情報保護學會論文誌
第19卷 第2號, 2009. 4

컨택센터의 고객 개인정보 보호 모델

권 영 관,[1†] 염 흥 열[2‡]
[1]카스정보통신(주), [2]순천향대학교

Security Management Model for Protecting Personal Information for the Customer Contact Center

Young-Kwan Kwon,[1†] Heung-Youl Youm[2‡]
[1]CASTEL Co.,Ltd, [2]Soonchunhyang University

요 약

일반적으로 컨택센터에서는 고객의 개인정보 취급이 필수적이며, 중요정보자산인 고객의 개인정보를 취급하는 고객정보취급자의 수가 매우 많아, 내부 고객정보 유출 가능성 등의 위협요인이 존재하고 있다. 본 논문에서는 컨택센터의 특성과 위협요인 및 취약점을 분석하였으며, 고객의 개인정보를 효과적으로 보호할 수 있는 방안을 연구하였다. 또한 내부 정보 유출 가능성을 사전에 예방할 수 있는 개인정보 보호 방안을 마련하였다. 그리고 컨택센터의 고객 개인정보보호 방안에 대하여 ISMS(Information Security Management System) 표준을 따르는 "컨택센터의 고객 개인정보 보호 모델"을 수립하여 제안한다.

ABSTRACT

In this paper, we analyze the Contact Center's specific-security characteristics, including the threat model and weakness and study effective security measures focussing on protecting customer's personal information. Also, we establish the information security management system to reduce the possibility of information leakage from the internal employee in advance. As a result, we propose the "Security management model for protecting personal information for customer Contact Center" that complies with current ISO/IEC JTC 1 ISMS 27000 series standards.

Keywords: Contact Center Security, Personal Information Security, Security Management Model

I. 서 론

현대사회의 기업들은 기업의 고객이나 소비자에 대한 서비스 품질향상을 위하여 자사의 상품이나 서비스 등에 대한 정보를 더 많이 고객에게 전달하고, 그에 대한 고객의 문의사항이나 요구사항 등을 보다 빠르고 편리하게 응대하여, 고객을 만족시키는 노력을 기우리고 있다. 이러한 활동의 주체가 되는 것의 하나가 고객접점인 컨택센터이며, 컨택센터는 고객 상담의 역할뿐만 아니라 기업의 수익창출 및 기업홍보 등의 전략적 창구로서 그 중요성이 커지고 있다. 컨택센터에서는 고객정보 등의 중요 정보자산을 활용하는 업무가 증대되고 있다. 일반적으로 개인정보는 "그 사람 자체"를 나타내는 중요한 정보로서 정보사회의 진전에 따라 개인정보의 유·무형가치가 증대 되고 있으며 정보사회의 핵심으로 평가 받고 있다. 따라서 개인정보는 철저하게 보호되어야 하는데, 요즈음 언론보도 등을 통하여 알려지고 있는 바와 같이 크고 작은 개인정보침해사고들이 많이 발생하고 있다. 이러한 개인정보유출에 대한 피해는 당사자들 뿐 만 아니라 관련회사 등에 치명적인 손실을 가져다 줄 수 있다.

컨택센터에 관련된 주요 개인정보 침해사례로는,

접수일(2008년 11월 11일), 수정일(2009년 1월 9일), 게재확정일(2009년 1월 30일)
† 주저자, ucop@paran.com
‡ 교신저자, hyyoum@sch.ac.kr

일본야후BB(BroadBand)의 고객 개인정보 유출을 들 수 있다. 정보유출자(전 야후BB고객센터 직원)는 야후BB 고객센터에서 근무하며 DB열람 등을 통해 고객정보를 입수하여 야후BB 고객 약451만 명의 개인정보를 유출하였다[1]. 국내에서는, 최근의 개인정보유출 사례로 1,100만 여명의 정보가 유출돼 사상 최대로 꼽히는 G사의 개인정보유출 사고를 들 수 있다. G사의 고객 개인정보를 유출한 사람은 고객정보 관리업무를 맡은 G사의 자회사 직원이었다. 이 직원은 한 달에 걸쳐 고객정보를 빼돌렸고 범행을 감추려고 사용하던 PC의 하드디스크를 마음대로 바꿨지만 회사 측은 이를 전혀 몰랐다고 한다[2].

컨택센터의 운영은 상품안내, 단순제품출시에 대한 안내, A/S(After Service), 교환이나 반품, 서비스 안내 등 산업부문 모든 분야에 확대되고 있다. 이러한 컨택센터의 주 업무는 고객에게 상담서비스를 제공하는 것이므로 업무처리 중에, 고객확인 및 고객서비스를 위한 개인정보를 취급하게 된다. 또한 컨택센터는 그 업무특성상 구성원의 대부분이 개인정보를 취급하므로 규모가 큰 컨택센터 일수록 고객정보 취급자수도 많아지게 된다. 일반적으로 주요정보자산의 보호대책으로 비인가자의 접근을 통제하거나 해킹방지 대책 등을 강구하고 있으며, 내부의 개인정보유출가능성 등을 줄이기 위하여 개인정보 취급자를 최소한으로 제한하고 있다.

그러나 컨택센터는 보안관점에서 봤을 때 매우 많은 인원이 개인정보를 취급하고 있으므로 일반적인 정보보호방안으로는 미흡한 면이 많다. 고객의 데이터베이스에 접속할 수 있는 고객정보취급자는 마음만 먹으면 손쉽게 정보를 유출할 가능성이 있는 위협요인이 상존하고 있기 때문이다. 컨택센터에서의 고객 개인정보 유출에 대한 위협요인 등에 효과적으로 대응하기 위해서, 컨택센터의 구성원 대부분은 고객정보취급자이며 그 취급자의 수가 매우 많은 등의 특성을 반영한 대책방안에 대한 연구가 필요하였다. 따라서 개인정보 관련 규정, 정보보호관리체계 등에 대한 분석 검토 및 컨택센터의 특성분석을 통하여 컨택센터에서 효과적으로 개인정보를 보호할 수 있는 방안을 연구하였다.

II. 컨택센터의 특성 및 정보보호 현황

2.1 컨택센터의 정의

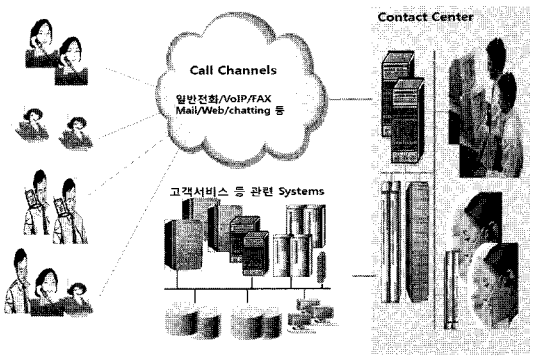
컨택센터는 기업이나 관공서 등과 고객 사이에 각종 정보통신 수단을 통한 커뮤니케이션적인 접촉이 이루어지는 곳으로 기업의 비즈니스에서 그 역할과 위상이 커지면서 매우 중요한 비즈니스 요소 중의 하나로 자리 잡고 있다. 컨택센터는 고객 상담이나 불만사항 처리, 주문접수처리, 제품설명 및 고객의 의문점이나 궁금증을 해소시켜주고, 마케팅활동이나 캠페인을 전개하는 등의 업무를 수행하는 중요한 고객접점(Consumer Contact Point)이라고 할 수 있다. 최근에는 신규 상품안내, 서비스 안내, 제품 기술지원, 설문조사, 여론조사 등 모든 분야의 고객접촉 채널로 컨택센터가 활용되고 있는 추세이다[3].

이러한 컨택센터는 고객센터, 고객 상담센터, 고객서비스센터, 고객감동센터, 고객행복센터, 소비자보호실, 민원실 등 다양한 형태로 존재하고 있으며, 기업이나 관공서 등에 따라 다양하게 불리고 있다.

2.2 컨택센터의 운영

일반적으로 컨택센터 서비스의 구성요소는 고객(Customer), 상담원(agents), 시스템(Machine System), 관리정책(Management Policy) 등으로 구분할 수 있다[4]. 그 중에 상담원은 핵심구성요소라 할 수 있는데, 우리나라의 컨택센터에 종사하는 상담원 수는 약 35만 명 정도이며[5], 컨택센터의 적용분야 및 업무영역 등의 확대로 향후에는 그 수가 크게 증가할 것으로 전망된다.

컨택센터의 일반적인 구성계통도는 [그림 1]과 같으며, 컨택센터의 시스템 설비는 상담효율성, 고객서비스 품질향상, 상담능률 향상 등에 주 기능을 부여하고, 고객서비스시스템 또는 통합DB시스템 등은 상담원 등에게 고객정보를 제공하기 위하여 고객정보의 수집, 분류, 분석, 관리 등을 관장하고 있다.



[그림 1] 컨택센터 구성 계통도 예시

2.3 컨택센터의 특성

컨택센터의 특성은 사회적인 여건과 산업분야, 수행업무, 규모, 운영형태 등에 따라 달라질 수 있는데, 업무처리 중심으로 고객정보취급에 주안점을 두고 그 주요 특징을 살펴보면 다음과 같다.

1. 고객의 개인정보 취급이 필수적이다.

컨택센터는 기업 등이 최 일선에서 고객과 접촉할 수 있는 채널이며, 고객에 관한 정보를 상세하고 효과적으로 활용함으로서 고객에 대한 서비스의 질을 더욱 향상시킬 수 있다. 따라서 고객에 대한 정확한 고객정보데이터를 수집 및 분석하고, 상담이력 등을 기록, 유지하는 활동을 한다.

2. 고객 접촉채널이 다양화 및 통합화 되고 있다.

최근의 컨택센터는 고객의 편의성과 서비스 향상을 위하여 기존의 전화뿐만 아니라 Web-Call, e-Mail, FAX, Mobile 통신 등 고객과의 모든 접촉채널을 통합하는 추세이다. 따라서 각 고객에 대한 다양한 접촉채널 등의 정보가 필요하며, 상담 시 등에 쉽게 검색할 수 있는 형태로 데이터베이스에 존재하게 된다.

3. 컨택센터요원 대부분이 개인정보취급자이며 그 수가 매우 많다.

최근에는 컨택센터의 적용범위 확대 등으로 수백명에서 천명이상의 컨택센터들이 많아지고 있다. 반면에 컨택센터 요원들에 대한 보수와 처우는 낮고, 이직률은 높은 실정이다. 그리고 상담인력이 계약직이거나 비정규직인 경우도 상당부분 존재하고 있다. 따라서 컨택센터는 고객의 개인정보를 취급하는 고객정보취급인가자의 수가 매우 많아 타 산업에 비하여 정보유출 가능성 및 취약성이 크다고 할 수 있다.

4. 보안 정책은 주로 서비스시스템에 의존한다.

일반적으로 컨택센터의 시스템설비와 연동하여 운용되고 있는 각 분야별 서비스시스템이나 데이터베이스 시스템은 고객정보를 통합적으로 관리하며, 상담원 등의 요청에 의해 고객정보를 해당 상담원에게 제공하고 있다. 따라서 컨택센터의 보안정책은 해당 서비스 시스템이나 데이터베이스시스템의 정보보호정책에 의존하는 경우가 많으며, 이 정책들은 주로 외부인이나 비인가자에 대한 불법적인 접근을 막는 정보보호 대책 등을 강구 하고 있다.

2.4 컨택센터 위협요인 및 취약점 분석

컨택센터에서는 고객관련 정보의 이용에 있어, 주로 해당 서비스시스템 등에서의 보안대책에 의존하므로 많은 부분이 컨택센터의 특성을 반영하지 못하고 있는 실정이다. 컨택센터의 고객 개인정보 취급에 따른 위협요인과 취약점을 살펴보면 다음과 같다.

1. 정보보호침해사고의 대부분은 내부자에 의한 경우가 외부자에 의한 경우보다 많이 나타나고 있다.

일반적으로 개인정보 침해사례의 정보보호침해사고 발생비율은 내부 75%, 외부 25%의 비율을 나타내고 있다. 또한 내부 침해사고 중에 내부의 인가자에 의한 침해사고 발생이 77%를 점유하고 있다[6]. 따라서 컨택센터의 모든 상담원은 고객의 개인정보를 수시로 접하게 되므로, 이들로 인한 정보 누출의 위협요인 등에 대한 대책이 필요하다.

2. 컨택센터의 집중화 대형화로 개인정보취급자가 매우 많아지고 있다.

최근에는 상담원이 수백 명에서 천 명이상에 이르는 컨택센터들이 증가하고 있어 고객정보취급자가 매우 많아지고 있다. 따라서 종사원이 많은 대규모의 컨택센터는 소규모 컨택센터에 비해 정보누출에 대한 위협요인이 그만큼 높다고 볼 수 있다.

3. 고객의 개인정보보호 대책이 미흡하다.

일반적으로 상담원에게 고객정보를 제공하는 서비스시스템 등은, 주로 외부자나 비인가자에 의한 불법침입 등에 대한 정보보호대책을 강구 하고 있는 경우가 많다. 또한 대부분 주요정보자산취급자는 소수이므로 이들에 의한 내부정보 유출 방지 대책으로, 주로 교육훈련 등의 방법을 택하고 있다. 그러나 고객정보취급자가 매우 많은 대부분의 컨택센터에서도 고객의 개인정보 보호대책으로, 주로 교육훈련에 의존하고 있는 실정이다.

4. 컨택센터 특성에 맞는 정보보호 정책이 필요하다.

일반적인 정보보안 원칙중의 하나는 "고객의 개인정보를 취급하는 인가자의 수를 최소화 한다" 이다. 그러나 컨택센터는 업무특성상 거의 모든 구성원이 고객정보취급자이므로 일반적인 보안원칙과는 배치(背馳)된다. 따라서 컨택센터 특성에 맞는 정보보호정책을 수립하여 운영함이 바람직하다.

III. 컨택센터의 개인정보보호모델

컨택센터에서의 개인정보에 대한 위협요인과 고객정보 누출 가능성 등을 해결하기위하여 다음과 같은 방향으로 개선방안을 마련한다.

1. 컨택센터 특성에 맞는 개인정보 보호 방안을 수립한다.

개인정보 보호 방안으로 내부 정보 유출 가능성을 사전에 차단하거나 예방할 수 있도록 시스템적인 해결방안을 강구하고, 고객정보 누출 사고 발생 시에도 신속하게 대응 가능한 방안 등을 모색하여 적용한다.

2. "고객 개인정보 보호 모델"을 수립하여 제안한다.

제1항의 고객 개인정보보호 방안에 대하여 ISMS (Information Security Management System) 형식을 따르는 "컨택센터의 고객 개인정보 보호 모델"을 수립하여 제안한다.

3.1 컨택센터 개인정보보호 방안

컨택센터에서 고객의 개인정보를 효과적으로 보호하기 위한 방안에 대한 주요사항들을 정보보호정책, 개인정보취급자, 시스템설비 분야로 나누어 다음과 같이 제안한다.

3.1.1 정보보호정책

1. 대부분의 컨택센터에서의 개인정보 보호대책으로 교육에 의존하고 있으므로, 체계적이고 효과적인 개인정보보호를 위하여 시스템적인 접근 및 세부적인 운영방안을 다음과 같이 제시한다.

가. 시스템적인 대책을 강구할 수 있도록 하고, 시스템에서의 처리절차 등을 보강한다.

나. 개인정보취급자의 접근권한 및 범위를 업무특성에 맞게 세분화하여 부여한다.

다. 상담용 단말장치는 상담목적으로만 사용토록 한다. 상담용 단말장치로 개인용 컴퓨터(PC) 등을 사용하는 경우에는 저장기능, USB 포트, 프린트 등의 기능을 차단하거나 제한한다. 또한 메일에 의한 상담업무 외에는 메일 발송을 제한 또는 차단하고, 채팅상담을 위한 경우 외에는 채팅기능 차단, 그리고 파일전송 기능 등을 차단한다.

2. 많은 고객을 확보한 서비스나 상품을 취급하는 대형컨택센터 등은 개인정보 유출시 막대한 피해가 예상된다. 이에 대한 대책 방안으로는,

가. 개인정보접근 허용통제 및 한계치를 설정하여 운용한다. 즉, 한 명의 인가자가 정보자산에 접근하여 취급할 수 있는 정보의 한계치나 한 번에 조회할 수 있는 고객정보 범위 등을 설정한다.

나. 고객개인정보에의 접근기록이나 접근이력 등의 정보를, 필요시 해당상담원 등 개인정보취급자에게 알려준다. 고객 개인정보 취급에 대한 분석결과, 특이사항 등의 필요정보를 Pop-up이나 메일 등을 활용하여 해당 상담원 등에게 알려준다.

3. 소수의 주요고객에 대한 개인정보 유출 등은 쉽게 알 수 없고, 개인정보 누출 시에도 신속한 대응이 곤란하며 추적이 늦다. 이에 대한 대책으로,

가. 고객개인정보에 접근할 때마다 접근기록DB에 그 내역을 기록하고 분석, 관리할 수 있도록 한다.

나. 시스템에서 ID별, 그룹 별, 일자 별 등으로 개인정보 접근내역들을 알 수 있도록 한다. 이에 대한 사전 조치로 ID부여 시부터 상담그룹, 업무그룹, 고객 그룹 등을 구분하여 관리할 수 있고, 유출사고 발생 시 신속한 추적이 가능하도록 고려한다.

3.1.2 고객정보취급자

1. 상담원들은 고객정보취급자이며 그 수가 매우 많다. 따라서 정보누출의 위협요인이 존재한다. 이에 대한 대책으로,

가. 상담원의 업무취급 범위와 권한을 최소단위로 세분화하고 명확하게 구분하여 운영한다. 즉, 취급업무별, 서비스 별, 상담그룹 별, 담당고객 군별 등으로 분류하고, 각각의 업무 영역별로 개인정보 취급범위 등을 명확하게 정한다.

나. 상담원들의 고객정보조회를 위한 고객정보에의 접근은 상담 중에만 가능하도록 한다.

다. 상담원은 담당업무에 해당하는 서비스와 그에 대한 고객정보만을 취급하도록 한다.

라. 개인정보취급자의 실명을 확인할 수 있는 ID를 사용토록 한다.

마. 고객의 개인정보 접근 및 조회 자를 바로 알 수 있도록 한다.

바. 상담중인 고객과 무관한 고객관련 정보에 접근하거나 접근을 시도하는 횟수를 확인할 수 있도록 한다.

사. 고객 개인정보의 변경이나 수정, 주요고객 또는 다량의 고객정보 접근이 필요한 경우에는 직상급자 등의 승인을 받도록 한다. 또한 승인 내역에 대한 관리를 할 수 있는 방안을 강구한다.

2. 컨택센터 종사원의 퇴직, 이직 등이 잦아 개인정보취급자의 개인정보유출 방지를 위한 관리 통제가 어렵다. 이에 대한 대책으로는, 직원의 퇴사 시 비밀유지서약서 환기와 함께 고객정보 접근내역 등의 분석내용을 알려 준다.

3.1.3 컨택센터 시스템

대부분의 컨택센터는 많은 수의 개인정보취급자에 대하여 시스템적인 통제 방안 등이 고려되지 않았거나 매우 미흡하다. 이에 대한 시스템적인 정보보호 방안을 마련하기위하여 다음과 같은 사항들을 반영한다.

1. 개인정보취급자들의 고객정보 접근내역 등을 알 수 있도록 접근기록용 DB, Pop-up DB 등을 구축하고 시스템의 업무처리 절차 등을 보강하거나 보완한다.

2. ID별로 그 권한 범위내의 정보자산 접근 내역을 관리할 수 있도록 한다.

3. 시스템 로그뿐만 아니라 개인정보취급자의 고객정보접근 로그 등을 포함하여 관리한다.

4. 고객정보접근에 대한 체계적인 분석 및 관리가 될 수 있도록 한다. 그 방안은 다음과 같다.

가. 각 ID별로 평상시의 로그온 동안의 고객정보 등 주요 정보자산에의 접근을 분석한다.

나. 인가자의 권한별, 해당서비스별 등의 주요정보자산 접근내역을 분석할 수 있고, 통계자료로도 제공할 수 있도록 한다.

다. ID별 고객정보 검색기록, 접속시간, 고객정보 접근 건수 등의 자료 수집, 저장, 분석, 관리가 가능하도록 한다.

라. 평상시의 통계자료와 업무 변경, 퇴직 전의 일정기간 동안의 통계자료를 비교 분석하여 급격히 많아지는 경우 등을 관리한다.

3.2 컨택센터 개인정보보호 제안 모델

제3.1절에서 제안하는 "컨택센터 개인정보 보호 방안"에 대하여 효용성 있는 정보보호 모델 체계를 갖추기 위하여, ISMS의 개인정보보호 관련 사항들을 분석·검토하여 그 형식을 따르는 "컨택센터의 고객 개인정보 보호 모델"을 수립하였다. 본 논문에서는 KISA-ISMS의 15개 통제분야 120개 통제항목[7]에 대하여 분석·검토하였다. 그 제안모델의 요약내용은 [표 1]과 같다.

제안모델은 "정보보호정책", "인적보안", "접근통제", "운영관리", "검토, 모니터링 및 감사" 등 5개 통제분야에 대하여 6개 통제목적, 11개 통제사항 및 그 내용으로 구성되었다. KISA-ISMS의 대상분야 중 통제목적이나 통제사항이 없는 항목은 신설하거나 보강하여 적용하였다. 5개 통제분야 중에 "정보보호정책" 및 "인적보안" 분야에 2개 통제목적을 신설하고 해당 통제목적들에 7개 통제사항을 신설하여 적용하였다. "접근통제", "운영관리", "검토, 모니터링 및 감사" 등 3개 분야에 대하여는 3개 통제사항을 신설하여 적용하였으며, "운영관리" 분야의 "로그관리" 통제사항의 내용을 컨택센터의 특성에 적합한 내용으로 보완하였다.

3.3 제안모델의 특성

제안모델은 컨택센터의 특성을 반영하여 고객의 개인정보보호를 위한 실행방안 및 방법 등을 제시하였으며, 일반적이며 모든 분야에 공통적으로 적용되는 사항들은 포함하지 않았다.

〔표 1〕 컨택센터의 고객 개인정보 보호 모델 요약

통제분야	항목수	통제목적	통제사항	통제내용 요약
정보보호정책	4	주요정보자산 취급	개인정보취급자관리	업무취급권한의 세분화 및 최소화
			고객정보취급관리	고객정보조회자를 알 수 있게 한다, 등
			개인정보유출예방	개인정보취급 한계치 설정 운영 등
			개인정보접근관리	고객정보접근시마다 그 내역을 기록, 관리
인적보안	3	내부정보유출예방활동	직원퇴직관리	일정기간이상 개인정보취급기록 보관, 관리
			로열티향상대책	정보보호 기업문화 형성 등의 향상대책 강구
			불만해소대책	수시로 직원들의 불만해소 방안 강구, 시행
접근통제	1	접근통제영역	인가자의접근통제	고객정보취급자별 접근통제 방법 세분화 등
운영관리	2	시스템운영	로그관리	고객정보취급자별 로그도 같이 관리한다,
		매체, 문서관리	매체제한 및 통제	상담용 단말장치는 상담목적으로만 사용
검토, 모니터링, 감사	1	모니터링	모니터링결과 활용	개인정보 접근에 대한 분석결과의 공지
5개 분야	11	6개 통제목적 11개 통제사항		

3.3.1 제안모델의 특징

1. 내부정보보호 강화 방안 및 개인정보 유출 예방 측면

제안모델에서는, 다수의 인가자에 대한 내부정보보호 강화를 위하여, 고객정보 접근에 대한 통계 자료 등에 근거한 과학적인 개인정보 유출 예방대책을 강구할 수 있도록 하였다. 따라서 교육에 의존하는 기존방식에 비하여 체계적이고 실질적으로 고객의 개인정보 유출 등을 방지하거나 예방하는 효과가 클 것으로 생각한다.

2. 개인정보취급자의 보안관리 측면

제안모델에서는 고객정보취급자의 고객개인정보 접근기록 등의 자료를 분석하여 관리할 수 있으며, 필요시에는 주의나 경고 조치 등을 취할 수 있다. 이러한 데이터에 근거한 분석 및 통계 등은 고객정보유출 징후나 가능성을 알기가 쉬워지므로 사전적인 예방조치를 취할 수 있다. 또한 Pop-Up 화면 등의 공지활동에 실질적이고 현실감 있는 정보의 활용으로 고객 개인정보보호 효과를 높일 수 있다.

3. 로그 기록 관리 및 개인정보 취급현황 관리 측면

평상시에 상담활동의 로그기록이나 고객의 개인정보 접근 형태, 일일 처리 건수 등의 취급 현황 등을 분석하여 급격한 변화 발생 시에는 해당상담원에게 알려줌으로서 개인정보 누출 가능성을 최소화하거나 예방가능성을 높일 수 있도록 하였다. 이러한 개인정보취급 통계자료 수집 등에 대한 활동이 상담원 등에게 알려지게 되면, 컨택센터의 특성상 정보파급효과가 커서 예방효과 또한 클 것이다.

4. 침해사고 발생 시 추적성 확보 측면

각 상담원 등 ID별로 고객정보 취급이나 고객정보 접근 등에 대한 기록을 함으로서, 고객정보취급자들의 고객정보 접근 및 수집 동향과 평상시와 다른 특이점 등을 파악할 수 있으므로 침해사고 발생 시에는 신속한 대처가 가능하다.

5. 퇴직 및 이직 자 관리 측면

평상시의 통계자료와 업무 변경이나 퇴직 전의 일정기간 동안의 통계자료를 비교 분석하여 급격히 많아지는 경우가 있는지 등을 관리하며, 직원의 퇴직 또는 이직 시에는 비밀유지 서약서 환기와 함께 고객정보 Access, 로그 등의 분석내용을 알려 줌으로서 정보누출의 예방효과를 높일 수 있다.

6. 상담단말장치에서의 개인정보 누출 방지 측면

컨택센터에서의 상담용 단말장치에서는 고객의 개인정보 검색이 가능하므로, 고객의 개인정보 검색결과

를 USB 등의 매체로 복사하거나 인쇄하는 기능을 차단함으로서 개인정보 유출 가능성을 줄일 수 있다.

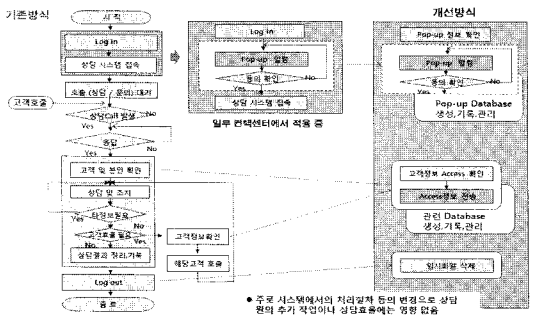
7. 제안모델의 적용 및 응용 측면

제안모델은 ISMS의 형식을 따르고 있어 컨택센터에서 ISMS를 도입할 때에 개인정보보호에 관련된 통제분야에 세부적인 실행방안으로 적용할 수 있다.

3.3.2 제안모델의 개선사항

대부분의 컨택센터는 고객정보취급자인 상담원들의 보안등급이 해당서비스시스템 등의 접속허용자 수준이며, 해당시스템의 일반적인 보안정책을 적용하고 있는 실정이다. 따라서 주요정보자산인 고객의 개인정보를 취급하는 고객정보취급자 등의 시스템접근권한이나 고객정보취급 사항들을 시스템에서 체계적으로 관리할 수 있는 방안을 모색하였다. 그 방법으로 고객정보 접근사항을 기록하는 접근데이터베이스와 고객접근기록 분석결과나 특이사항을 기록 관리하는 Pop-up 데이터베이스를 구축하도록 하였다.

또한 고객정보취급자의 고객정보 접근사항을 신속하고 정확하게 알 수 있도록, 고객정보보호에 관련한 정책, 자료수집 및 활용방안, 시스템의 처리사항, 운영방법 등을 제시하였다. 컨택센터의 상담업무처리나 시스템에서의 처리사항에 대하여 기존방식과 달라진 개선사항을 개략적으로 나타내면 [그림 2]와 같다.



[그림 2] 제안모델의 주요 개선사항

1. 컨택센터의 일반적인 업무절차에서, 상담원들은 업무를 시작하기위하여 상담시스템(각 서비스시스템 또는 고객정보제공 시스템 등)에 접속하게 되는데, 접속과정에 Pop-up 정보를 확인하고 동의하는 절차를 추가하였다. 각 상담원의 단말장치에 Pop-up 화면으로 뿌려주는 정보내용은 고객정보준수 사항 및 고객정보접근분석 내용이 될 수 있으며, 정보보호정책에 따라 변경이 가능하다. 제안모델의 시스템적인 처리나 변동사항은 Pop-up 정보의 데이터베이스를 생성하고 필요한 내용들을 기록하여 필요시 해당상담원에게 Pop-up 화면이나 메일 등을 통하여 알릴 수 있도록 한 점이다.

2. 상담업무 중에는 고객정보 확인을 위하여 고객정보데이터베이스에 접속할 때마다 조회자의 ID와 접속시간, 조회대상 등의 사항을 접근정보데이터베이스에 기록하고, 해당서비스시스템이나 상담시스템에 접근정보를 전송한다. 이 과정은 고객정보접근 및 접속시마다 이루어지며 상담업무가 종료될 때까지 시스템에서 반복하여 처리한다.

3. 상담업무를 종료하고 로그아웃을 하는 경우에는 시스템에서 상담용 단말장치 등에 존재하는 고객정보조회 등에 관련한 임시파일을 삭제하도록 한다.

3.3.3 제안모델의 장단점

1. 장점

가. 고객정보 접근에 대한 통계데이터 등을 활용하여 다수의 고객정보취급자에 대한 효과적인 내부정보보호 강화 및 실질적인 개인정보 유출 예방 등의 효과를 높일 수 있다.

나. 침해사고 징후 및 가능성을 알아낼 수 있어 사전에 조치가 가능하다.

다. 침해사고 발생 시에도 특이점 등의 추적이나 신속한 대응이 가능하다.

라. 퇴직 및 이직 자의 고객정보취급에 대한 데이터를 적정하게 활용함으로서 정보누출의 예방효과를 높일 수 있다.

2. 단점

제안모델에서 제시하는 방안들을 적용할 수 있는 사전 조치사항으로, 서비스시스템이나 데이터베이스 시스템의 DB 생성 및 운영관리 방안의 적용이 필요하다. 또한 정보보호정책의 적용·운영을 위한 시스템의 업무절차 변경 등의 조치가 필요하다.

IV. 결 론

컨택센터에서의 개인정보보호를 위한 구체적인 방안과 대책을 도출하기 위하여 개인정보보호에 관련된 기술적, 정책적 연구사항을 비롯하여 관련 법률 규정, 개인정보 침해사례 등을 분석·검토하였다. 또한 컨택센터의 특성분석과 위협요인 및 취약점을 분석하고, 고객의 개인정보를 효과적으로 보호할 수 있는 방안들을 검토하였다. 그리하여 컨택센터에서의 고객의 개인정보 보호를 위한 시스템적인 해결방안을 강구하고, 고객의 개인정보 누출 사고 발생 시에도 신속하게 대응 가능한 방안 등을 모색하여 컨택센터 특성에 맞는 "컨택센터 개인정보 보호 방안"을 수립하였다. 그리고 "컨택센터 개인정보 보호 방안"에 대하여, ISMS형식을 따르는 "컨택센터의 고객 개인정보 보호 모델"을 수립하여 제안하였다.

따라서 컨택센터에서 ISMS를 도입하거나 컨택센터ISMS 인증 시 등에, 개인정보보호에 관련된 통제사항들의 세부적인 지침이나 구체적인 실행방법으로 본 논문의 제안모델을 활용할 수 있을 것이다.

제안모델은 고객의 개인정보가 내부요인에 의해 유출될 가능성을 차단하거나 예방할 수 있는 등, 효과적으로 대응할 수 방안을 제시하였다. 따라서 접근기록 데이터 및 통계자료 등을 활용하여, 체계적이고 과학적인 고객의 개인정보보호 대책방안을 수립하고 실행함으로서 실질적인 효과를 얻을 수 있을 것이다. 제안모델을 적용하면 침해사고 징후 및 가능성을 파악할 수 있어 사전에 조치가 가능하며, 침해사고 발생 시에도 신속한 대응이 가능하다.

본 논문에서는 고객정보를 제공하는 서비스시스템이나 데이터베이스 시스템의 고객정보 수집 등에 대한 일반적이고 기본적인 정보보호대책 등은 다루지 않았다. 향후에는 제안모델을 컨택센터에 효과적으로 적용하는 구현방법과 Pop-up DB, Access DB에 대한 시스템구축이나 개발의 구체적인 방법, 그리고 개인정보접근 통제에 대한 적정한 한계치 설정 등의 세부적인 사항에 대한 추가적인 연구가 필요하다고 본다.

참 고 문 헌

[1] 한국정보보호진흥원, "개인정보보호 관련 법률 및 사례," http://www.kisa.or.kr/개인정보보호 전문교육(06년3차).pdf, pp. 62-66, 2006년 9월.

[2] Chosun.com 뉴스, "'정보 유출' 주범은 내부직원 한달간 고객DB 멋대로 복사," http://news.chosun.com/site/data/html_dir/2008/09/07/2008090700819.html, 2008년 9월.

[3] 고은경, "내부마케팅요인과 이직의도가 미치는 영향에 관한 연구(통신회사 인·아웃바운드 콜센터 중심으로)," 석사학위논문, 동국대학교, 2006년 6월.

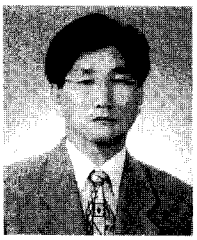
[4] 박응희, "정보기술을 활용한 대고객서비스에서 인적오류의 영향에 관한 탐색적 연구," 석사학위논문, 전남대학교, 2006년 2월.

[5] 이정훈, "CTI Infra," 월간 Contact Journal, 통권(96), pp. 21, 2008년 3월.

[6] 문승주, "중소기업 침해사고 대응팀 SMB -CERT 구축," KISA, pp. 4, 200606CERT구축및운영.pdf.

[7] 정보통신부고시, "정보보호관리체계 인증 심사 기준," pp. 23-40, 2007년 8월.

〈著者紹介〉



권 영 관 (Young-Kwan Kwon) 종신회원
1986년 2월: 국립 경기공업개방대학교 전자공학과 졸업(학사)
1990년 9월: 연세대학교 산업대학원 전자공학과 졸업(석사)
2009년 2월 : 순천향대학교 일반대학원 정보보호학과 졸업(박사)
1982년 1월~2000년 3월: 한국통신 및 KT 부장, 국장
2000년 3월~2005년 4월: KT 중앙데이터통신국장, 인터넷기술담당(상무급)
2005년 4월~2006년 12월: KT Linkus 신사업추진본부장
2007년 1월~ 2009년 1월:카스정보통신 주식회사 사장
2002년 1월~ 2008년 1월: 한국정보통신기술사협회 부회장
2002년 1월~ 현재: 한국인터넷진흥협회 이사
현재: 정보통신기술사, CISSP
〈관심분야〉 네트워크보안, 망관리 및 보안관제, Building Security, Security Service

염 흥 열 (Heung-Youl Youm) 종신회원
1981년 2월: 한양대학교 전자공학과 졸업(학사)
1983년 2월: 한양대학교 대학원 전자공학과 졸업(석사)
1990년 2월: 한양대학교 대학원 전자공학과 졸업(박사)
1982년 12월~1990년 9월: 한국전자통신연구소 선임연구원
1990년 9월~현재: 순천향대학교 공과대학 정보보호학과 정교수
1997년 3월~2000년 3월: 순천향대학교 산업기술연구소 소장
2000년 4월~2006년 2월 순천향대학교 산학연컨소시엄센터 소장
1997년 3월~현재: 한국정보보호학회 총무이사, 학술이사, 교육이사, 총무이사(역), 논문지 편집위원회 위원장(현), 상임부회장(현)
2005년~2008년: ITU-T SG17 Q.9 Rapporteur
2006년 11월~2009년 2월: 정보통신연구진흥원 정보보호전문위원
2009년 - 현재: ITU-T SG17 부의장/SG17 WP2 의장
〈관심분야〉 인터넷보안, USN 보안, IPTV 보안, 홈네트워크 보안, 암호 프로토콜