번호	표시제한 내용	Chi-Square	sig	회귀계수 추정치	표준 오차	통계량	sig	OR 추정치	
화면조회 사용정도	1	화면에 주민등록번호 7자리 표시제한	26.334	0.000	0.571	0.145	15.606	0.000	1.770	75.6%
파일 다운로드 사용정도	2	다운로드 파일에 주민 등록번호 7자리 표시제한	2.401	0.121	0.152	0.098	2.414	0.120	1.164	66.7%
인쇄 사용정도	3	인쇄물에 주민등록번호 7자리 표시제한	0.109	0.741	0.032	0.097	0.109	0.741	1.032	77.8%

<표 7>에 나타난 바와 같이 주민등록번호 뒤 7자리 표시제한으로 인한 업무지장 분석결과는 3가지 중 1가지만 연구 관심결과인 업무지장에 유의한 영향을 미치는 것으로 나타났다.

유의한 결과로 분석된 화면 표시제한은 'omnibus tests of model coefficients'의 검정 통계량 값(sig)이 0.000으로 유의수준(0.05) 이하임에 따라 설명변수가 연구 관심결과와 관련성이 있음을 알 수 있다. 또한 회귀 계수 추정치에 대한 sig 값도 0.000으로 유의수준(0.05) 이하이며 영향도를 나타내는 OR 추정치는 1.770으로 분석되었다. 즉 고객정보의 화면조회 사용 정도가 한 단계 높아짐에 따라 주민등록번호 뒤 7자리 표시제한으로 인한 업무지장 영향은 1.770배가 증가함을 알 수 있다.

반면 다운로드 파일과, 인쇄물의 표시제한으로 분석 결과는 'omnibus tests of model coefficients'의 검정 통계량 값(sig)이 95% 신뢰구간에 유의하지 않음에 따라 연구 관심결과인 업무지장과 관련성이 없었고, 로지스틱 회귀계수도 유의하지 않은 것으로 나타났다.

이를 통하여 고객정보를 화면에서 조회하는 사용이 많은 사람(부서)들에게 주민등록번호 뒤 7자리를 화면에 표시제한하는 보안통제는 사용이 증가함에 따라 1.770배의 업무지장 영향도가 있으므로 보안통제 필요성과 업무영향간의 경중을 신중하게 검토해야 할 것이다. 그러나 고객정보를 파일로 다운로드하거나 인쇄하는 사용은 업무지장 영향과 관련이 없음에 따라, 주민등록번호 표시제한 보안정책을 수립할 때 해당 고객정보 사용이 많고 적음을 고려하지 않아도 됨을 알 수 있다.

4.3 계좌번호 표시제한

고객정보 식별자 중 계좌번호에 대하여 계좌번호 8자리 중 뒷부분의 3자리 표시제한으로 인한 업무지장 영향도를 분석하였다. 분석 결과는 다음 <표 8>과 같다.

<표 8>에 나타난 바와 같이 계좌번호 뒤 3자리 표시제한으로 인한 업무지장 분석결과는 3가지 중 3가지 모두가 연구 관심결과인 업무지장에 유의한 영향을 미치는 것으로 나타났다. 앞서 진행한 주민등록번호 뒤 7자리 표시제한보다 많은 업무지장 영향이 있음을 알 수 있다.

영향도를 나타내는 OR 추정치는 4번이 1.824, 5번이 1.348, 6번이 1.187로 분석되었다.

<표 8> 계좌번호 표시제한

고객정보 사용정도	고객정보 식별자 (계좌번호) 표시제한		omnibus tests of model coefficients		로지스틱 회귀계수 추정치와 유의성 검증					예측 효율성
	번호	표시제한 내용	Chi-Square	sig	회귀계수 추정치	표준 오차	통계량	sig	OR 추정치	
화면조회 사용정도	4	화면에 계좌번호 3자리 표시제한	31.650	0.000	0.601	0.123	23.900	0.000	1.824	86.7%
파일 다운로드 사용정도	5	다운로드 파일에 계좌번호 3자리 표시제한	8.232	0.004	0.299	0.113	6.967	0.008	1.348	62.2%
인쇄 사용정도	6	인쇄물에 계좌번호 3자리 표시제한	4.374	0.036	0.171	0.083	4.211	0.040	1.187	57.8%

즉 고객정보 사용 정도가 한 단계 높아짐에 따라 계좌번호 뒤 3자리 표시제한으로 인한 업무지장 영향은 4번 1.824배, 5번 1.348배, 6번 1.187배가 각각 증가함을 의미한다.

계좌번호 화면 표시제한은 영향도가 1.824로써 다른 경우에 비해 상대적으로 높다. 이는 표시제한 보안정책 수립 시, 보안통제 필요성과 업무영향간의 경중을 더욱 신중하게 검토해야 함을 의미한다. 그리고 다운로드 파일과 인쇄물에 표시제한하는 보안통제는 각각 1.348과 1.187의 업무지장 영향도가 나타났다. 이 또한 업무지장 영향도가 있으므로 표시제한 보안정책 수립 시 각각의 영향도를 고려해야 할 것이다.

4.4 고객번호 표시제한

고객정보 식별자 중 고객번호에 대하여 고객번호 9자리 중 뒷부분의 3자리 표시제한의 업무지장 영향도를 분석하였다. 분석 결과는 다음 <표 9>와 같다.

<표 9>에 나타난 바와 같이 고객번호 뒤 3자리 표시제한으로 인한 업무지장 분석결과는 3가지 중 2가지가 연구 관심결과인 업무지장 영향에 유의한 결과로 나타났다.

유의한 결과로 분석된 7번, 8번의 OR 추정치는 각각 1.528, 1.279로 분석되었다. 즉 고객정보 사용 정도가 한 단계 높아짐에 따라 고객번호

<표 9> 고객번호 표시제한

고객정보 사용정도	고객정보 식별자 (고객번호) 표시제한		omnibus tests of model coefficients		로지스틱 회귀계수 추정치와 유의성 검증					예측 효율성
	번호	표시제한 내용	Chi-Square	sig	회귀계수 추정치	표준 오차	통계량	sig	OR 추정치	
화면조회 사용정도	7	화면에 고객번호 3자리 표시제한	15.576	0.000	0.424	0.129	10.741	0.001	1.528	65.6%
파일 다운로드 사용정도	8	다운로드 파일에 고객번호 3자리 표시제한	6.323	0.012	0.246	0.099	6.106	0.013	1.279	72.2%
인쇄 사용정도	9	인쇄물에 고객번호 3자리 표시제한	3.948	0.047	0.180	0.093	3.700	0.054	1.197	70.0%

뒤 3자리 표시제한으로 인한 업무지장 영향은 7번 1.528배, 8번 1.279배가 각각 증가함을 의미한다.

이를 통하여 고객정보를 화면에서 조회하는 사용이 많은 사람(부서)들에게 고객번호 뒤 3자리를 화면에서 표시제한하는 것은 1.528배의 업무지장 영향이 있으므로 해당 영향도를 고려하여 표시제한 보안정책에 신중을 기할 필요가 있다. 그리고 고객정보를 파일로 다운로드하는 사용이 많은 사람(부서)들은 고객번호 뒤 3자리를 다운로드 파일에 표시제한하는 보안통제는 1.279배의 업무지장 영향도가 있다. 이 또한 영향도가 있으므로 표시제한 보안정책 수립 시 해당 영향도를 고려하여야 할 것이다.

인쇄물 표시제한의 경우는 'omnibus tests of model coefficients'의 검정 통계량 값은 0.047로 유의하여 설명변수(인쇄 사용)가 연구 관심 결과(업무지장)와 관련성은 있었으나, 회귀 계수 추정치(0.180)에 대한 유의도(sig) 값이 0.054로 95% 신뢰구간에 유의하지 않아 영향도 분석은 제외하였다.

4.5 표시제한 보안통제 高低분석

4.5.1 보안통제 高低 시나리오

표시제한 보안통제 수준이 높을 경우(高)와 낮을 경우(低)의 업무지장 영향도를 비교 분석하기 위하여 주민등록번호, 계좌번호, 고객번호 각각에 대하여 표시제한 보안통제 高低에 따른 업무지장 설문을 병행하였다. 표본 구성과 설문 및 표시제한 대상은 동일하며, 실증 분석은 앞서 진행한 방법과 동일하게 '로지스틱 회귀분석'으로 통계 검증을 실시하였다. 표시제한 보안통제 수준의 高低 시나리오는 다음 <표 10>과 같이 정의하였다.

<표 10> 표시제한 보안통제 수준의 高低 시나리오

고객정보 식별자	보안통제 수준 高 (높음)	보안통제 수준 低 (낮음)
주민등록번호	주민등록번호 뒤 7자리 표시제한	주민등록번호 뒤 4자리 표시제한
계좌번호	계좌번호 뒤 3자리 표시제한	계좌번호 뒤 2자리 표시제한
고객번호	고객번호 뒤 3자리 표시제한	고객번호 뒤 2자리 표시제한

보안통제 수준이 높은 경우는(高) '화면, 다운로드 파일, 인쇄물 각각에 대하여 주민등록번호 뒤 7자리', '계좌번호 뒤 3자리', '고객번호 뒤 3자리'의 표시제한 업무지장 설문 결과를 모두 더한 후 평균을 구하였다. 평균값이 로지스틱 회귀분석의 cutoff value인 0.5보다 크면 '1'로 분류하여 업무지장이 '있다'로 분류하였고, 0.5보다 작으면 '0'으로 분류하여 업무지장이 '없다'로 분류하였다.

동일한 방법으로 보안통제 수준이 낮은 경우는(低) '화면, 다운로드 파일, 인쇄물별로 주민등록번호 뒤 4자리', '계좌번호 뒤 2자리', '고객번호 뒤 2자리'의 표시제한 업무지장 설문 결과를 모두 더한 후 평균을 구하였다. 평균값이 로

지스틱 회귀분석의 cutoff value인 0.5보다 크면 '1'로 분류하여 업무지장이 '있다'로 분류하였고, 0.5보다 작으면 '0'으로 분류하여 업무지장이 '없다'로 분류하였다.

4.5.2 표시제한 보안통제 高低 분석

업무 정보시스템에서 고객정보 사용 정도와 표시제한 보안통제가 높은 경우와 낮은 경우의 업무지장 영향도 분석 결과는 다음 <표 11>과 같다.

<표 11> 표시제한 보안통제 高低 분석

고객정보 사용정도	고객정보 식별자 표시제한	omnibus tests of model coefficients		로지스틱 회귀계수 추정치와 유의성 검증					예측 효율성
		Chi-Square	sig	회귀계수 추정치	표준 오차	통계량	sig	OR 추정치	
화면조회 사용정도	화면 표시제한 高	29.714	0.000	0.598	0.140	18.263	0.000	1.819	80.0%
	화면 표시제한 低	18.457	0.000	0.462	0.131	12.385	0.000	1.587	68.9%
파일 다운로드 사용정도	다운로드 파일 표시제한 高	8.369	0.004	0.285	0.103	7.659	0.006	1.329	66.7%
	다운로드 파일 표시제한 低	4.267	0.039	0.199	0.098	4.159	0.041	1.221	66.7%
인쇄 사용정도	인쇄물 표시제한 高	2.511	0.113	0.140	0.090	2.411	0.120	1.150	68.9%
	인쇄물 표시제한 低	3.948	0.047	0.180	0.093	3.700	0.054	1.197	70.0%

<표 11>에 나타난 바와 같이 화면 표시제한과 다운로드 파일 표시제한의 2가지가 유의하여 비교 분석이 가능하였다.

업무 정보시스템에서 고객정보를 화면조회하는 사용은 화면 표시제한 보안통제 수준이 높을 때는 OR 추정치가 1.819이고, 표시제한 보안통제 수준이 낮을 때는 1.587의 업무지장 영향도가 나타났다.

엑셀 등의 파일로 다운로드하는 고객정보 사용은 다운로드 파일에 표시제한 보안통제 수준이 높을 때는 OR 추정치가 1.329, 표시제한 보안통제 수준이 낮을 때는 1.221의 업무지장 영향도가 나타났다.

인쇄물 표시제한의 경우는 'omnibus tests of model coefficients'의 검정 통계량 sig값이 유의하지 않거나, 로지스틱 회귀계수 추정치의 유의성 검정이 95% 신뢰구간인 유의수준 0.05이하가 되지 못하여 분석에서 제외하였다.

표시제한 보안통제 高低 분석을 통하여 보안통제 수준이 높을수록 업무지장 영향도가 커지는 것을 알 수 있다.

V. 결 론

5.1 연구 결과

본 연구는 증대되는 개인정보 침해 및 내부자의 고객정보 오·남용을 예방하기 위하여 기업

이 적용하고 있는 보안통제와 그로 인하여 업무지장에 미치는 영향을 연구하였다.

이를 통하여 학문적으로는 등간 척도로 측정되는 설명변수와 이분형 값으로 측정되는 종속변수와의 인과 관계를 파악하고, 인과 관계가 있을 경우 설명 변수가 종속 변수에 미치는 영향의 정도를 수치화함으로써 정량적 데이터를 기반으로 보안정책을 수립할 수 있는 기법을 제시하였다.

보안정책은 접속 정도, 사용 정도와 같이 등간 척도로 분류될 수 있는 다양한 경우에 대하여 이분적 의사 결정을(보안통제 적용 여부, 권한 부여 여부 등) 요구하는 경우가 많다. 이러한 경우에 본 연구에서 수행한 방법을 활용한다면 실무적으로도 효과적 보안정책을 수립할 수 있을 것이다.

본 연구에서 실증 분석한 결과를 요약하면, 주민등록번호 뒤 7자리 표시제한으로인한 업무지장은 화면 표시제한만 유의한 영향을 미치는 것으로 분석되었다. 계좌번호(총8자리) 뒤 3자리 표시제한으로인한 업무지장은 화면 표시제한, 다운로드 파일 표시제한, 인쇄물 표시제한 모두가 유의한 영향을 미치는 것으로 분석되었다. 고객번호(총9자리) 뒤 3자리 표시제한으로 인한 업무지장은 화면 표시제한과 다운로드 파일 표시제한이 유의한 영향을 미치는 것으로 분석되었다. 표시제한 보안통제 高低 분석에서는 보안통제 수준이 높을 때가 낮을 때보다 업무지장 영향도가 높았다.

실증분석 결과를 통하여 연구 결과를 정리하면 다음과 같다.

첫째 화면 표시제한이 다운로드 파일이나 인쇄물 표시제한보다 업무지장 영향도가 높게 나타났다. 고객정보 식별자 중에서는 계좌번호가 주민등록번호와 고객번호보다 표시제한으로 인한 업무지장 영향이 높았다. 따라서 화면조회 사용이 많은 사람(부서)들과 계좌번호에 대하여는 더욱 신중한 표시제한 보안정책 검토가 필요하다. 업무 수행이 중요하다면 보안통제 수준을 낮추는 정책을 고려할 수 있고, 고객정보 보호가 중요하다면 업무영향을 감수하고, 높은 보안통제 수준을 고려할 수 있을 것이다. 업무지장 영향과 관련성이 없는 경우는 해당 고객정보 사용의 많고 적음을 고려하지 않아도 됨을 알 수 있었다.

둘째 고객정보 식별자 표시제한 高低 분석을 통하여 표시제한 보안통제 수준이 높을수록 업무지장 영향도도 높아짐을 알 수 있었다.

셋째 표시제한으로 인한 각각의 영향 여부와 영향도는 다르게 나타났다. 이는 기업이 표시제한 보안통제 정책을 수립할 때 일률적 보안정책이 아닌, 각각의 업무지장 영향을 고려한 보안정책 수립이 필요함을 의미한다.

기업은 업무 정보시스템 사용 로그에서 화면조회, 파일 다운로드, 인쇄 등의 고객정보 사용 정도를 사용자별, 부서별로 추출할 수 있다. 추출된 고객정보 사용과 본 연구 결과를 활용한다면 고객정보를 보호하면서 표시제한 보안통제로 인한 업무영향을 최소화하여 내부 사용자들의 업무 효율성을 높일 수 있을 것이다.

5.2 연구 한계 및 향후 연구

본 연구를 통하여 기업이 고객정보 식별자 표시제한 보안통제를 적용할 경우 업무 수행에 미치는 영향을 고려하여야 한다는 의미있는 시사

점을 도출하였음에도 다음과 같은 연구 한계가 있다.

본 연구는 중요 정보의 노출을 최소화하기 위한 표시제한 보안통제와 업무지장 영향에 대한 연구이었다. 정보보안에는 표시제한 외에도 인증, 권한관리, 암호화 등 다양한 보안통제가 존재한다. 이러한 다양한 보안통제 영역에서의 연구가 필요하다.

또한 본 연구는 국내 금융업종 중 증권 업무를 중심으로 연구를 수행하였다. 금융권내에서도 다양한 금융 비즈니스 가 존재하며, 금융권외에도 공공, 제조, 통신 등 다양한 업종이 존재한다. 보안통제로 인한 업무영향은 수행하는 업무 형태에 따라 영향 여부와 영향도가 다를 수 있으므로 향후 연구에서는 다양한 연구 모집단을 대상으로 연구가 확대되어야 할 것이다.

참고문헌

강상욱, 박승범, 강경훈, 강호갑, 이규정, 디지털 콘텐츠 고유 식별자를 이용한 불법콘텐츠 추적연구, 한국경영정보학회 추계학술대회, 2007, pp.481-486

금융감독원, IT검사매뉴얼 제6장 IT서비스제공 및 지원 8.전자금융 거래등, 2013, pp.489

금융감독원, IT검사매뉴얼 제6장 IT서비스제공 및 지원 8.전자금융 거래등, 2013, pp.489

금융감독원, 개인신용정보 관리·보호 모범규준, 2005

김정연, 개인정보 유출이 기업의 주가에 미치는 영향, 한국전자거래학회지 v.18 no.1, 2013, pp.1-11

김영희, 정기원, 컴포넌트 기반 개발에서의 프로세스 관리와 산출물 관리를 통합하는 도구의 모델 연구, 한국인터넷 정보학회, 제5권 4호, 2004, pp.11-22

김윤용, 의학통계학 '로지스틱 회귀 분석', 2011, http://blog.naver.com /libido1014?Redirect= Log&logNo=120122772781

김희수, 이평로, 신정요, 개인정보 수집·저장·이용의 적법성과 한계, 국가인권위원회 연구용역보고서, 2006

나석현, 박석, 사용목적 분류를 통한 프라이버시 보호를 위한 접근제어 모델, 정보보호학회논문집. 제16권 제3호, 2006, pp.39-52

노영희, 도서관의 개인정보보호정책 개발 및 제안에 관한 연구, 한국문헌정보학회지 v.46 no.4, 2012, pp.207-242

박경아, 이대용, 구철모, 최종사용자의 인터넷과 소셜 네트워크 보안 행동에 대한 실증 연구, 정보시스템연구. v.21 no.4 , 2012, pp.1-29

박용성, 공공 조직내 정보화 시스템의 내재화 요인에 대한 연구, 한국정책분석평가학회, 권3호, 2008, pp. 59-91

박종찬, 민간부문 및 기업의 개인정보 활용성 및 효율성을 고려한 개인정보보호기본법의 바람직한 제정 방향에 관한 연구, 경상논집:고려대학교, vol 29. no 2, 2006, pp. 117-135

박철주, 임명성, 보안 대책이 지속적 보안 정책 준수에 미치는 영향, 디지털정책연구 (The Journal of Digital Policy &

Management), v.10 no.4, 2012, pp.23-35

방송통신위원회, 개인정보의 기술적·관리적 보호조치 기준, 방송통신위원회 고시 제2012-50호, 2012

유한나, 김형주, 이재식, 박태성, 전문석, 국내 개인정보보호법의 발전방향 제시를 위한 국외 개인정보보호법 분석, 정보보호학회논문지 v.22 no.5, 2012, pp.1091-1102

이동훈, 전자정부와 개인정보보호, Information Security Review 제1권 제2호, 2004, pp76

이석형, 김광영, 류범종, 곽승진, 디지털자료 납본 보상금관리시스템에 관한 연구, 한국도서관·정보학회지, 제40권 제1호, 2009, pp.233-251

이경근, 류시욱, 정보보안 방안 선택을 위한 퍼지 AHP 방법의 비교 검토, 정보시스템연구. v.19 no.3, 2010, pp.59-73

이기혁, 윤재동, 민간 기업의 개인정보 유출 위험에 대한 측정 방법과 그 사례에 대한 연구, 정보보호학회지 v.18 no.3, 2008, pp.93-100

이민영, 주민등록번호 남용억제에 관한 법제적 고찰, 정보통신정책. 제16권 8호. 통권 346호, 2008, pp.1-17

이은곤, 인지된 정보통제가 소셜 네트워크 이용자의 정보제공 의도에 미치는 영향, 한국전자거래학회지 v.18 no.1, 2013, pp.107-127

이장형, 김종원, 보안 및 통제와 정보기술 사용자의 성격의 관계, 정보시스템연구. v.19 no.3, 2010, pp.1-12

임규건, 이해령, 증권사 영업사원의 개인 성향이 PI저항에 미치는 영향에 관한 연구, JOURNAL OF INFORMATION TECHNOLOGY APPLICATIONS & MANAGEMENT, 14권. 4호, 2007, pp.199-219

장덕성, 누출 차단과 식별을 위한 다큐먼트 보안 디자인, 한국컴퓨터정보학회지, 제10권 제2호, 2003, pp. 16-24

정성민, 금융 어플리케이션을 위한 효율적인 역할추출과 안전한 역할기반 접근통제 적용 방안, 정보보호학회지 v.18 no.5, 2008, pp.49-61

정우진, 신유형, 이상용, 금융회사의 고객정보보호에 대한 내부직원의 태도 연구, Asia pacific journal of information systems / v.22 no.1, 2012, pp.53-77

장은경, 김성천, 나광식, 손나래, 개인정보 도용 방지 및 도용 피해 회복방안에 관한 연구, 한국소비자보호원, 2006

정태석, 임명성, 이재범, 기업의 지속적 정보보안 강화를 위한 접근법 개발, 디지털정책연구(The Journal of Digital Policy & Management), v.10 no.2, 2012, pp.1-10

홍영란, 김동수, CC인증이 정보보호 솔루션의 보안성에 미치는 영향 분석, 한국전자거래학회지 v.17 no.4, 2012, pp.57-68

황기영, 주성원, 네트워크 기반의 보안정책 관리 모델 체계에 관한 연구 : 신속성, 보안강화 측면의 관리모델, 한국정보보호학회지, Vol 18. no3, 2008, pp.109-117

Allaert, F.A. and Quantin, C., The patients' personalized medical record: Thoughts on the single point of access and the

masking of information in the record, IRBM, Vol. 30, No. 3, 2009, pp.114-118

Chan, M., Woon, I. and Kankanhalli, A., Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior, Journal of Information Privacy & Security, 1(3), 2005, pp.18-41

Culnan, M.J. and Bies, R.J., Consumer privacy : Balancing economic and justice considerations, Journal of SocialIssues, Vol. 59, No. 2, 2003, pp.323-342

OECD, Guidelines on the protection of privacy and trans-order flow of personal data, annex to the recommendation of the council of 23rd September. Pt. 1. cl.(1)(b). 1980

Herath, T. and Rao, H.R., Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations, European Journal of Information Systems, 18, 2009, pp.106-125

ISO/IEC 10181-3, Security frameworks in open systems : Access control Framework, ITU-T Rec. X.812, 1996

Laudon, K. and Laudon, J., The Essentials of Business Information Systems, 12/E, Prentice Hall, 2012

Pepard, J., Customer Relationship Management (CRM) in Financial Services, European Management Journal, Vol. 18, No. 3, 2000, pp. 312-327

Priscilla, C. and William, Y. Arms., Reference Linking for Journal Articles, D-Lib Magazine, 5(7/8), 1999

Sandhu, R.S. and Samarati, P., Access Control : Principles and Practice, IEEE Communications Magazine, 1994, pp.40-48

Werlinger, R., Hawkey, K. and Botta, D., Beznosov, K., Security Practitioners in Context: Their Activities and interactions with Other Stakeholders within Organizations, International Journal of Human-Computer Studies, 67, 2009, pp.584-606

신상철(Shin, Sangchul)

동국대학교(정보관리학과)를 졸업하고, 동국대학교 국제정보대학원(정보보호학과) 석사과정을 졸업하였으며, 동국대학교(경영정보학과) 박사과정을 수료하였다. 현재 하나금융지주 회사에서 금융 정보보안을 담당하고 있으며, 주요 관심분야는 정보보호 거버넌스, 정보보안 아키텍처, 정보보안 업무 프로세스 효율화 등이다.

이영재(Lee, Youngjai)

동국대학교(전자계산학과)를 졸업하고 George Washington 대 정보관리 전공으로 이학박사를 취득하고 현재 동국대학교 경영대학 경영정보학 교수로 재직 중이다. 주요 관심분야는 의사결정, 비즈니스 위기관리, 재난관리 등이다.

<Abstract>

Business Performance Impact Caused by Display Restriction of Customer Information Identifier:
Focusing on Domestic Securities Business

Shin, Sangchul · Lee, Youngjai

Recently, enterprises have reinforced security control in order to prevent infringement of personal information and abuse of customer information by insiders. However, the reinforcement of security control by enterprises makes it difficult for internal users to perform business by using a business information system. There is, therefore, a need for research on various fields, which makes it possible to establish an appropriate security control policy while minimizing an impact on business. The present research verifies and analyzes an impact on difficulty in business of internal users using customer information, which is caused by security control performed by display restriction on customer information identifiers. The present research is intended to academically develop a technique for statistically analyzing an impact degree and a causal relationship between security control and an impact on business, which is a dichotomous variable, and to practically contribute to the establishment of an efficient security policy in consideration of an impact on business when an enterprise applies security control. A research target was internal business information systems of domestic securities enterprises, data was collected by questionnaire, and verification/analysis was performed by logistic regression analysis.

Keywords: Security Controls, Business Impact, Display Restriction, Security Policy Customer Information Identifiers

* 이 논문은 2013년 10월 17일 접수하여 1차 수정을 거쳐 2013년 12월 3일 게재 확정되었습니다.