情 報 保 護 學 會 誌
第18卷 第5號, 2008. 10

컨택센터의 정보보호관리체계 적용에 관한 연구

권 영 관*, 염 흥 열**

요 약

본 논문에서는 고객과 기업 간에 커뮤니케이션이 이루어지는 고객접점인 컨택센터에 대한 정보보호관리체계의 적용방안을 연구하였다. 이를 위하여, 국제 및 국내의 정보보호관리체계 표준을 살펴보고, 컨택센터의 특성을 분석하여 정보보호 대책에 반영할 요구사항을 도출하였다. 따라서 국내의 정보보호관리체계를 토대로 하여, 컨택센터의 특성과 정보보호요구사항을 반영한 컨택센터의 정보보호관리체계 모델을 제안하였다.

Ⅰ. 서 론

풍요로운 생활을 향한 생산 및 서비스분야의 발전으로 기업의 소비자에 대한 서비스 품질향상이 필요하게 되었다. 기업은 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 서비스 품질향상 활동의 주체가 되는 것의 하나가 고객접점인 컨택센터이며, 컨택센터는 고객 상담 및 응대의 역할 뿐만 아니라 기업의 수익 창출원, 기업홍보 등의 전략적 창구로서 그 중요성이 더해 가고 있다. 현재의 컨택센터는 인터넷을 비롯한 여러 디지털 뉴미디어의 발전에 따라 정보기술의 활용이 증대되고 있다.

정보기술의 활용은 우리의 삶의 질을 높이며, 정보화의 향상 발전은 국가경쟁력의 필수적인 요소로 등장하여 모든 산업의 패러다임을 변화시키고 있다. 그러나 지식정보화사회의 진전과 더불어 발생하고 있는 역기능은, 개인이나 단체의 주요 정보자산에 대한 정보보호 필요성과 함께 사회 각 부문별 정보보호대책 수립이 필요하게 되었다. 이러한 정보보호대책 수립의 필요성과 정보화 역기능에 효과적이고 체계적으로 대응하기 위한 정보보호관리체계(ISMS : Information Security Management System)가 국제 및 국내 표준으로 제정되어 권고하고 있어 각 산업분야에서 적용하거나 응용되고 있다. 본 논문에서는 표준으로 권고하고 있는 정보보호관리체계를 컨택센터에 효과적으로 적용할 수 있도록, 정보보호관리체계를 분석하여 컨택센터의 특성을 반영한 ISMS적용방안을 제안하고, 제안모델의 특성을 분석하였다.

1.1 기존 연구현황 분석

컨택센터는 단순전화응대의 콜센터로부터 발전하여 왔으며 컴퓨터와 전화의 통합(CTI : Computer Telephone Integration) 등 통신 및 정보기술의 발전에 따라 다양한 매체와 기술을 활용하고 있다.

컨택센터에 대한 연구 활동은, 컨택센터의 시스템 구축, 설계방안 등에 대한 연구 논문들이 다수 존재하여 효율적인 시스템 구축 및 관련 시스템의 설계방안 등의 방법론을 제시하고 있다. 반면에 컨택센터에서의 정보보안에 대한 연구는, 컨택센터 시스템 구축시의 방화벽 설치 및 시스템 보호 제시 등의 수준으로, 전반적이고 체계적인 정보보호대책으로는 미흡한 실정이다. 예를 들면, 동국대의 선종선[1]은 컨택센터의 운영 효율화를 위한 시스템 구축 방안을, 영남대의 김양규[2]는 CTI체계를 적용한 콜센터 구축방안을 제시하고 있다. 세종대의 임재범[3]은 IPCC(Internet Protocol Contact Center) 기반의 CTI최적화 방안을 제시하면서 컨택센터의 채널

* 카스정보통신주식회사 (ucop@paran.com)
** 순천향대학교 (hyyoum@sch.ac.kr)

이 공중망에 노출 시 등에 네트워크 보안 대책을 강구할 것을 언급하고 있다.

컨택센터에서의 체계적이고 효과적인 정보보호대책으로 ISMS를 도입· 적용하는 방안을 들 수 있다. 정보보호관리체계(ISMS)는 조직의 전반적이고 체계적인 정보보호대책이 가능하며, 국제 표준 및 국내 표준으로 제정되어 여러 분야에 적용되거나 응용되고 있다. ISMS에 관련된 연구로는 대전대의 정현준[4]은 국내 및 외국의 ISMS에 관한 연구를 하였으며, 동국대의 이창호[5]는 BS7799의 ISMS 기반에 정보보호위험관리시스템을 연구하였다. 연세대의 김상호[6]는 BS 7799의 프로세스 성숙도 모델과 ISMS 인증을 활용한 IT보안성 평가에 관한 사항을 연구하는 등, ISMS 구축이나 정보보호 관리방법, 통합보안관리 시스템의 구축 관련 연구 들이 다수 있다. 그러나 컨택센터에 적용할 ISMS에 관한 연구는 찾아 볼 수 없었다.

1.2 연구의 필요성

컨택센터는 단순제품출시에 대한 안내, 상품, A/S (After Service), 교환 반품, 서비스안내 등 산업부문 모든 분야에 확대되고, 전문분야로 확산되어가는 추세이다. 또한 기업의 CRM(Customer Relationship Management), DB(Data Base)마케팅의 중요성 인식으로 고객관련 업무를 취급하는 모든 분야에 컨택센터의 운영이 검토, 추진되고 있다. 컨택센터에서는 고객정보 취급등 기업의 중요 정보자산을 활용하는 업무가 증대되고 있어 정보보안은 필수요건이 되고 있으며, 컨택센터에서도 ISMS 도입의 필요성이 커졌다. 그러나 국내·외 ISMS는 각 산업분야의 조직유형이나 특성에 관계없이 공통적인 통제항목을 제시하고 있다. ISMS의 적용에 있어, 예를 들어 금융업, 제조업, 컨택센터산업 등 각각의 업종별 특성이 존재하는데, 일률적인 기준의 통제항목이나 통제사항을 적용하는 데는 무리가 있다고 본다.

컨택센터에 기존의 ISMS를 그대로 도입하면 미 도입 시보다는 나은 체계의 보안관리 효과가 있겠으나, 컨택센터의 업무특성으로 인한 위협요인 등에 대한 대책이 누락되거나 미흡한 면이 존재할 것이다. 예를 들면, 일반적인 컨택센터에서는 해당서비스 등의 데이터베이스와 연동하여 필요한 정보를 공동 사용하고 있으며, 해당서비스 시스템 등의 정보보호를 신뢰하여 전반적인 정보보호대책은 고려하지 않는 경향이 있다. 또한 컨택센터의 업무는 고객을 중심으로 이루어지며, 컨택센터 구성원의 대부분이 주요정보자산인 고객의 개인정보를 취급하는데, 이는 일반적인 정보보안의 원칙 중의 하나인 "주요정보 취급 등의 보안 취급자는 최소로 한다."에 위배되는 컨택센터의 주요 특성이다. 따라서 컨택센터에서의 정보보호가 효과적으로 이루어지기 위해서는 컨택센터의 조직특성을 반영한 정보보호관리체계의 도입이 필요하다고 생각한다.

Ⅱ. 정보보호관리체계(ISMS : Information Security Management System)

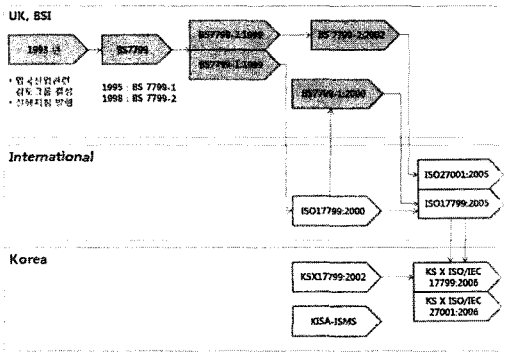
2.1 개요

정보보호관리체계(ISMS)는 조직의 주요 정보자산을 보호하기 위해 정보보호 관리 절차와 과정을 체계적으로 수립하여 지속적으로 관리 · 운영하기 위한 종합적인 체계로, 보호자산에 대한 기밀성 · 무결성 · 가용성을 높이기 위해 조직적 · 관리적 · 운영적 · 기술적 통제를 위해 존재한다. 그리고 이를 위한 조직적이고 체계적인 관리체계 프레임 워크를 가지며 대내외적인 인증제도로 그 표준이 정의 되어있다[7]. 대표적인 ISMS로 정보보호 및 관리에 대한 국제 표준이나 우리나라 표준의 근간이 된 BS7799를 들 수 있다.

2.2 BS 7799

BS 7799는 정보 보안을 위한 영국의 국가표준으로, IT산업만을 대상으로 한 규격은 아니며 정보보안을 위한 모든 조직에서 활용할 수 있도록 만든 규격이다[8]. 이 규격은 정보화의 진전 및 지식사회로의 발전과 정보의 가치가 높아지는 추세에 맞게 규격의 보완 및 개정이 이루어지고 있으며, 정보보호관리체계의 제정 과정은 [그림 1]과 같다.

1993년 1월에 영국에서 산업관련 검토그룹을 결성하여 9월에 실행 지침을 발행하였다. 영국의 BSI는 1995년 2월에 "BS 7799-1"을 발간하였으며 1998년 2월에는 "BS 7799-2"을 발간하였다. 1999년 4월에는 BS 7799-1 및 BS 7799-2를 개정하였고, 2000년 3월에는 BS 7799-1을 ISO 규격으로 채택하여 ISO/IEC 17799로 발간 후 2005년 6월에 개정되었다. BS 7799-2는 2002년 9월에 영국 BSI에서 개정하였으며 2005년 10



〔그림 1〕 ISMS 표준 제정과정

월에 ISO/IEC 27001로 전환 제정 되었다.

2.3 국제 ISMS

ISMS에 대한 국제표준규격은 BS 7799를 근간으로 한 ISO/IEC 17799와 ISO/IEC 27001 두 부분으로 구성되어 있다. 향후의 ISMS 국제표준 개발이나 제정 및 전환은 [표 1]과 같이 진행되고 있다. 2005년 10월에 BS 7799-2에서 전환 제정된 ISO/IEC27001을 시작으로 ISO/IEC 17799 : 2005는 ISO/IEC 27002로 변경되는 등 "ISO/IEC 27001 "family" of standards"의 개발 및 제정을 추진하고 있다.

〔표 1〕 Development of ISO/IEC 27001 "family" of standards

Standard	Description
27000	ISMS fundamentals and vocabulary
27001	Specification(BS7799-2) Issued October 2005
27002	Code of practice for ISM (ISO/IEC 17799 : 2005)
27003	ISMS implementation Guide
27004	Metrics and Measurement
27005	Risk Management
27006	Requirements for the accreditation of bodies providing certification of ISMS

출처 : ICGFM Annual Conference, May2006[9] 및 Standards Australia forum(19July2006)[10] 자료 재구성

2.3.1 ISO/IEC 17799

정보보호관리에 대한 실행 지침(Code of Practice for Information Security Management)이며, 참조 문서로 사용할 수 있다. 조직의 정보보호관리체계를 구현, 관리하는 데에 요구되는 사항을 제공하며, 다양한 조직의 보안표준 및 효과적인 보안관리에 적용되는 공통적인 기준을 제시한다. 현재 사용하고 있는 최상의 정보보호 실행지침(Best Practice)이며, 12개의 조항 중 "범위"와 "용어의 정의" 등 2개 조항과 10개의 관리항목으로 구성되고, 기밀성, 무결성 및 가용성 유지에 초점을 맞추고 있다[11]. 10개 관리항목은 "보안 정책, 보안 조직, 자산의 분류와 통제, 인력 보안, 물리적 환경적 보안, 의사소통과 운영관리, 접근 통제, 시스템 개발과 관리, 사업연속성 관리, 일치성" 이다.

2.3.2 ISO/IEC 27001

정보보호관리체계(ISMS)에 대한 요구사항으로 조직의 ISMS 구축과 운영을 위한 실제적인 기준이며 개별 조직이 필요성에 따라 실행할 수 있는 보안요건을 규정한다.[12] 이 기준은 모든 산업분야에 적용 가능하다. ISO/IEC 27001의 통제항목은 "정보보호정책, 정보보호조직, 자산관리, 인력자원보안, 물리적 및 환경적 보안, 통신 및 운영관리, 접근통제, 정보시스템 구축 개발 및 유지, 보안사고 관리, 사업 연속성 관리, 적법성" 의 11개 도메인이다. BS7799 규격에서는 10개 도메인에 127개 통제항목으로 구성되어 있었으며, 국제표준으로 되면서 11개 도메인에 133개 통제항목으로 변경되었다. 가장 큰 변화는 "보안사고 관리"에 대한 도메인을 추가하여 보안 사고에 대한 관리의 중요성을 강조하고 있다.

2.4 국내 ISMS

우리나라에서는 2002년 7월에 ISO/IEC 17799를 한국산업규격으로 채택하여 KSX 17799를 제정 하였으며, 2006년 12월에 "ISO/IEC 17799 : 2005"에 맞게 개정하여 현재에 이른다. BS 7799-2의 국제 표준인 "ISO/IEC 27001 : 2005"는 2006년 12월에 한국산업규격 "KS X ISO/IEC 27001 : 2006"으로 제정되었다. 우리나라의 정보보호관리체계(ISMS)에 대한 표준규격은, 국제표준을 따른 한국산업규격(KS)과 "정보통신망이용촉진 및 정보보호 등에 관한 법률"에서 정하고 있는 KISA-ISMS가 있다.

- 한국산업규격 KS X ISO/IEC 17799 : 2006 (정보기술-보안기술-정보보안관리를 위한 실무지침) ← ISO/IEC 17799 : 2005
- 한국산업규격 KS X ISO/IEC 27001 : 2006(정보기술-보안기술-정보보안관리시스템-요구사항) ← ISO/IEC 27001 : 2005
- KISA-ISMS ← 정보통신망법 제47조, 정보통신부 고시 제2007-30호

국내 정보보호관리체계인 KISA-ISMS는 2002년5월에 "정보보호관리체계인증심사기준"으로 공표되었으며(정보통신부 고시 제2002-22호), 2007년 8월에 개정되었다(정보통신부고시제2007-30호).

KISA-ISMS는 "정보보호정책 수립", 범위 설정", "위험관리", "구현", "사후관리"의 5단계를 기본으로 한다. 국내 ISMS는 "정보보호관리과정", "문서화", "정보보호대책"으로 구성되어있으며, 정보보호관리과정의 14개 통제사항, 문서화의 3개 통제사항, 정보보호대책에 대한 15개 분야, 120개 통제사항 등 총137개 통제사항의 항목이 있다.[13,14]

2.4.1 정보보호관리체계의 수립

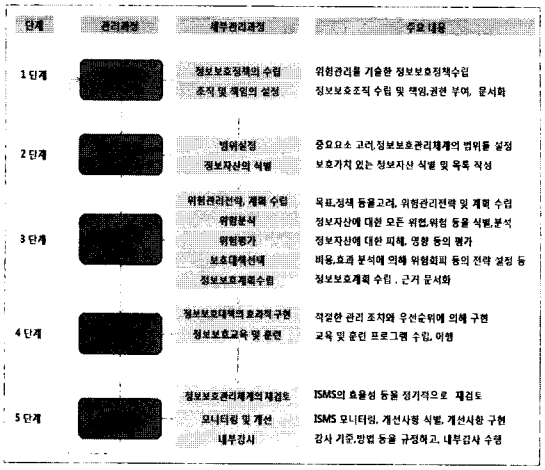
조직의 전반적인 사업활동과 위험환경에서의 정보보호를 위한 정책과 목표를 수립하기 위해서 조직은 문서화된 정보보호관리체계를 개발, 구현, 유지하고 지속적으로 개선한다. 이 문서화된 정보보호관리체계는 "2.4.2 정보보호관리과정"을 통해 수립되어지며, 보호될 자산과 위험관리를 위한 조직의 접근방법, 통제사항, 조직이 요구하는 보증의 정도를 포함한다.

2.4.2 정보보호 관리과정

정보보호관리를 이행하기 위해서 조직은 정보보호정책 및 조직, 범위설정 및 정보자산 식별, 위험관리, 구현, 사후관리 활동으로 구성된 5단계의 논리적이고 체계적인 정보보호관리 프레임워크를 수립하고, 기획 관리한다. 정보보호관리과정은 5단계의 14개 통제사항으로 구성되어 있으며 세부관리과정과 그 주요내용은 [그림 2]와 같다.

2.4.3. 정보보호대책

정보보호대책은 정보보호관리체계를 수립·구축하기



〔그림 2〕 국내 ISMS의 정보보호 관리과정

통제분야(Domain)	주 요 내 용
1. 정보보호정책	정보보호 정책의 체계적인 수립, 검토, 절차 및 심위 검토과정의 적절성 여부
2. 정보보호조직	조직 내 정보보호에 대한 조직체계, 책임 및 역할 활당 여부
3. 외부자 보안	아웃소싱 또는 제3자에 대한 정보보호대책 여부
4. 정부자산 분류	조직의 정부자산 주관 및 책임활당의 적절성 여부 · 조직의 정부자산의 식별한 분류 및 취급 여부
5. 정보보호 교육 및 훈련	업무별 및 정보자산 취급 관리자에 대한 정보보호 교육 프로그램의 수립 및 시행 · 관리 여부
6. 인적 보안	직원의 실수 오용 부주의으로 인한 위험 감소 여부
7. 물리적 보안	물리적 침입으로부터 IT자산을 효과적으로 보호하는지 여부
8. 시스템 개발보안	IT 자산 개발 과정에서의 위험요소에 대한 대책 여부
9. 한호통제	IT자산의 정보보호를 위한 적절한 한호 정책의 수립 및 관리 여부
10. 접근통제	정보 자산에 대한 접근통제(Access Control)
11. 운영 관리	조직 핵심업무의 항상적 유지를 위한 대책 및 점검
12. 전자거래 보안	전자거래 시 조직의 정보보호를 위한 대책 및 점검 여부
13. 보안사고 관리	보안사고 발생시 부구 및 복구체계 여부
14. 점검, 모니터링 및 감사	관계법령 및 조직의 정책에 따른 준수 및 감사 실행 여부
15. 업무연속성 관리	조직 핵심업무의 항상적 유지를 위한 대책 및 점검 여부

출처 : 한국정보보호진흥원, 정보보호대책,p 5, http://isms.kisa.or.kr,2005.6.

〔그림 3〕 정보보호대책의 통제분야(Domain) 요약

위한 세부통제 사항으로서 정보보호정책 등 15개 분야의 120개 통제사항이 있으며, [그림 3]에 15개 통제분야(domain)에 대한 주요내용을 나타내고 있다.

Ⅲ. 컨택센터의 특성 분석

3.1 컨택센터의 정의

컨택센터란 고객을 대상으로 정보안내, 고객문의처리, 고객 불만접수 및 처리 등 고객과의 의사소통을 수행하는 채널로, 초기의 전화응답센터 형태로 출발하여 보통은 콜센터라는 명칭으로 많이 알려져 있다. 최근에는 신규 상품안내, 서비스 안내, 제품 기술지원, 설문조사, 여론조사 등 모든 분야의 고객접촉 채널로 컨택센터

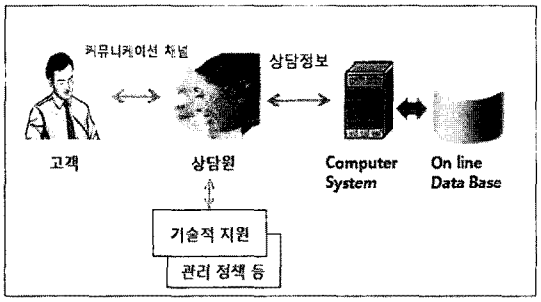
가 활용되고 있는 추세이다.[15]

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

3.2 컨택센터의 서비스

컨택센터서비스는 고객(Customer), 상담원(agents), 시스템(Machine System), 관리정책(Management Policy) 등으로 구성된다. 개략적으로 도식화하면 [그림 4]와 같다. 고객은 상담원과 커뮤니케이션 채널을 통해 연결되고 상담원은 고객의 요구사항을 충족시키기 위해 상담정책 및 관리 정책에 따라 컴퓨터시스템과 데이터베이스를 활용하여 서비스한다.[16]

컨택센터는 종합적인 고객 접점의 기능을 수행하는 고객지원, 기술지원, 고객 상담 등 고객과의 원활한 커뮤니케이션이 핵심적인 역할이라 할 수 있다. 컨택센터의 운영은 언제 어디서나 접촉이 가능한 완전 개방형 고객 상담센터를 지향하고 있으며, 해당 상품이나 기업의 로열티를 증대하고, 관련 상품이나 서비스 등에 고정고객화 내지는 영구적인 고객화에도 중요한 임무를 부여 할 수 있다.

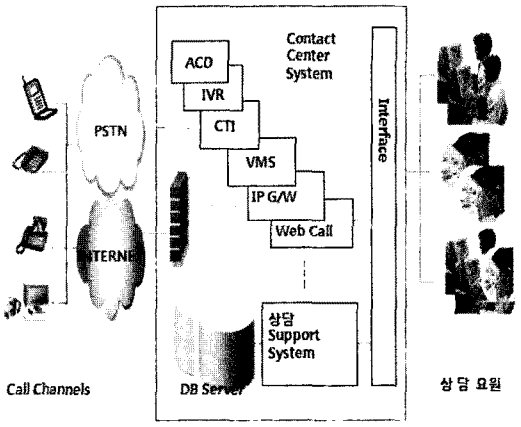


출처 : 박응희[16] 자료 재구성

〔그림 4〕 컨택센터 서비스의 구성요소

3.3 컨택센터의 시스템

컨택센터는 고객을 호출하거나 고객으로 부터의 호출을 적절하게 접속할 수 있는 시스템과 컨택센터요원(상담원 또는 기술지원요원 등), 그리고 고객 상담이나 지원 등을 효과적으로 하기위한 고객 데이터베이스와



〔그림 5〕 컨택센터 구성 계통도 예시

상담내역기록이나 통계 등을 지원하는 시스템 등으로 구성 된다.

컨택센터에 적용·운영되는 대표적인 기술 및 기능은, 컴퓨터전화 통합(CTI : Computer Telephone Integration), 음성자동응답(IVR : Interactive Voice Response), 번호자동인식(ANI : Automatic Number Identification), 인터넷전화(VoIP : Voice over Internet Protocol)기술, 호자동분배(ACD : Automatic Call Distribution), 음성인식시스템(VRS : Voice Recognition System), 예측 다이얼링 시스템(PDS : Predictive Dialing System) 등이 있다.

그밖에 화자검증(SVS : Speaker Verification System), TTS(Text To Speech,음성합성), 음성메일(VMS : Voice Mail System), 팩스메일(FMS : Fax Mail Service), 통합메시지(UMS : Unified Message Service), 이메일자동응대솔루션(EMRS : E-Mail Response Management Solution), 채팅 등의 기능이 활용되고 있다.

3.4 컨택센터의 운영

컨택센터의 유형은 업무성격, 조직구성원, 장비구성, 규모, 통합성 유무, 고객지향정도 등에 따라 달라지며 그 운영 형태도 달라질 수 있으며[17], 인바운드(In-bound)/ 아웃바운드(Out-bound) 컨택센터, 내부공급(Insourcing 또는 In-house)/ 아웃소싱(Outsourcing)형 컨택센터 등으로 나눌 수 있다, 최근에는 아웃소싱형태의 컨택센터가 증가하고 있는 추세이다. 컨택센터의 운영형태나 운영방법 등의 체계도 수행업무, 수행목적 및 비즈니스형태에 따라 다르다.

일반적으로 고객들은 다양한 콜 채널을 통하여 컨택센터에 접속하고 상담원은 고객의 문의사항 등에 대한 상담을 하게 되는데, 고객에 대한 상담이나 서비스를 향상시키기 위해 자체 시스템의 커뮤니케이션 스크립터 및 CRM 등의 관련시스템에서 고객 관련 정보를 검색하여 상담에 응하게 된다. 이때 관련시스템의 고객 상담 관련 정보들이 체계적으로 정비되고 관리되어 있으면 상담의 질을 높일 수 있으며 고객만족을 이끌어 낼 수 있다. 고객이 이용하는 서비스 등의 관련 정보에 대한 데이터베이스 시스템은 컨택센터와 같이 구축되거나, 개별 서비스 시스템의 DB 또는 각종 서비스의 통합 DB형태로 존재하기도 한다. 일반적으로 소규모인 경우는 서비스 시스템에 컨택센터의 기능을 갖추기도 하나, 대부분의 경우는 해당 서비스 시스템의 고객관련 정보를 컨택센터와 공유하도록 구축 운영한다.

3.5 컨택센터의 특성 및 분석

컨택센터는 사회적인 여건과 산업분야, 수행업무, 규모, 운영형태 등에 따라 그 특성이 달라질 수 있으며, 정보보호에 관련된 주요특징을 살펴보면 다음과 같다.

1) 고객 접촉채널의 다양화 및 통합화
고객의 편의성과 서비스 향상을 위하여 고객과의 모든 컨택포인트(전화, Web-Call, e-Mail, FAX, Mobile 등)를 통합한 종합적인 컨택센터 추세이며 고객접촉채널의 다양성과 편리성, 용이성을 추구하고 있다. 따라서 다양한 접촉채널에 대한 고객정보 등이 필요하다.

2) 고객관계개선 업무의 중심역할
컨택센터는 고객과 기업 간의 관계개선으로 고정고객을 확보하고, 고객의 다양한 니즈를 충족시키는 등의 마케팅성과를 창출할 수 있다.

3) 고객 개인정보 취급이 필수적이다
컨택센터는 최 일선에서 고객과의 컨택채널로서 고객에 관한 정보를 상세하고 효과적으로 활용함으로서 고객에 대한 서비스의 질을 더욱 향상시킬 수 있다.

4) 최근에는 컨택센터의 적용범위가 확대되어 가고 있으며, 전문성 확보를 위한 아웃소싱이 증가하는 추세이다. 반면에 컨택센터 요원(상담원)들에 대한 보수, 처우 등이 낮고, 회사에 대한 로열티(Loyalty)도 매우 낮으며, 이직률은 높은 실정이다. 그리고 상담인력이 계약직이거나 비정규직인 경우도 상당부분 존재하고 있다.

컨택센터는, 그 업무특성상 중요정보자산인 고객의 개인정보를 취급하며 그 취급자가 매우 많다. 즉 수십명에서 수백명, 천명이상의 컨택센터에서도 그 구성원의 대부분이 중요정보 취급자이므로 타 산업에 비하여 정보유출 가능성 및 취약성이 크다고 할 수 있다. 컨택센터는 일반적인 정보보안의 원칙인 "인가자의 수를 최소화 한다"에 배치되는 업무특성이 있다. 따라서 업무 특성이나 업무내용 등에 따라 정보자산 접근 및 취급 권한, 관리 등에 보다 세부적인 방안이 강구되어야 할 필요가 있다.

Ⅳ. 컨택센터의 정보보호관리체계 적용

KISA-ISMS는 국제 표준 등을 참고하여 국내의 환경에 맞게 제정된 정보보호관리체계로서, "정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제 47조와 정통부 고시 제2002-22호(2002년5월) 및 정보통신부 고시 제2007-30호(2007년8월)에서 정보보호관리체계와 인증 심사기준 등을 정하고 있다. 따라서 컨택센터에서의 정보보호관리체계 적용은 국내의 ISMS를 기준으로 하여 적용 분석하도록 한다. ISMS는 전 산업분야에서 적용 가능한 규격으로 대부분의 항목들은 공통적으로 적용가능하며 제3장에서 살펴본 컨택센터의 특성을 고려하여 보강되어야 할 사항에 대하여 중점적으로 분석하고 적용방안을 도출하고자 한다. 그리고 도출된 고려사항을 반영한 컨택센터 ISMS 모델을 제안하고 그 특성을 살펴본다.

4.1 컨택센터 ISMS의 고려사항

컨택센터의 주요 구성요소는 고객, 상담원, 시스템 설비 등이며 컨택센터 서비스는 고객 중심으로 이루어지고 있으므로 고객관련 정보에 대한 보안 대책이 강구되어야 한다. 또한 고객접촉 채널이 일반전화, 이동전화, 인터넷전화, e-mail 등으로 다양하므로 각 채널들이나 통신매체에 대한 보안을 고려한다. 일반적으로 컨택

센터의 시스템 설비는 상담효율성, 고객서비스 품질향상, 상담능률 향상 등에 주 기능을 부여하고 있으며, 고객정보의 수집, 분류, 분석, 관리 등을 각각의 서비스 시스템 또는 통합DB시스템에서 관장하고 있다. 따라서 중요정보자산에 대하여 해당 시스템에서 보안대책을 강구 하고 있는 경우가 많이 있어 컨택센터에서는 보안대책이 소홀할 수 있으나, 컨택센터에서는 해당 서비스나 고객관련 정보 등을 공통으로 이용할 수 있으므로 이에 대한 대책도 강구되어야 한다.

제3장의 컨택센터 특성분석 내용을 토대로 한 컨택센터의 주요 고려사항은 다음과 같다.

1) 다양한 고객접촉 채널이나 무 중단서비스 시스템 등에 대한 보안을 위하여 시스템 개발보안이나 물리적 보안, 운영관리 등의 사항이 고려되어야 한다.

2) CRM 시스템이나 고객정보 DB 등에 대한 접근통제, 암호통제, 운영관리 등이 고려되어야 한다.

3) 많은 인력을 운영하고 있는 컨택센터는 종사원의 퇴직 등으로 인한 변동과 개별업무능력의 격차가 큰 편이므로, 인적보안, 접근 및 권한 통제, 운영관리, 모니터링 등의 사항이 고려되어야 한다.
   - 컨택센터 구성원의 대부분을 차지하는 상담원은 계약직 또는 비정규직 비율이 높고, 이직 율이 높으며, 회사에 대한 로열티가 낮은 등의 특성이 있어 구체적인 인적보안, 보안 교육 등이 필요하다. 컨택센터의 상담원은 고객관련 정보를 검색하거나 변경 등의 취급할 수 있어야 하므로 권한관리 및 접근통제정책이나 문서관리, 매체관리에 대한 대책방안 등이 통제사항에 반영되어야 한다.

4) 컨택센터의 아웃소싱 운영에 대한 보안 대책 및 관리가 필요하다.
   - 최근의 컨택센터 운영형태는 아웃소싱 방식이 전 산업분야에서 활발하게 진행되고 있으며 증가 추세에 있다. 인력의 아웃소싱뿐만 아니라 센터운영의 아웃소싱도 활발하게 이루어지고 있으며, 취급하는 업무도 다양해지고 있다.

5) 많은 인력이 주요정보자산에의 접근권한을 가진 인가자이므로 세부적인 내부정보 유출 방지대책을 고려하여야 한다.
   - 컨택센터는 타 산업분야에 비하여 주요정보자산에 대한 접근권한을 가진 인가자가 매우 많은 편이며, 종사원이 많은 대규모의 컨택센터는 소규모 컨택센터에 비해 정보누출에 대한 위협요인이 그만큼 높다고 볼 수 있다. 또한 퇴직이나 타 컨택센터로의 이직, 재입사도 빈번하게 일어나고 있으므로 내부정보 누출 가능성이 큰 취약점을 갖고 있다. 따라서 인력 채용 시부터 퇴직 후 까지 인력관리, 취급업무에 대한 비밀유지 등 인적보안과 모니터링 방안 등을 고려하여야 한다.

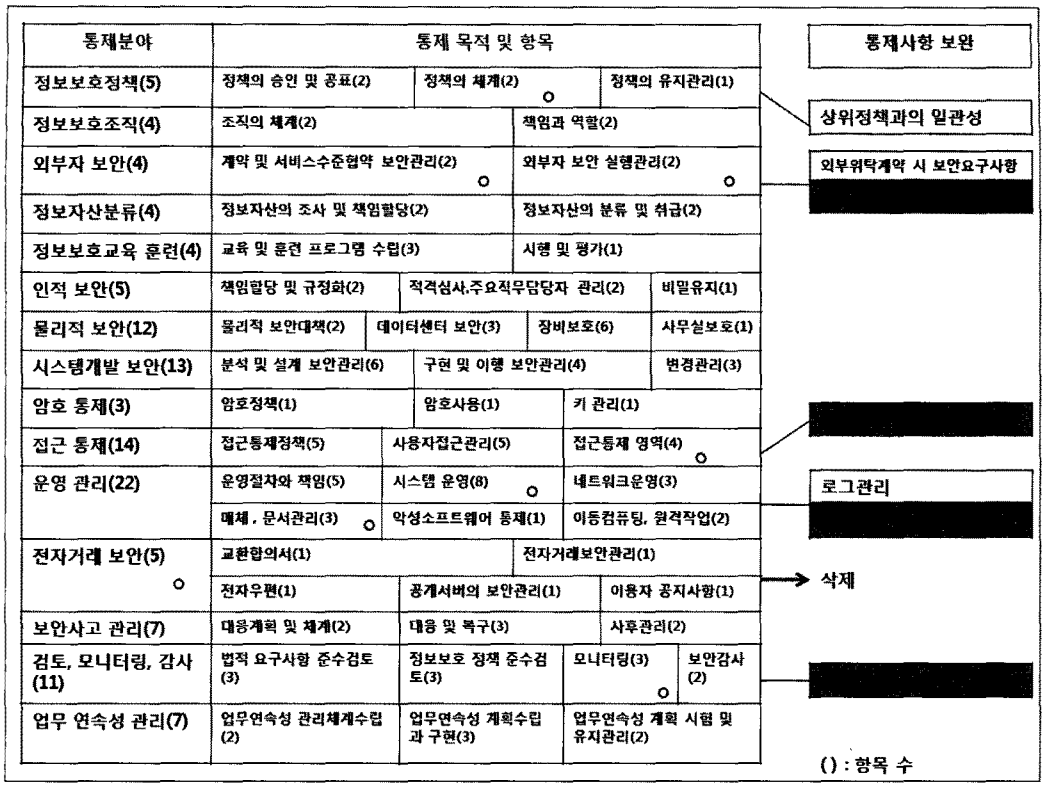
6) 정보보호는 예방이 가장 좋은 방법이며 효과적인 대책이 될 수 있으므로, 접근권한 인가자인 상담원에 대하여 지속적인 교육과 주요정보자산의 접근과 검색 등의 활용 현황을 주지시키는 등의 예방대책 수립을 고려한다.
   - 상담원의 업무개시는 보통 상담시스템에 로그온 하는 시점부터 시작되며, 로그오프 시에 업무가 종료되므로 로그관리가 중요하다. 또한 타 서비스시스템이나 해당시스템에의 엑세스가 필요하게 되는 경우가 많으므로, 접근권한의 세분화가 필요하며 이에 대한 이행상태, 권한 이외의 접근시도 등에 대한 분석을 포함한 로그관리를 고려하여야 한다.

4.2 컨택센터의 ISMS 적용 분석

제3장과 제4.1절에서 살펴본 바와 같이 컨택센터의 특성이나 주요 고려사항을 반영하기 위하여, KISA-ISMS의 120개 통제사항에 대하여 적용 가능성을 살펴보았다. 또한 통제사항 등의 보완이나 추가 등이 필요한 통제사항을 분석하였으며 그 상세내용은 [그림 6]과 같다.

4.2.1 정보보호정책 분야 : 5개 통제사항 중 1개 통제사항 보완

정보보호정책 분야는 "정책의 승인 및 공표", "정책의 체계", "정책의 유지관리" 등에 5개 항목으로 구성되어있으며, 그중에 "정책의 체계" 항목 중 "상위정책과의 일관성" 통제사항에, 아웃소싱 형태의 컨택센터



〔그림 6〕 ISMS 통제사항 및 검토, 보완 할 항목

운영사항을 반영하기위하여 "업무를 위탁받아 운영하는 경우는 위탁자의 정보보호정책을 따라야 한다." 라는 통제내용을 추가한다.

4.2.2 외부자 보안 분야 : 4개 통제사항 중 1개 통제사항 보완 및 1개 통제 사항 추가

외부자 보안 분야는 "계약 및 서비스 수준협약보안관리"에 2개 항목, "외부자 보안 실행관리"에 2개 항목 등 4개 항목이 있으며, 이들은 업무를 외부에 위탁하는 경우에 대한 사항들이다. 따라서 컨택센터의 아웃소싱 운영에 있어, 위탁 사항뿐만 아니라 업무 수탁에 대한 사항들이 반영되어야 한다.

즉, "계약 및 서비스 수준협약보안관리"중의 "외부위탁 계약 시 보안 요구사항"에 대한 통제 사항에 " 외부위탁을 받는 경우는 계약서나 SLA에서 명시하는 보안요구사항을 준수 한다."라는 통제 내용을 추가한다. 또한 "외부자 보안 실행관리"에 "외부수탁 보안관리" 항목과 "외부수탁 업체는 계약서 및 서비스 수준 협약에 명시된 위탁자의 보안요구사항 점검 및 감사 등에 응하고, 외부자 보안 실행관리 정책 및 방침을 따른다."라는 통제 내용을 추가한다.

4.2.3 접근통제 분야 : 14개 통제사항에 1개 통제사항 추가

"접근통제"분야는 "접근통제정책", "사용자접근관리", "접근통제영역" 등에 14개 항목이 있으며, "접근통제 영역"에 "인가자 접근"항목을 추가한다. 컨택센터의 상담원은 상품구매정보, 서비스가입정보 등의 주요정보자산에 대한 검색 등이 가능한 권한을 가진 인가자이며, 컨택센터의 규모가 커짐에 따라 인가자의 규모도 커지게 되므로 다수의 인가자에 대한 권한관리나 접근통제가 고려되어야 한다. 컨택센터는 구성원 대부분이 주요정보자산에 접근할 수 있는 인가자이며, 인가자가 비인가자 보다 많아 내부정보 유출 가능성이 크다고 볼 수 있다. 그러므로 컨택센에서의 접근통제는 비인가자에 대한 접근통제 뿐만 아니라 인가자에 대한 접근통제가 구체적으로 이루어 져야 한다고 생각한다. 즉 인가자의 권한별, 해당 서비스별, 서비스건별 고객정보접속 등

의 주요정보자산 접근내역을 분석할 수 있고, 인가자의 접근 권한이나 범위를 세분화하여 통제할 수 있어야 할 것이다.

따라서 "접근통제영역"의 "인가자의 접근"항목에 대한 통제내용으로 " 다수의 인가자에 대한 권한관리나 접근통제 방법을 세분화하여 반영한다. 접근권한별 정보자산 취급 한계치 등을 설정한다, 내부정보 유출 예방을 위한 세부대책을 수립하여 이행한다."를 추가한다.

4.2.4 운영관리 분야

"운영관리"분야는 "운영절차와 책임", "시스템 운영", "네트워크 운영", "매체 및 문서관리", "악성소프트웨어통제", "이동컴퓨팅 및 원격작업" 등에 22개 항목으로 구성되어있으며, "시스템운영"의 "로그관리" 통제사항을 보완하고, "매체 및 문서관리"에 통제사항으로 "매체 제한 및 통제" 항목을 추가한다.

컨택센터의 주 구성요소인 상담원은, 타 산업분야에 비해 상대적으로 보수, 처우, 회사에 대한 로열티 등이 낮고 계약직이나 비정규직인 경우도 많아 이직률이 높은 편이다. 이들 상담원은 주요정보 자산에 접근을 하는 업무를 취급하므로, 내부정보의 유출 가능성을 예방하는 차원으로 정보보호대책이 마련되는 것이 바람직하다. 운영관리 차원의 내부정보보호 방안으로 로그관리와 매체관리를 들 수 있다.

일반적으로 개인용 컴퓨터를 상담용 단말장치로 사용하고 있는 경우가 많으며, 요즘의 개인용 컴퓨터는 성능이 우수하며 다양한 기능을 갖추고 있다. 따라서 매체관리 방안으로 상담용 단말장치에서의 정보유출 가능성을 미리 차단하기위하여, 상담 시에 활용하기 위해 수집된 정보, 주요정보의 검색 결과 등을 다른 목적으로 이용하기 어렵도록 상담용 단말장치(개인용 컴퓨터)의 USB 포트, 프린트 등의 기능을 차단하거나 제한하도록 조치를 취한다. 즉, 상담용 단말장치는 상담원에게 정보제공 목적으로만 사용토록 한다. 이에 "매체 제한 및 통제"항목을 추가하고, 통제내용은 "주요정보 누출 방지를 위하여 상담용 단말장치의 매체에 대한 한 제한 및 통제 방안을 수립하고 운영하여야 한다."라고 한다.

로그관리 방안으로는 각 Agent(상담원) 별로 평상시의 로그 기록, 로그인과 로그오프 동안의 고객정보 등 주요 정보자산에의 접근을 분석· 관리할 수 있도록 한다. 따라서 "로그관리" 통제사항에 "내부정보 유출 예방을 위한 로그관리 및 분석 방안을 수립하고 운영 한다."라는 내용을 추가·보완한다.

4.2.5 전자거래 보안 분야

전자거래 분야는 5개 통제 항목으로 이루어져 있으며, 전자거래시의 보안대책을 강구하기 위한 통제사항을 제시하고 있다. 일반적으로 컨택센터에서 전자거래가 이루어지는 것은 아니며, 전자거래 시스템에서의 전자거래 전이나 후에 해당서비스에 대한 문의사항이나 처리결과 등에 대한 상담을 컨택센터에서 하게 되므로, 전자거래분야는 포함되지 않아도 될 것으로 판단된다.

4.2.6 검토, 모니터링, 감사 분야

"검토, 모니터링 및 감사"분야는 "법적요구사항준수 검토", 정보보호정책 준수 검토", "모니터링", "보안감사" 등에 11개 항목이 있으며, "모니터링" 부분에 "모니터링 결과 활용"의 통제 사항을 추가한다. 4.2.4. 항에서 제시한 바와 같이 로그관리에 대한 분석결과를 일일 또는 주간 단위 등 주기적으로 해당자들에게 통보해 줌으로서 정보보호 마인드를 상기시키고 내부정보의 유출 예방 효과를 얻을 수 있다고 생각한다. 이러한 운영은 정보 누출 등의 사고 발생 시에는 신속한 증거자료 수집 등에도 유용할 것이다. 또한 "인적보안"분야의 "비밀유지서약서"통제사항에서도 제시하는바와 같이, 직원의 퇴사 시 비밀유지 서약서 환기와 함께 고객정보 Access, 로그 등의 분석내용을 알려 줌으로서 정보누출의 예방효과를 높일 수 있다고 본다.

이러한 맥락에서 "모니터링 결과 활용"의 통제내용을 " 주요정보자산에 대한 접근 등에 대한 모니터링 결과를 내부 정보유출 예방 등에 활용할 수 있도록 분석하여 당사자 등에게 제공할 수 있다."라고 한다.

4.3 컨택센터 ISMS 모델 제안

컨택센터 ISMS 모델은 KISA-ISMS를 기반으로 하여 컨택센터의 특성을 반영하여 120개 통제사항에 대하여 적용방안을 분석·적용하였다. 제4.1절의 고려사항과 제4.2절의 ISMS 적용 분석을 살펴본바와 같이 정보보호정책 등 3개 통제 분야에 대하여, 3개 통제 사항의 내용에 컨택센터 관련 사항을 추가하여 보완 하였다.

통제분야	항목수	통제 목적 및 항목			( ) : 항목 수
정보보호정책	5	정책의 승인 및 공표(2)	정책의 체계(2)	정책의 유지관리(1)	
정보보호조직	4	조직의 체계(2)	책임과 역할(2)		
외부자 보안	5	계약 및 서비스수준협약 보안관리(2)	외부자 보안 실행관리(3)		
정보자산분류	4	정보자산의 조사 및 책임할당(2)	정보자산의 분류 및 취급(2)		
정보보호 교육 · 훈련	4	교육 및 훈련 프로그램 수립(3)	시행 및 평가(1)		
인적 보안	5	책임할당 및 규정화(2)	적격심사,주요직무담당자 관리(2)	비밀유지(1)	
물리적 보안	12	물리적 보안대책(2)	데이터센터 보안(3)	장비보호(6)	사무실보호(1)
시스템개발 보안	13	분석 및 설계 보안관리(6)	구현 및 이행 보안관리(4)	변경관리(3)	
암호 통제	3	암호정책(1)	암호사용(1)	키 관리(1)	
접근 통제	15	접근통제정책(5)	사용자접근관리(5)	접근통제 영역(5)	
운영 관리	23	운영절차와 책임(5)	시스템 운영(8)	네트워크운영(3)	
		매체 · 문서관리(4)	악성소프트웨어 통제(1)	이동컴퓨팅, 원격작업(2)	
보안사고 관리	7	대응계획 및 체계(2)	대응 및 복구(3)	사후관리(2)	
검토, 모니터링, 감사	12	법적 요구사항 준수검토(3)	정보보호정책 준수검토(3)	모니터링(4)	보안감사(2)
업무 연속성 관리	7	업무연속성 관리체계 수립(2)	업무연속성 계획수립 과 구현(3)	업무연속성 계획 시험 및 유지관리(2)	

〔그림 7〕 컨택센터의 ISMS 모델

또한 "외부자 보안", "접근통제", "운영관리", "검토, 모니터링 및 감사" 등 4개의 통제 분야에 4개의 통제사항 신설 및 통제내용 추가 하였으며, "전자거래 보안" 분야 5개 통제사항을 삭제 하였다. 따라서 KISA-ISMS의 "정보보호대책" 120개 통제사항을 119개 통제사항으로 수정한, [그림 7]의 ISMS 모델을 컨택센터의 ISMS모델로 제안한다. 제안모델의 세부 수정사항은 [표 2]와 같다.

4.4 제안 모델의 특성 및 비교 분석

기존의 ISMS는 모든 산업분야에서 정보보호를 체계적이고 종합적으로 적용할 수 있는 정보보호관리체계이며, 각 산업분야 별 공통적인 부분들이 반영되어 있다.

제안한 ISMS 모델은 공통적인 부분은 기존의 방식을 따르고, 컨택센터의 특성 및 반영이 필요한 통제 분야나 통제사항 및 통제 내용을 추가하거나 보완하는 방안을 제시하였다. 이 논문에서 제안한 컨택센터 ISMS는 컨택센터의 기술 등의 발전추세와 운영방식, 확장 및 확대 추세를 맞추었으며 다음과 같은 특징이 있다.

1) 컨택센터의 아웃소싱 및 대형화 추세에 따른 보안관리 측면
   - 아웃소싱에 의한 업무 위탁의 경우에, 기존체계에서는 위탁자에 대한 정보보호 정책이나 관리방안 등에 대한 사항을 제시하고 있으나, 수탁자에 대한 사항은 누락되어 있다. 따라서 제안모델에는 수탁자에 대한 정보보호정책 사항, 보안요구사항의 준수 내용 등을 제시하였다.

2) 일반적으로 대부분의 정보보호대책에서는 주요정보자산이나 비밀 또는 보안 취급자를 최소한으로 제한하도록 제시하고 있다. 그러나 컨택센터는 주요정보자산에 대한 접근권한을 가진 인가자가 전체구성원의 대부분을 차지하고 있으므로 제안모델에서는 내부정보보호 조치 측면을 강화하는데 초점을 맞추었다.

〔표 2〕 제안모델의 통제 분야 및 통제사항의 보완 내역

	통제분야	통제목적	통제사항	주요 통제내용
1	정보보호 정책	정책의 체계	상위 정책과의 일관성	정보보호정책은 사업목표 및 정보기술정책과 일관성을 유지하여야 한다. 업무를 위탁받아 운영하는 경우에는 위탁자의 정보보호정책을 따라야 한다.
3	외부자 보안	계약 및 서비스 수준협약 보안관리	위부위탁 계약 시 보안 요구사항	업무를 외부위탁 하는 경우, 정보시스템, 네트워크, 인력 및 사무환경 등을 관리 · 통제하기 위한 보안요구사항을 계약서상에 명시하고 요구사항을 서비스수준협약(SLA : Service Level Agreement)에 반영한다. 업무를 위탁 받는 경우는 계약서나 SLA에서 명시하는 보안요구사항을 준수 한다.
		외부자 보안 실행관리	외부수탁 보안관리	외부수탁 업체는 계약서 및 서비스 수준 협약에 명시된 위탁자의 보안요구사항 점검 및 감사 등에 응하고 외부자 보안 실행관리 정책 및 방침을 따른다.
10	접근통제	접근통제 영역	인가자의 접근	다수의 인가자에 대한 권한관리나 접근통제 방법을 세분화하여 반영한다. 접근권한별 정보자산 취급 한계치 등을 설정한다, 내부정보 유출 예방을 위한 세부대책을 수립하여 이행한다.
11	운영관리	시스템 운영	로그관리	시스템 운영의 확인이나 사고조사를 위해 활동에 대한 기록을 남기고 주기적으로 검토하여야 한다. 내부정보 유출 예방을 위한 로그관리 및 분석 방안을 수립하고 운영 한다.
		매체 및 문서관리	매체 제한 및 통제	주요정보 누출 방지를 위하여 상담용 단말장치의 매체에 대한 한 제한 및 통제 방안을 수립하고 운영하여야 한다.
12	전자거래보안	삭제		삭 제
14	검토, 모니터링 및 감사	모니터링	모니터링 결과 활용	주요정보자산에 대한 접근 등에 대한 모니터링 결과를 내부 정보유출 예방 등에 활용할 수 있도록 분석하여 당사자 등에게 제공할 수 있다.

3) 컨택센터의 구성원은 상담원이 대부분을 차지하고 있으며, 컨택센터의 집중화, 통합화 등으로 수백 명에서 천 명이상의 상담원을 운영하는 컨택센터들이 많아지고 있다.
따라서 상담원들의 마인드 고취 및 무의식적인 정보누출 가능성을 예방하고자 하는 측면을 고려하여, 평상시에 로그기록이나 주요 정보 취급 현황 등을 해당상담원에게 알려 줌으로서 누출 가능성을 최소화하거나 주요정보 누출 예방 가능성을 높일 수 있도록 하였다.

4.4.1 기존방식과의 비교분석

1) 기존의 ISMS는 15개 통제분야의 120개 통제 사항으로 구성되어있으며, 제안모델은 14개분야 119개 통제항목으로 구성되었다. 일반적으로 컨택센터에서는 전자거래가 이루어지지 않으므로 전자거래 보안 분야를 삭제하였다.

2) 기존 ISMS의 통제분야 중에 공통적으로 적용 가능한 9개 통제분야("정보보호조직", "정보자산분류", "정보보호교육 및 훈련", "인적보안", "물리적보안", "시스템개발보안", "암호통제", "보안사고관리", "업무연속성관리")의 통제항목과 내용은 그대로 적용하였다.

3) "정보보호정책"분야의 "상위정책과의 일관성"통제사항에 대하여 업무수탁 운영시의 위탁자의 정보보호정책과의 일관성을 유지토록 내용을 보완하였다. 수탁자가 여럿인 경우에도 위탁자의 보안정책을 따르도록 함으로서 효과적인 정보보호를 이룰 수 있을 것이다.

4) "외부자보호"분야에 1개 통제사항("외부자 수탁보안관리")을 추가하고, 업무수탁 운영시의 수탁자의 의무사항을 명문화하고 SLA 등의 보안요구사항을 준수토록 하는 내용을 신설하였다.

5) "접근통제"분야에 1개 통제사항("인가자의 접근")을 추가하고, 정보자산에의 접근권한 인가자가 다수인 특성을 반영하고, 내부정보 유출 예방 대책을 수립토록 하는 내용을 신설하였다. 따라서 다수의 인가자에 대한 접근통제권한을 업무특성별로 세분화 및 그룹화 하여 관리하는 등의 대책으로 효과적인 정보보호가 가능하다.

6) "운영관리"분야에 1개 통제사항("매체제한 및 통제")을 추가 및 내용을 신설하고, 1개 통제사항("로그관리")의 내용을 보완하여, 주요정보 및 내부정보 유출 시도 등을 예방하는 내용을 반영하였다. 내부 정보유출을 방지하기 위하여 체계적인 로그관리나 단말장치의 매체에서의 복사 등을 제한함으로서 외부로의 정보유출을 예방하는 효과를 거둘 수 있다.

7) "검토,모니터링 및 감사"분야에 1개 통제사항("모니터링 결과 활용")을 추가하고, 모니터링 결과 등을 내부정보 유출 예방에 활용할 수 있는 내용을 신설하였다. 이러한 활동은, 모니터링 결과 등을 감독자나 당사자에게 제공함으로서 중요정보자산 취급자들의 정보보호마인드를 환기시키고 정보유출가능성을 최소화할 수 있다.

V. 결 론

컨택센터는 상품이나 서비스 등에 대한 단순안내 업무에서 출발하여 전문적이고 기술적인 상담업무 등으로 그 업무영역이 확대되고 있으며, 적용분야나 규모 면에서도 여러분야로 확대되고 많은 성장을 하고 있다. 또한 기술적인 면에서도 많은 발전을 이루어 최신의 멀티미디어 기술을 활용하는 컨택센터들이 등장하고 있으며, ALL IP 기반의 컨택센터로 전환이 이루어지면, 고객에게 다양하고 보다 편리한 서비스를 제공할 수 있어 효과적인 컨택센터를 기대할 수 있다. 또한 기업의 CRM 마케팅 등의 활성화 추세로 컨택센터의 중요성이 커지고, 고객정보 데이터베이스의 공동사용, 지역이나 기능을 통합한 통합컨택센터 구축이 활발하다. 따라서 컨택센터의 대형화와 통합화에 따른 고객정보 등의 주요정보자산에 쉽게 접근할 수 있는 이점과 함께 정보보호의 필요성은 더욱 커졌다.

컨택센터에서의 정보보호를 체계적이고 종합적으로 할 수 있는 방법은 정보보호관리체계(ISMS)를 도입하는 것이 효과적이라 생각되어, 국제 ISMS 표준을 기반으로 하여 국내 실정에 맞게 제정된 국내의 KISA-ISMS 모델을 분석하고 연구하였다. 또한 컨택센터의 특성분석을 통하여 ISMS 도입 시 반영하여야 할 사항

을 중점적으로 분석하여 고려사항을 도출하였다. 컨택센터의 구축에 있어 고객관련정보 등의 주요정보를 수집·활용하기 위한 시스템 및 데이터베이스를 직접 갖추거나, 다른 서비스시스템들의 데이터베이스를 공동이용 또는 통합데이터베이스로 부터의 주요정보 등을 이용하는 방법 등이 있다. 일반적으로 체계적인 정보보호의 필요성이 큰 컨택센터의 경우는 해당 서비스 시스템의 데이터베이스나 통합데이터베이스의 주요정보자산을 공동 이용한다. 따라서 본 논문에서는 컨택센터에서의 고객관련정보 데이터베이스 등의 시스템구축이나 고객관련정보 이용에 대한 시스템개발 분야의 보안에 대하여는 별도로 다루지 않았다. 그러나 개별서비스 시스템이나 통합데이터베이스 시스템의 개발이나 구축 시에 컨택센터에서의 고객관련정보 등 주요정보자산 이용에 대한 보안을 고려함이 바람직하다.

컨택센터는 주요정보를 취급하는 권한을 가진 많은 사람들로 인해, 정보누출의 위협이나 취약점이 타 산업분야나 타 조직체 등에 비해 상대적으로 높은 편이다. 따라서 컨택센터의 아웃소싱 형태의 운영추세와 컨택센터의 구성원 대부분이 주요정보자산에 접근하는 인가자이며 그 수가 매우 많은 특성 등을 반영하여 컨택센터에 적용할 수 있는 ISMS 모델을 제안하였다. 제안 모델은 컨택센터의 아웃소싱 운영방식 및 대형화, 통합화 추세에 따른 보안대책을 강구할 수 있고, 내부정보유출 위협 등에 대비할 수 있도록 통제사항에 반영이 되어 있으므로 내부정보 유출가능성을 최소화할 수 있을 것이다. 또한 내부정보유출 예방 대책 방안을 제시하였다. 본 논문에서 제안하는 컨택센터 ISMS를 적용하면, 컨택센터에서 체계적이고 효과적인 정보보호관리가 가능하여, 보다 향상된 대고객 서비스를 제공할 수 있을 것이다.

향후에는 컨택센터 ISMS의 효율적인 구축을 위한 세부실행방안이나 실행지침들에 대한 연구를 통하여 세부기준이나 방법 등을 제시하여, 컨택센터에서의 ISMS 도입 및 구축 효과를 높이는 작업이 필요하다. 또한 본 논문에서 제시한 컨택센터 ISMS 사항을 인증심사 기준에 반영하여, 한국정보보호진흥원에서 컨택센터에 대한 ISMS인증 시, 평가에 적용함이 바람직하다고 생각한다. 컨택센터 ISMS의 인증심사기준 채택은 컨택센터의 ISMS 도입 필요성의 인식을 확산시키고, 증가하고 있는 컨택센터들의 정보보호활동과 ISMS 도입 및 인증에 많은 도움을 줄 것으로 생각한다.

참고문헌

[1] 선종선, "효율적 Contact Center 운영방안에 관한 연구", pp. 4-11, p23, pp42~54, *동국대학교 경영대학원*, 2006. 2.

[2] 김양규, "CTI체계하에 효율적인 콜센터 구축방안에 관한 연구", pp. 17-21, *영남대학교 산업대학원*, 2003. 8.

[3] 임재범, "IPCC 기반의 CTI 최적화 구축", *세종대 정보통신대학원*, 2005. 8.

[4] 정현준, "국내외 정보보호관리체계 연구", *대전대학교 산업정보대학원*, pp. 13-15, 2003. 2.

[5] 이창호, "BS7799 정보보호관리체계 기반의 정보보호위험관리 시스템(ISRMS)에 관한 연구", *동국대 국제정보대학원*, 2007. 2.

[6] 김상호, "프로세스 성숙도 모델 및 보안관리체계 인증을 활용한 IT보안성 평가에 관한 연구", *연세대 대학원*, 2006. 2.

[7] 황완식, "정보보호와 사람", *Network Times*, pp. 227-228, 2007. 4, www.dataNet.co.kr

[8] "BS7799", http://www.dnv.co.kr/Binaries/BS7799 Description_tcm34-89786.pdf

[9] James St. clair, http://www.icgfm.org/documents/StClair.ppt

[10] Johe Snare, "Information Security Management", *Standards Australia Forum*, 19July2006

[11] http://www.dnv.co.kr/Binaries/BS7799_Description_tcm34-89786.pdf

[12] http://www.dnv.co.kr/certification/managementsystems/iso27001.asp

[13] TTAS.KO-12.0036, "정보보호관리체계 수립지침", *한국정보통신기술협회*, pp. 2-6, 2006. 12.

[14] 정보통신부고시 제2007-30호, "정보보호관리체계 인증심사기준", *정보통신부*, 2007. 8. 14.

[15] 이종남, 박민규 , "지역 비즈니스 서비스산업 활성화 방안 : 컨택센터를 중심으로", *대구경북연구원*, pp. 22-27, 2005.

[16] 박응희, "정보기술을 활용한 대고객서비스에서 인적오류의 영향에 관한 탐색적 연구", pp. 31-38, *전남대학교 대학원*, 2006. 2.

[17] 고은경, "내부마케팅요인과 이직의도가 미치는 영향에 관한 연구(통신회사 인.아웃바운드 콜센터

중심으로)", pp. 6-14, *동국대학교 정영대학원*, 2006. 6.

〈著者紹介〉

권영관 (Young-Kwan Kwon)
종신회원

1986년 2월 : 서울산업대학교 전자공학과 졸업(학사)
1990년 9월 : 연세대학교 산업대학원 전자공학과 졸업(석사)
1982년 1월~2000년 3월 : 한국통신, KT 부장, 국장
2000년 3월~2005년 4월 : KT 중앙데이터통신국장, 인터넷기술담당(상무)
2005년 4월~2006년 12월 : KT Linkus 신사업추진본부장
2002년 1월~2008.1 : 한국정보통신기술사협회 부회장
2007년 1월~현재 카스정보통신 주식회사 사장
2002년 1월~현재 : 한국인터넷기반진흥협회 이사
현재 : 정보통신기술사, CISSP
<관심분야> 네트워크보안, 망관리 및 보안관제, Security Service

염흥열 (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, 논문지 심사위원장, 상임부회장
2004년 1월~현재 : 한국인터넷정보학회 이사, 논문지 편집위원
2005년 ~현재 : ITU-T SG17/Q9 Rapporteur
2006년 11월~현재 : 정보통신연구진흥원 정보보호전문위원
<관심분야> 인터넷보안, USN 보안, 홈네트워크 보안, 암호 프로토콜