

HRM 시스템의 개인정보보호기술 적용방안

강민영*, 박석천**, 홍석우***

*가천대학교 일반대학원 모바일소프트웨어학과

**가천대학교 컴퓨터공학과 정교수(교신저자)

***화이트정보통신 사업총괄 부사장

ceciwow@naver.com

Applied Method of Personal Information Protection Technology in HRM System

Min-Young Kang*, Seok-Cheon Park**, Suk-Woo Hong***

*Dept. of Mobile Software, Gachon University(Corresponding Author)

**Dept. of Computer Engineering, Gachon University

***White Information Networking Co., Ltd

요 약

올해 정보보호 10대 이슈로 ‘SW 개발보안 의무화 및 정보관리범위 확대’ 등이 제시되었으며, 이는 개인정보 보호에 대한 중요성이 더욱 부각될 것임을 보여주고 있다. 특히, 인적자원관리 시스템의 경우는 대부분 조직체 내 구성원들의 개인정보를 관리하고 있기 때문에 다른 시스템에 비해 보다 강화된 개인정보보호기술이 적용되어야 한다. 본 연구에서는 IT시장 동향 및 통계자료를 통해 개인정보보호기술의 중요성을 확인하고 국내외 관련 개발기술동향과 사례분석을 통해 HRM(인적자원관리) 시스템 내 개인정보보호기술 적용방안을 제안한다.

I. 서론

방송통신위원회에 따르면 '12년도 개인정보 침해 건수가 총 166,801건으로 전년대비 약 26.7% 증가하였다. 침해 세부사항을 살펴보면 주민등록번호 등 타인 정보의 훼손·침해·도용에 관한 침해 신고가 139,724건(전년대비 약 52% 증가)으로 가장 많았고(전체의 83.8% 차지), 기술적·관리적 조치 미비에 관한 침해신고가 3,855건(전년대비 약 65% 감소)으로 그 뒤를 이었다.

조직체 내 구성원들의 개인인사정보를 전략적으로 관리하여 해당 조직의 경쟁력을 강화시키는 것이 HRM(인적자원관리) 시스템의 궁극적인 목표이다. [그림1]과 같이 개인정보침해 신고 건수가 매년 증가하고 있는 상황에서 민감한 개인인사정보를 관리하는 인적자원관리시스템이 가지는 개인정보보호기술의 중요성은 매우 크다고 할 수 있다.

본 연구에서는 개인정보보호기술의 필요성을 증대시키는 IT업계 시장 동향과 사회적 이슈를 살펴보고 국내외 관련 개발기술 사례분석을 통해 인적자원관리시스템 내 적용가능한 개인정보보호기술 적용방

안을 제시한다.



[그림1] 개인정보침해신고 상담건수

II. 개인정보보호 기술의 필요성 증대

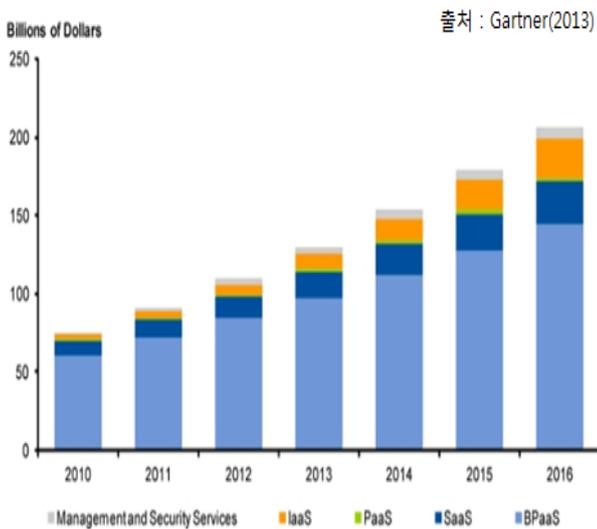
[표1]과 같이, 옥션(2008년 1월)을 시작으로 지난 4년간 민간기업의 고객정보 유출사고가 끊임없이 발생하였고 이로 인해 총 개인정보 유출건수는 1억 657만 건에 달하였다. 개인정보 침해사고로 인한 피해가 속출하자 정부는 개인정보보호법을 제정하여 2011년 9월 30일 부로 시행하고 있다. 이후 기업들

[표1] 민간기업 개인정보 유출사례

일시	위치 (기업)	유출 건수	비고
2008년 1월	옥션	1,863 만 명	해킹
2008년 9월	GS칼텍스	1,125 만 명	내부 직원의 판매
2009년 4월	네이버	9 만 명	유출
2010년 3월	인천(조선족 해커)	2,000 만 명	해커가 개인정보 판매
2010년 3월	대전(중국 해커)	650 만 명	해커가 개인정보 판매
2010년 4월	부산(중국 해커)	1,300 만 명	해커가 개인정보 판매
2011년 4월	현대 캐피탈	175 만 명	해킹
2011년 7월	SK컴즈, 네이트	3,500 만 명	해킹
2011년 8월	한국 엡손	35 만 명	해킹
총 개인정보 유출 건수		1억 657 만 명	

은 해당 법률에서 제시하고 있는 개인정보 라이프 사이클을 숙지하고 각 단계에 맞는 정보보호방안을 모색하여 투자 비중을 늘려가고 있다. 이처럼 개인정보보호법 제정 및 강화 추세로 인한 기업들의 개인정보보호기술에 대한 수요는 증대하고 있다.

몇 해에 걸쳐 주요 IT이슈로 언급되고 있는 클라우드 컴퓨팅 시장의 수요 증대 역시 개인정보보호 기술의 중요성을 부각시키고 있다. [그림2]에서 보는 것처럼 클라우드 서비스 시장규모는 2016년까지 17.7%의 성장률을 보이며 꾸준히 증대할 것으로 전망된다.



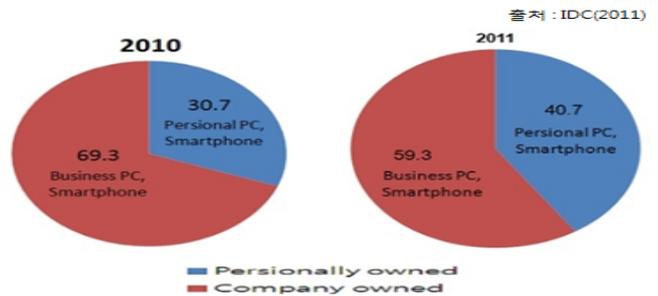
[그림2] 클라우드 서비스 부문별 시장규모

클라우드 컴퓨팅은 인터넷을 통해 서버, 스토리지, 소프트웨어 등 IT 자원을 필요시 이용하는 방식으로서 온라인을 통한 데이터 공유가 용이해진 만큼 해킹이나 악성코드에 대해 취약하기 때문에 보안성 문제가 두드러지는 것이 특징이다. 그러나 클라우드 컴퓨팅 방식은 거스를 수 없는 IT 흐름으로서 많은 기업들이 보안 취약성을 감안하더라도 클라우드 컴퓨팅 방식을 적용하고자 한다. 국내 HR분야에서도

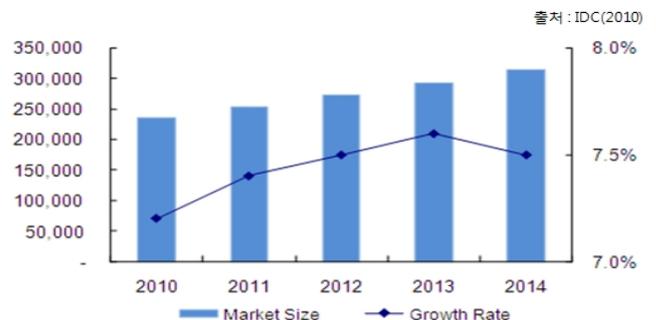
인적자원관리 시스템을 고객사에 직접 설치하는 방법에서 클라우드 컴퓨팅 방식 중의 하나인 SaaS(Software as a Service) 형태로 인적자원을 관리하려는 움직임이 일어나고 있다. 엔드 유저(End-User)의 기기에 소프트웨어나 애플리케이션을 설치하는 대신 웹 접속을 통한 임대 형태로 소프트웨어를 사용하도록 하는 SaaS형태로의 HR 서비스 제공은 정보보호기술에 대한 필요성을 더욱 증가시킬 것이다.

III. 국내외 개발기술 동향

다양한 태블릿 PC, 스마트폰의 등장으로 개인 소유의 모바일 기기가 증가함에 따라 [그림3]에서 보는 바와 같이 개인 소유의 단말기를 업무에 활용하는 비율이 점차 늘어가고 있다.



[그림3] 개인용 업무 디바이스 활용 비율
기업 구성원들이 자신의 모바일 기기를 업무에 활용하는 BYOD(Bring Your Own Device) 시장의 확산 및 기업 내 클라우드 컴퓨팅 환경의 확산 등 다양한 이슈들이 [그림4]와 같은 보안 소프트웨어 시장 전망을 가져오고 있다. IDC에 따르면 국내 보안 소프트웨어 시장규모가 연평균 7.4%의 성장세를 보이며 2014년에는 3,142억원 규모에 이를 것이라 하였다.

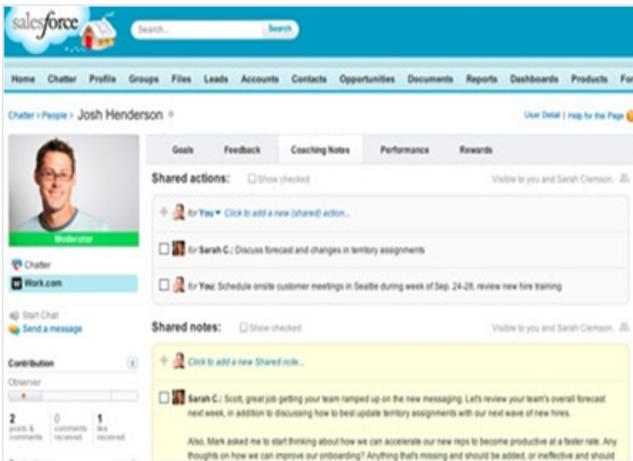


[그림4] 국내 보안 소프트웨어 시장 전망
정보 보안에 대한 수요가 지속적으로 증가해가는 시장 동향에 따라 인적자원관리시스템 내 개인정보 보호 기술에 대한 수요도 증대할 수밖에 없다. 특히, 앞서 언급한 SaaS 등 클라우드 기반의 인적자원관

리 시스템으로의 전환이나 BYOD 시장에 최적화된 인적자원관리시스템 개발은 필수 전제조건으로서 개인정보보호 기능 강화가 필요하다.

인적자원관리 패키지 솔루션 개발부문의 글로벌 기업인 SAP은 지난해 데이터베이스 단계뿐만 아니라 애플리케이션 단계에서도 완벽하게 접근제어를 할 수 있는 'SAP UI 마스킹 및 로깅 솔루션'을 개발하였다. 이를 통해 ERP(전사적자원관리) 애플리케이션 상의 레벨 보안을 테이블 및 필드 단계로까지 확장하여 성명, 주소, 계좌번호, 카드번호 등에 대한 접근권한제어와 차등적 권한부여 및 접속기록 구축 등이 가능해졌다. 권한이 없으면 절대 테이블 및 필드 상의 데이터를 조회할 수 없게 됨에 따라 고도화된 보안체계를 확보하였다.

클라우드 기반의 CRM(고객관계관리) 솔루션을 제공하는 글로벌 기업 Salesforce.com은 CRM분야뿐만 아니라 인적자원관리 요소 중의 하나인 성과관리 솔루션을 SaaS형태로 제공하고 있다. [그림5]와 같이 직원을 정렬하고 팀에 동기를 부여하며 성과를 향상시킬 수 있는 새로운 방식을 Work.com 소셜 성과 관리 플랫폼을 통해 서비스하고 있다.



[그림5] Salesforce Work.com 성과관리 플랫폼

이러한 SaaS 형태로의 솔루션 제공을 위해 Salesforce.com는 철저한 보안정책을 수립하여 실시하고 있다. 업계 표준 보안 소켓 계층(SSL) 기술을 사용하여 사이트 접근 시 서버 인증 및 데이터 암호화를 모두 사용해 고객의 데이터를 보호하고, 방화벽, 침입 탐지 시스템 및 기타 고급 기술을 사용하여 외부 침입자의 방해나 액세스를 방지하는 보안 서버 환경에서 이 웹사이트를 호스팅하고 있다.

삼성은 모바일 월드 콩그레스 2013(Mobile World Congress 2013)에서 안드로이드 기반의 기업용 보안 솔루션 '녹스(KNOX)'([그림6])를 공개하면서

BYOD시장 공략을 시작하였다. 녹스는 하나의 스마트 기기에 암호화된 컨테이너라는 별도 공간을 만들어 업무용 데이터와 개인용 데이터를 분리하여 관리하고 암호화된 컨테이너를 통해 해킹, 바이러스, 정보유출 등의 위협으로부터 업무용 데이터를 보호한다.

Samsung KNOX for Enterprise

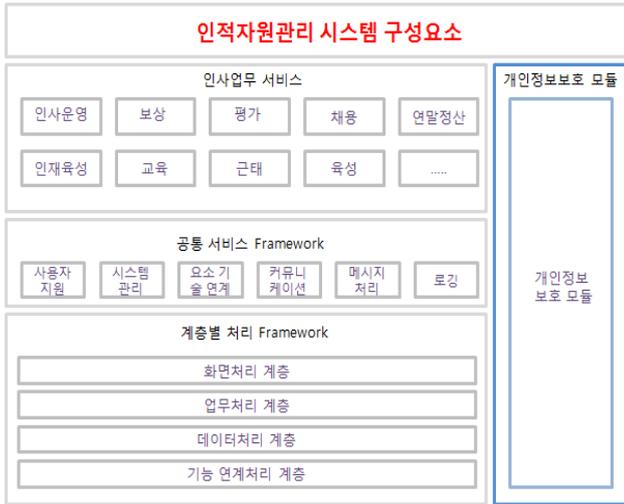


[그림6] Samsung KNOX for Enterprise

삼성의 녹스 개발 등 BYOD시장의 성장은 인적자원관리 솔루션을 개인 모바일 기기 안에서 자유롭게 사용하고자 하는 인사담당자들의 수요에도 영향을 미칠 것이다. 인적자원관리에 녹스 기능을 적용시킨다면, 암호화된 컨테이너 안에 성과관리, 채용관리, 보상관리 등 필요한 인적자원관리 요소를 어플리케이션으로 담아놓고 개인 모바일 기기로 자유롭게 업무를 볼 수 있을 것이다.

IV. HRM 시스템 내 개인정보보호기술 적용방안

기존의 인적자원관리 솔루션 관련 글로벌 벤더들은 보안 솔루션을 확보한 후, 이를 기존의 인적자원관리 솔루션과 융합하여 판매하는 전략을 택하고 있다. 하지만 이러한 방식은 개인정보보호법 등 국내외 컴플라이언스를 준수하여 커스터마이징 하는 것이 어렵다는 단점이 있다. 이 점에 착안하여 본 논문에서는 인적자원관리 시스템을 구성하고 있는 인사운영, 보상, 채용 등과 같은 인사업무 전 영역에 개인정보보호기능을 삽입할 수 있도록 설계하고자 한다. 이는 별개의 보안 솔루션을 만드는 것이 아니라 [그림7]과 같이 기존의 인적자원관리 솔루션 안에 개인정보보호 모듈을 삽입하여 이 모듈이 기존 솔루션의 구성요소로서 한 부분을 차지하도록 하는 형태이다.



[그림7] 개인정보보호 기능을 강화한 인적자원관리시스템 모듈 구성도

이러한 모듈 구성은 국가별 개인정보보호법에 따른 개인정보 라이프 사이클을 반영한 커스터마이징이 용이하고, 관련 법률의 수정이나 신설사항에 대해서도 유연하게 시스템에 반영할 수 있다.

개인정보보호 모듈은 [그림8]과 같이 5가지 주요 기능을 제공할 수 있도록 설계한다. 첫째, 저장 중인 데이터, 이용 중인 데이터, 전송 중인 데이터들을 보호하기 위해 백업데이터 암호화, 네트워크 암호화, 데이터베이스 암호화를 진행한다. 둘째, RBAC(Role Based Access Control) 기반의 접근통제 및 사용자 인증을 통한 사용자 확인기능을 진행한다. 셋째, 사용자 권한관리를 진행한다. 넷째, 감사로그를 통한 사용자 행위 모니터링을 진행한다. 마지막으로 규제 준수, 리스크 관리 등 정보보호 현황을 한눈에 확인할 수 있는 대시보드를 제공한다.



[그림8] 개인정보보호 모듈 기능

이러한 주요 5가지 기능을 구현할 수 있는 개인정보보호 모듈을 설계하여 개인정보보호 기반의 고도화된 인적자원관리 시스템 구축이 필요하다. 위에 언급한 개인정보보호 모듈의 5가지 기능 이외에 보다 강화된 정보보호를 위한 인적자원관리 시스템 콘텐츠를 지속적으로 고안하여 개인정보보호 모듈에 적용시켜 나가야할 것으로 판단된다.

V. 결론

정보통신기술(ICT)산업의 발전으로 삶의 질과 생활 편리성이 증대되었지만 동시에 해킹으로 인한 개인정보유출, 전산망 마비 등 개인 및 국가핵심기반에 치명적인 결과를 가져올 수 있는 문제점들이 빈번하게 발생하고 있다. 이러한 사회적 이슈는 각종 시스템에 대한 보안기술의 강화 필요성을 다시 한번 강조해주고 있다. 특히, 조직 구성원들의 신상정보를 기반으로 데이터를 형성하는 인적자원관리시스템에 대한 개인정보보호기술의 중요성은 더욱 클 수밖에 없다.

본 논문에서는 별개의 보안 솔루션이 아닌 기존 솔루션 내에 개인정보보호 모듈을 삽입하여 보상, 채용 등 인사업무 전 영역에 걸쳐 최적화된 개인정보보호 기술을 적용한 모델을 제안한다. 개인정보보호 모듈을 통해 국가별 개인정보보호 표준을 유연하게 반영할 수 있는 편의성과 확장성이 보장된 개인정보보호 기반의 인적자원관리 시스템을 개발할 수 있을 것이다. 이는 국내뿐만 아니라 글로벌 시장을 목표로 인적자원관리 서비스를 제공할 수 있는 기반을 마련해준다는 점에서 의의가 있다.

앞서 언급한 개인정보보호 모듈 5가지 주요기능 이외에 국내외 개인정보보호법 및 개인정보 라이프 사이클을 고려한 정보보호 관련 콘텐츠를 지속적으로 발굴하고 모듈화하여야 한다. 그리고 개발된 개인정보보호 모듈과 기존 인적자원관리시스템과의 연계를 위한 인터페이스 개발 연구도 진행되어야 할 것이다.

VI. 결론

본 연구는 2013년도 지식경제부의 SW전문인력양성사업의 재원으로 정보통신산업진흥원의 고용계약형 SW석사과정 지원사업(HB301-13-1003)으로부터 지원받아 수행되었습니다.

참고문헌

- [1] 행정안전부, “개인정보보호법 주요내용 및 이행사항”, 2012.02
- [2] 김재필, “스마트 오피스의 새로운 트렌드 BYOD”, KT 경제경영연구소, 2011.
- [3] “방송통신위원회 홈페이지”, <http://www.kcc.go.kr>
- [4] “삼성 글로벌 홈페이지”, <http://www.samsung.com/global/business/mobile/solution/security/samsung-knox>
- [5] “세일즈포즈닷컴홈페이지”, <http://www.salesforce.com>