I

개인정보보호 기술의 현황 및 전망

닉스테크(주) ‖ 김 상 진

1. 개인정보보호의 필요성

1.1 연구의 필요성 및 목적

정보통신 기술의 발전과 인터넷의 급속한 파급으로 모든 산업분야에 정보화가 이루어져 가고 있으며, 지식정보기반의 사회구조로 빠르게 진행되고 있다. 경제, 사회 활동 전반에 걸쳐 인터넷이나 정보통신 시스템을 이용한 개인정보의 수집 및 이용이 일상화되고 그 활용범위가 확대되고 있다. 생산 및 서비스 분야의 발전으로 기업의 소비자에 대한 서비스의 품질향상이 필요하게 되었고 기업은 상품이나 서비스 등에 대한 정보를 더 많이 고객에게 전달하고, 그에 대한 고객의 문의사항이나 요구사항 등을 보다 빠르고 편리하게 응대하여 고객을 만족시키려는 노력을 기울이고 있다. 고객 만족을 이끌어 내어 향후의 신상품이나 서비스 등에서도 자사의 상품이나 서비스를 이용토록 하는 영구고객화 전략 등에 많은 자원을 투입하고 있으며 이를 위해서 개인정보의 수집 및 활용범위가 더욱 확대되고 있으며 그에 따라 개인정보의 가치 향상과 함께 개인정보 침해사고의 발생 가능성은 더욱 증가되고 있다. 언론에 발표된 여러 사례에서도 보듯이 개인정보 침해사고가 크게 증가하고 있으며 개인정보 침해사고 발생 시에는 당사자의 정신적, 경제적 피해는 물론 해당 기업에게도 막대한 손실과 피해를 가져다 주게 된다. 개인정보의 유출은 회사가 법적인 책임을 물어야 하기에 이에 따른 비용이 엄청나게 많이 필요할 뿐 아니라 회사의 대외 이미지 손상 및 고객으로부터의 신뢰감 실추로 인한 간접적인 영업의 손실 등의 비용 외적인 손실을 감수해야만 한다. 즉 기업입장에서는 개인정보는 단순히 보호해야만 하는 중요한 기밀 정보일 뿐만 아니라 최대한 활용해야하는 정보이며 따라서 최대한 보호하면서 동시에 최대한 활용할 수 있는 방안을 찾아야 하는 골치 아픈 문제이다.

또한 정부에서도 인터넷 이용자들의 개인정보 침해 우려가 날로 증가하자 인터넷 기업들의 무분별한 개인정보 수집과 오남용을 억제하기 위하여 개인정보보호와 관련된 정책 및 법률을 제정하고 이를 지키도록 의무화하고 있다. 그러나 인터넷을 이용하여 개인정보를 취급하는 기업의 입장에서 보면, 개인정보 수집과 활용을 무작정 규제하거나, 제지하는 것은 바람직하지 않다. 디지털 경제시대에 있어서는 개인정보를 효과적으로 보호하는 것 못지 않게 기업들이 인터넷을 통하여 고객의 개인정보를 일정한 조건하에서 자유롭게 수집하고 이를 가공하여 활용할 수 있도록 보장하는 것이 필요하다.

최근 여러 개인정보 유출 사례에서 보듯이 개인정보유출은 외부로부터의 악의적인 공격 보다 내부의 일반직원들의 부주의와 기업의 프로세스 위반으로 인해 주로 발생하는 것을 알 수 있다. 미 "경제스파이법(Economic Espionage Act. 1996)"의 대표적인 사건(유죄판결) 15건 중 전.현직 직원이 주범인 경우가 13건으로 판명되었고(국가정보원 (2007. 2.). "첨단 산업기술 보호동향" (제7호)), McAfee사의 퍼듀대학교 공동조사에 따르면(McAfee (2009). Unsecured Economies: Protecting Vital Information), 정보보안의 위협요소는 해고직원 유출(42%) 〉 외부인 절취(39%) 〉 내부직원 유출(36%) 등(복수응답)으로 판명되었다. 특히 근래와 같이 전 세계를 휩쓸고 있는 경제위기 상황에서는 내부자에 의한 정보 유출위협이 더욱 증가될 것으로 예상되는데 그 이유는 크게 두 가지를 들 수 있다. 우선, 인원감축과 인건비 동결 등으로 직원들의 경제적인 압박이 심해지면서 금전적인 이득을 취하기 위한 정보유출이 늘어날 것으로 보인다. 내부직원의 정보유출은 장기적인 계획보다 순간적인 감정에 의한 결정으로 발생하는 경우가 많기 때문에 기업은 기밀정보가 어디에 있으며, 어떻게 사용되고 있는지 정확히 파악해 손실을 최소화하기 위한 방안을 마련해야 한다. 다음으로 경기불황 속 M&A가 활발히 진행되면서 정보유출 위협이 증가할 수 있다. M&A는 기업의 생

존을 건 문제인 동시에 대규모 인력감축에 대한 불안감을 증폭시켜 내부자에 의한 정보유출이 발생할 위험이 크다. 특히, M&A 진행 이전 관련 계약 내용의 유출로 계약이 무산되는 등의 문제가 발생할 수 있다. (삼성경제연구소, SERI 경영 노트, 제 10호, 2009. 6. 11, 4page-7page)

본 연구에서는 위에서 언급한 점을 고려하여 기업의 입장에서 내부자(현.전직직원)에 의한 개인정보유출방지에 초점을 맞추어 기업의 입장에서 사용하고 있는 개인정보보호를 위한 솔루션들에 대하여 살펴보고 기존 솔루션이 개인정보의 최대한 활용과 보안을 동시에 만족시킬 수 있는지 확인을 통해 한계점을 살펴보고 기존의 한계점을 극복할 수 있는 향후 기술의 방향을 제시해 보는데 그 목적을 둔다.

2. 배경지식

2.1 개인정보란?

공공기관의 개인정보보호에 관한 법률 제2조 제2호에서는 개인정보를 다음과 같이 정의한다.

"생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 성명, 주민등록번호 및 화상 등의 사항에 의하여 개인을 식별할 수 있는 정보(당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함한다)".

민간부문의 개인정보의 정의는 정보통신망이용촉진 및 정보보호 등에 관한 법률 제2조 제1항 6호에는 다음과 같이 정의하고 있다.

"생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호, 문자, 음성, 음향 및 영상 등의 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)".

전자서명법 제2조 제13호에서는 "생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호, 문자, 음성, 음향, 영상 및 생체특성 등에 관한 정보(당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함한다)"로 생체특성 정보에 대해서도 직접 언급하고 있다.

예를 들어서, 주소와 이름을 결합하면 "어디 사는 아무개"와 같이 특정인을 식별할 수 있는 정보가 되므로 이는 개인정보에 해당한다. 따라서 여권번호, 자동차 운전면허번호, 이메일 주소, 전화번호, 성명 등 주민등록번호 이외에도 개인을 식별할 수 있는 다양한 정보들이 모두 보호해야 할 개인정보라 할 수 있다. 다만, 법의 보호 범주에 포함된 개인정보는 생존하는 개인에 관한 것이기 때문에 사망하였거나 사망으로 추정되는 개인에 관한 정보는 보호대상이 아니다. 그 외에도, 전자태그(RFID)에 의한 개인 위치정보, CCTV/디지털카메라 등에 의해 수집된 화상정보, 지문인식과 같은 생체인식 기술에 의한 생체정보 등 개인을 식별할 수 있는 정보의 범위는 점차 확대되고 있다. 따라서 정보화 및 지식기반 사회로의 발전에 따라 개인정보와 프라이버시를 동일 시 하는 경향이 있다. 법제도 부문에서도 정보통신망법을 비롯하여 위치정보보호법, 생체정보 가이드라인 등 사회발전에 따른 새로운 분야에서의 개인정보보호 관련 법제도를 검토 및 제정해가는 추세이다.

아래 표 1은 이해를 돕기 위해 개인정보의 종류를 몇 가지로 분류해 보고 그 예를 들어 보았다.

2.2 개인정보 유출 사례 및 피해

일반적으로 개인정보는 "그 사람 자체"를 나타내는 중요한 정보로서 정보사회의 진척에 따라 개인정보의 유·무형 가치가 증대되고 있으며 정보사회의 핵심으로 평가 받고 있다. 따라서 개인정보 침해사고가 발생하게 되면 개인적으로는 정신적, 경제적 피해를 입

표 1 개인정보의 세부적인 구분

구분	세부항목
신분정보	성명, 주소, 주민등록번호, 본적, 가족관계 등
심신정보	신장, 체중, 건강상태, 병력, 장애 여부 등
내면의 비밀	사상, 신조, 종교, 정치적 성향 등
경제정보	소득규모, 재산상황, 거래내역, 신용등급, 채권채무관계 등
사회관계 정보	전화번호, 주소, 이동전화번호, 직장, 직위 등
생체정보	지문, 홍채, DNA 등
위치정보	GPS, 휴대폰 위치정보, RFID 등
네트워크정보	쿠키(Cookies), 로그(log) 등
기타 정보	교통이용정보, 차량 및 이용 정보, 통신사실 확인자료 등

을 뿐 아니라 기업이나 공공관에 큰 손실을 야기하게 되고 심한 경우 사회적 혼란을 초래하기도 한다. 개인정보침해사고는 다양한 형태로 발생하고 있으며 그 규모나 피해도 점차 커지고 있다. 요즈음 언론보도 등을 통해 알려지고 있는 바와 같이 크고 작은 개인정보침해 사고들이 많이 발생하고 있다. 특히 최근에 우리나라에서 발생한 유명 쇼핑몰 및 경매사이트를 운영하는 옥션사의 개인정보유출과 하나로텔레콤의 개인정보유출, GS칼텍스사의 개인정보유출 사고 등은 사회적 문제로 대두되고 있다. 해외 및 국내 사례를 살펴보면 다음과 같다.

2.2.1 해외사례

가. 일본야후BB(BroadBand)의 고객 개인정보 유출 사례

2003년 발생한 일본야후BB의 고객 개인정보 유출 사건의 정보유출자는 전야후BB고객센터의 직원이었다. 그는 야후BB센터에 근무하면서 DB열람 등을 통해 고객정보를 입수하여 야후BB에 대해 고객정보 수백만건을 가지고 있다고 협박하여 현금 수억 엔을 요구하다 공갈미수혐의로 경찰에 체포되었다. 경찰 수사 및 야후BB 자체조사 결과에 의하면 고객 약451만명의 개인정보가 실제 유출된 것으로 확인하였다. 이에 대하여 야후BB는 다음과 같은 사후조치를 취했다.

- 야후BB(소프트뱅크) 대표이사 손정의씨의 대국민 사과
- 경영진 징계 : CEO 50% 6개월 감봉 등
- 고객에 대한 사과 : 전체 가입자에게 명의 도용 여부 상관없이 500엔 상당 상품권 지급(총 지급 비용 40억엔, 한화 330억 상당)

이 사건에 대하여 일본 오사카 지방법원은 야후BB 고객정보 유출로 정신적 피해를 입었다며 야후BB 회원 5명이 제기한 손해배상 소송 판결에서 원고 1인당 6천엔을 지급하도록 판결하였다.(2006년) 손해배상의 주요 이유로는 "정기적인 비밀번호 변경 등 보안조치 소홀"과 "성명, 주소 등 비밀정도가 낮은 개인정보가 유출되었더라도 기업은 고객의 사생활 침해에 대한 책임 부담을 해야한다"고 밝혔다.

나. 일본 미즈호 은행 직원의 고객정보 유출 사례

2006년 2월에 일본 미즈호 은행 직원이 고객 628명의 개인정보를 외부인에게 판매한 혐의로 체포되었다. 유출된 정보는 "성명, 주소, 계좌번호 등 주요 신용정보"였다. 일본 금융청은 미즈호 은행에 대해 일본 개인정보법 제20조에 의한 시정조치를 권고하였는데, 이 조치는 미즈호 은행이 2006년 5월말까지 개인정보보호조치 및 직원 관리 감독 개선사항을 금융청에 보고하여야 하는 것이었다. 일본 금융청의 조치는 은행 경영진의 직접책임을 인정한 것으로, 향후 기업경영진의 정보보호 의무가 더욱 강화 될 것을 예고하였다는데 큰 의미를 부여할 수 있다.

다. 미국 Choice Point사 고객정보 유출 사례

2004년 10월 미국의 신용정보제공사인 Choice Point사 고객 약 14만명의 개인정보가 유출되어 신용카드 위조 등 불법이용 되었다. 미국FTC(연방거래위원회)는 Choice Point사에게 개인정보취급에 대한 소비자 권리 침해 등의 이유로 미국 FTC 사상 최고액인 1천만 달러 벌금 및 5백만 달러 손해배상을 결정하였다(2006년 1월).

2.2.2 국내사례

국내의 개인정보침해사례도 적지 않으며, 2006년에는 온라인게임 리니지 명의도용, 초고속인터넷 고객정보 유출 등에 대해 피해자들의 손해배상 청구 소송이 제기되었다. 2007년 3월에는 국민은행 고객 30,000여명의 개인정보 유출 사건에 대하여 1심법원은 개인정보가 노출된 1,024명에게 각 10만원, 전자우편만 노출된 2명에게 각 7만원의 손해배상을 판결하였다. 아래 표 2는 초고속인터넷에 관련된 개인정보유출 사례이다.

표 2 초고속인터넷에 관련된 개인정보유출 사례

일자	주요내용	유출건수
06.3월	초고속인터넷업체 텔레마케팅 대행업자가 고객 정보 유출	300만명
06.4월	텔레마케팅 회사가 개인정보를 유통시키고 유통된 정보를 고객 영업에 활용	771만명
06.5월	초고속인터넷업체 전.현직원들이 고객 정보 불법 유출 및 텔레마케팅 업체에 판매	837만명
06.9월	초고속인터넷 고객정보를 P2P를 통해 구매한 후 타 영업점에 유통, 가입 전환 유치에 활요	300만명
06.10월	타 초고속인터넷업체의 전산망을 해킹하여 고객 정보를 유출한 후 가입 유치에 활용	14만명
07.3월	인터넷 카페에서 주요 초고속인터넷업체 사업자들의 고객정보가 담긴 CD 구입 후, 스팸(사채광고) 발송에 활용	400만명

출처 : "초고속인터넷서비스 영업망에서의 개인정보 침해 개선을 위한 소고" , KISA

표 3 개인정보유출사례

회사명	일시	내용	진행상황
엔씨소프트	2005. 5	리니지 게임 업데이트 과정에서 개인정보 파일을 암호화하지 않아 40-50만명(추정) 개인정보 유출	2심에서 엔씨소프트측에 소송제기 5명중 3명에게만 10만원씩 배상판경, 44명 소송중
국민은행	2006. 6	고객에게 단체메일을 발송하면서 3만여명의 개인정보가 담긴 명단을 파일로 첨부	1심에서 1000여명에게 20만원씩 배상판결
LG전자	2006. 9	채용사이트가 해킹되어 응시자 일부 입사지원서 유출	1심에서 31명에게 70만원씩 배상판결
옥션	2008. 2	해킹으로 1,000만명 회원정보 유출	13만명 1심진행
하나로텔레콤	2008. 4	고객 600만명 개인정보 텔레마케팅 업체에 유출	1만 7000여명 1심진행
LG텔레콤	2008. 4	고객정보 사이트 보안 허술로 780만명의 개인정보 유출	270명 1심진행
다음 한메일	2008. 7	접속 오류로 43만명의 회원정보 유출	시민소비자모임이 주축이 되어 소송인단 모집
GS칼텍스	2008. 9	1,100만명의 회원정보를 직원이 유출	온라인카페 30여개 개설돼 소송인단 모집

출처 : 중앙일보 보도자료, http://article.joins.com/article/article.asp?total_id=3293075, 2008. 9

표 3은 최근의 개인정보 유출 사례를 나타내고 있다. 2005년에는 엔씨소프트가 온라인 게임 '리니지2'의 서버 업데이트 중 50만명의 정보가 노출되어 회원 50여명이 소송을 냈다. 2008년 2월에는 중국발 해킹으로 1,000만명의 회원정보가 유출된 옥션은 현재 13만명이 원고로 나섰다. 1,100만여명의 정보가 유출되어 사상 최대로 꼽히는 GS칼텍스 역시 소송이 이어질 전망이다.

GS칼텍스 고객 1,100만 여명의 개인정보를 유출한 사람은 고객정보 관리업무를 맡은 GS칼텍스 자회사 직원이었다. 이 직원은 한 달에 걸쳐 고객정보를 빼돌렸고 범행을 감추려고 사용하던 PC의 하드디스크를 마음대로 바꿨지만 회사측은 이를 전혀 몰랐다. 그는 고객DB를 열어놓고 이를 복사한 뒤 엑셀프로그램에 옮겨 붙이는 단순한 방법으로 1,125만명에 이르는 방대한 개인정보를 빼돌렸다. 그는 한번에 평균 2만건씩 500-600번이나 같은 작업을 했다. 작업을 끝내는데 한달이 넘게 걸렸다. 이와 같이 고객의 데이터베이스에 접속할 수 있는 고객정보취급자는 마음만 먹으면 손쉽게 얼마든지 정보를 유출할 가능성이 있는 위협요인으로 상존하고 있다.

앞에서 언급한 여러 사례들을 보면 전·현직사원 또는 협력사 직원들이 실수 또는 고의에 의해 개인정보를 유출한 경우가 많음을 알 수 있고 특히 내부직원의 경우 업무를 위해 개인정보에 접근권한이 허용되어 있어 손쉽게 개인정보 접근하여 유출할 수 있었음을 알 수 있으며 그 유출의 범위 및 피해 규모도 해킹 등 외부자에 의한 경우에 비해 더욱 크다는 것을 알 수 있다.

3. 개인정보보호 기술의 현황

국내의 개인정보보호 기술은 아직 시작단계에 있으며, 개인정보보호에 특화된 기술개발보다는 기존 정보보호기술을 개인정보에 적용하는 수준에 머무르고 있다. 따라서 클라이언트 기반의 개인방화벽, 서버기반의 방화벽 및 VPN, 클라이언트/서버기반의 암호화 기반 기술 등이 개인정보보호를 위한 목적으로 적용되고 있고, 개인정보보호를 위한 전문기술이 개발된 사례로는 검색기술, 개인정보 인증기술, 홈페이지 개인정보 노출 검색 및 차단기술, 홈페이지 변조를 통한 스파이웨어 삽입 탐지 기술 등에 대한 사항이 진행되고 있다.

개인정보유출 방지를 위해 도입 사용되는 기술은 기존 내부정보유출방지 기술로 활용되고 있던 다음과 같은 기술들이 활용되고 있으며 개인정보유출방지만을 위해 개인정보 검출/삭제/암호화 기능을 제공하는 전문 솔루션도 개발되어 출시되고 있다.

3.1 통합PC보안 솔루션

통합PC보안의 대부분의 정보가 생성되고 가공되어지는 주체가 되는 내부직원이 사용하는 PC단말에 대한 보안을 통해 정보의 유출을 차단하는 솔루션이다. 상대적으로 보안이 잘 갖춰진 서버에 비해 개개인이 관리하는 PC의 경우 보안의 취약점을 보이고 있으며 또한 PC단말의 성능이 기하급수적으로 증가함에 따라 보안이 취약한 한 대의 PC를 통해서도 사내 전체 네

트웍을 마비시킬 수 있을 정도로 위험이 증가함에 따라 개개인의 PC에 대한 보안 적용이 필수적이며 국내외 개인정보유출사례에서 보듯이 내부자에 의한 정보유출의 경우 다양한 매체를 통해 더욱 손쉽게 이루어지고 그 피해가 상당함으로 보더라도 내부직원의 PC를 통한 정보유출을 차단할 수 있는 솔루션은 필수적이다.

통합PC보안솔루션은 PC 보안기능, 자산·시스템 관리기능, 패치관리기능, 정보유출방지기능(매체제어기능), 출력물 보안기능, 노트북반출기능이 유기적으로 결합돼 사용자에 의한 정보유출 위험성을 미연에 방지하는 솔루션이며 주요기능은 다음과 같다.

분류	세부기능
PC보안 기능	PC 접근 제어 기능 공유폴더 현황 및 접근로그 확인 Client Program 자체보호 기능 PC방화벽 기능 - Port, Protocol 별, Inbound / Outbound 차단 기능 - 중앙관리서버에서 설정한 정책을 사용자가 변경 불가 - 해킹탐지기능/웜 차단 기능, 알람 기능 - 임계치 설정에 의한 웜 차단 기능 특정 URL 차단기능
자산관리 기능	특정 프로그램 실행 통제 이벤트 관리 PC내 자원(S/W, H/W변경이력)관리 불법 S/W관리 기능 원격제어 기능 보안진단 패치관리 PC실명 관리
정보유출방지 기능	On-line을 통한 정보유출 제어 로그(SMTP/Telnet/FTP/웹메일/게시판) Off-Line을 통한 정보유출 제어로그 (FDD, CD-RW, USB, 모뎀, 각종 이동 저장 장치) 프린트 보안(출력물 보안) 화면보호기 기능(중앙관리자 시간 세팅) 제어판 / IP변경 / Proxy서버 금지 / 컨텐츠 업로드 차단 파일 암/복호화 기능 (선택적, 강제적) 노트북 반출 기능 / 외주용역 관리 NIC 제어 / 보안자가진단
중앙관리 기능	PC보안정책의 개별 및 일괄조정 기능 PC인터넷 사용로그 기능 통계 및 레포트 기능 알람 메시지 발송 및 실시간 명령 관리자 계정 관리 에이전트 업데이트 서버 상태 모니터링

3.2 보안USB 솔루션

2008년 주목 받았던 정보보호 솔루션인 보안USB 솔루션의 경우 국가정보원이 국가 공공기관들의 기밀유출 방지를 위해 발표한 "USB메모리 등 보조기억매체 보안관리 지침"에 의해 2008년 4월 의무화 시행 되고 있다. 공공기관에서 일반 USB메모리 대신 보안 USB 메모리를 사용하도록 하며, 보안 USB메모리의 필수 보안 기능으로 △사용자 식별·인증 △지정데이터 암·복호화 △저장된 자료의 임의복제 방지 △분실시 데이터 보호를 위한 삭제 등 4가지를 규정하고 있으며 이 규정에 따라 보안적합성 검증을 실시하고 있다. 보안USB솔루션은 안전한 정보이동 및 유출방지를 위해 만들어진 솔루션으로 기본적으로 모든 매체에 대해 통제하고 보안이 강화된 특별한 보안USB를 통해서만 자료를 반출할 수 있도록 하는 솔루션이다. 제공하는 기능은 다음과 같다.

분류	세부기능
사용자 식별/인증 기능	사용자 인증 및 매체 인증 없이 매체에 접근이 불가 인증 횟수 지정 및 인증 횟수 초과 시도에 대한 장치 사용 제어 보안 USB 사용 로그관리로 사용자 확인 가능
데이터 암복호화 기능	보안USB로 데이터 전송 시 데이터 자동 암호화 기능 보안USB로부터데이터 확인 시 자동 복호화 기능 USB내의 비밀문서는 매체 내에 암호화 되어 있음 지정 파일 암/복호화 기능 보안 USB사용 로그 관리
복제방지 기능	데이터 임의 복사 방지 기능 보안 USB 외부 별도 정책 관리/적용
파기 기능	분실된 보안USB 사용 제어 기능 (파일 완전삭제/사용 차단)
일반매체 통제 기능	보안USB외 PC매체 제어 기능(CD-RW, 시리얼/ 패러럴포트, 적외선포트, PDA, 무선랜 제어 등) 제공 PC매체 사용에 대한 로그 / 레포팅 기능 제공 일반 USB에 대해 읽기 기능만 제공(파일 쓰기 통제)

3.3 DRM 솔루션

DRM 솔루션은 정보 자체를 암호화하여 보안문서로 생성하며 이 보안문서에 대하여 접근 제어, 권한 관리 및 사용내역에 대한 로깅 기능을 기본으로 한다. DRM 솔루션은 문서의 생성시점부터 암호화하고 사용중에도 암호화를 유지함으로써 문서가 복사, 유출되더라도 해당 문서에 대한 사용권한(라이센스)을 획득하지 못하면 사용할 수 없도록 하여 정보유출을 차단한다. 세부적인 기능을 아래와 같다.

분류	세부기능
암복호화 기능	파일/폴더 암·복호화 - 파일, 폴더 대상 암·복호화 자동 암·복호화 - 파일 생성, 편집 저장 시 자동 암·복호화
사용권한 통제 기능	사용권한 통제 - 조직도에 따른 그룹/개인의 사용권한 제어 - 문서등급/사용자분류에 따른 사용권한 제어 편집/ 화면캡쳐 통제 - 문서편집기능(Copy&Paste, Screen Capture 등)을 통한 외부 유출 방지 프린트 통제 - 권한에 따른 출력 차단/마킹/로깅 보안폐기
사용내역 로깅 기능	조회/편집/복호화/출력/권한변경 행위에 대한 로깅 관리자의 정책 변경 로깅
중앙관리 기능	보안정책 관리 사용자 및 조직(그룹) 관리 로그 관리

3.4 DB보안 솔루션

DB에 대한 위협과 보안취약점은 다음과 같다. 첫째, 서버 관리자(또는 일반사용자)가 DB 접근권한을 오.남용하여 실제 업무와 연관되지 않은 데이터를 열람하거나 유출시키는 경우, 둘째, DB를 관리하는 관리자(또는 DB에 접속할 수 있는 사용자)의 아이디와 패스워드를 도용하여 데이터를 유출하는 경우, 셋째, 운영체제 및 DB관리시스템의 취약점을 고려한 해킹툴, 바이러스, 웜 등을 통하여 DB에 저장된 데이터를 유출하는 경우를 들 수 있으며 이를 효과적으로 방지하기 위한 솔루션이 DB보안 솔루션이다. DB보안 솔루션은 기존 DB관리시스템의 인증의 취약점을 보완하여 단순 아이디, 패스워드 기반의 인증에 사용자의 IP, MAC 및 기타 정보를 통해 사용자의 식별, 인증 기능을 보완하고 사용자별로 업무에 연관되지 않은 데이터를 열람할 수 없도록 query분석을 통해 권한을 벗어난 데이터에 대한 접근을 막는다. 더불어 보안강화를 위해 컬럼단위 암호화나 데이터 마스킹 기능을 제공하기도 한다. 최근에는 DB관리시스템을 만든 Oracle에서 자체적으로 암호화를 포함한 DB보안 기능을 제공하기도 한다.

분류	세부기능
접근제어 기능	사용자 IP/MAC/Host Name/DBMS계정/Application/일정기간/시간별 제어
권한제어 기능	SQL 분석을 통한 접근, 명령(create, drop, update) 제어
모니터링 및 이력관리 기능	사용자/세션별 접속이력 명령어와 결과값
기타 기능	컬럼 단위 암호화, 데이터마스킹, 결재기능

3.5 네트워크 발신통제 솔루션

네트워크 발신통제 솔루션은 기업 내부의 정보가 인터넷 등 네트워크를 통해 유출되는 것을 차단하기 위해 네트워크 유출 경로(이메일, 웹메일, 메신저 등) 및 각종 인터넷 자원 사용을 모니터링 함으로써 내부자에 의한 정보유출을 사전에 방지하고 자발적인 보안 업무를 유지하도록 유도하는 솔루션이다.

분류	세부기능
모니터링 기능	SMTP, POP3, HTTP, Telnet, FTP, NNTP, IMAP 등 다양한 프로토콜 분석 내용 저장 메일 본문내용, 첨부파일, 압축파일 모니터링 웹메일, 웹게시판 모니터링
검색 기능	키워드, 사용자 정의, 규칙 설정, 패턴 매칭 검색 등 다양한 검색 첨부파일에 대한 내용 검색
통계 기능	사용자 정의에 의한 상세 조건 리포트 기능 예약통계, 요약통계 등 다양한 통계방법 제공 다양한 포맷의 통계결과 저장 기능

3.6 프린트 보안 솔루션

프린트 보안 솔루션은 기업 내부의 출력 시스템을 원격으로 통제/관리감독을 할 수 있는 솔루션이다. 기업내부에 연결된 PC에서 인쇄되는 모든 내용(사용자, IP, 인쇄매수, 인쇄원본)에 대해 로깅을 남기고 각각의 내/외부에 연결된 프린터 및 모든 PC를 중앙에서 통제/관리함으로써 기업의 인쇄 시스템 관리를 일괄적으로 관리감독 하고 통제가 가능한 솔루션이다.

분류	세부기능
출력통제 워터마크 삽입	그룹/사용자/어플리케이션/프린터/IP대역별 출력권한 제어 워터마크 삽입(Visible/Invisible) 인식표 삽입 출력된 문서에 바코드를 인쇄하여 저장된 Log를 손쉽게 검색
출력이력 로그	출력 이력로그 및 출력사본(내용)/텍스트 추출 저장 기능 Offline에서 인쇄시 Log관리
기타	Log 통계관리 - 개인/부서/전체/프린터별 출력물을 통계 처리 - 인쇄 업무를 관리하고 비용을 절감 효과

3.7 개인정보 검출/삭제/암호화 솔루션

개인정보 검출/삭제/암호화 솔루션은 기업의 업무

상 개인정보가 개개인의 PC에 흩어져서 활용되고 있고 이런 현황을 개인정보관리자가 파악할 수조차 없는 점을 고려하여 만들어진 솔루션이라고 할 수 있다. 각 PC에 흩어져 있는 개인정보 파일을 검출해서 중앙관리서버에 보고하고 관리정책에의해 개인정보가 포함된 파일을 강제 삭제하거나 암호화하여 개인정보의 유출을 차단하는 솔루션이며 제공 기능은 아래와 같다.

분류	세부기능
개인정보 보관 검출	기본 검색 패턴 및 사용자 정의 검색 패턴을 상용한 개인정보 포함 파일 검출 검사대상 설정 - 사용자/부서에 대한 검출 정책을 부여 검사조건 설정 - 문서파일/사용자 정의 확장자/압축 파일/하위 폴더/검색 대상 제외/빠른 검사
패턴추가 및 편집기능	기본 패턴 - 주민 번호, 계좌 번호, 카드 번호, 전화번호, 핸드폰 번호, 여권번호 등 사용자 지정 패턴 - 정규식으로 표현하여 새로운 패턴을 추가 가능 관리자 정책에 의한 지정 패턴 관리자 정책에 의한 예약 검색 설정
강제삭제 강제 암호화	관리정책에 의한 강제 삭제, 암호화 기능 사용자 선택에 의한 삭제, 암호화 기능
로그조회 통계	사용자 및 관리자 지정 검색 패턴에 대한 결과 리포팅 - 검색을 통한 결과를 그래프로 표현 - HTML, EXCEL 형식으로 출력 위험인물, 위험부서 관리

4. 기존 개인정보보호 기술의 문제점

각각의 솔루션들이 나름대로의 영역에서 정보유출을 차단하고 보안을 점검해주는 기능을 제공하지만 각각의 제품은 독자적으로는 정보유출을 100% 차단하지는 못하고 있다. 각 솔루션의 한계점에 대해서 살펴보도록 하겠다.

통합PC보안 솔루션의 경우 패치관리 및 보안점검을 통해 PC자체의 전반적인 보안을 강화하고 PC자체에 대한 접근 제어, 공유폴더 접근제어, 개인방화벽 및 온라인, 오프라인 매체들에 대한 허용/차단의 권한 제어를 통해 정보유출을 차단하고 정보의 흐름을 로깅하는 기능을 제공하지만 해당 기능에 대한 제어가 정보 자체의 중요성(개인정보 포함여부 등)에 의한 것이 아니라 PC를 사용하고 있는 사용자의 권한 또는 PC자체에 대한 권한 설정으로 단순히 차단 또는 허용을 설정하여 제어함에 따라 업무에 불편을 초래하게 된다. 따라서 실제 업무를 위해서 하나의 매체 이상을 허용하게 되며 이 경우 허용된 매체를 통해서는 모든 자료가 유출될 수 있는 문제가 발생한다.

보안USB 솔루션의 경우도 통합PC보안과 마찬가지로 기본적으로 매체에 대한 차단/허용을 기반으로 정보유출을 차단하는 솔루션이므로 통합PC보안 솔루션과 마찬가지로 사용자별 매체에 대한 사용권한을 제어하므로 매체에 대한 사용권한이 있는 사용자를 통한 유출을 차단할 수는 없다.

DRM솔루션의 경우 문서생성 시점부터 암호화를 통해 문서 유출시 에도 문서를 열어볼 수 없도록 하여 정보유출방지 기능을 제공하고 있으나 문서보안에서 지원하는 문서포맷이 한정되어 있으며 또한 해당 문서포맷을 지원하는 어플리케이션의 버전이 변경될 때마다 DRM솔루션의 에이전트가 변경되어야 하는 문제점을 가지고 있다. 즉 사용자가 악의적 목적으로 개인정보를 유출하고자 할때 DRM솔루션에서 지원하지 않는 어플리케이션을 통해 문서를 작성하여 저장하는 경우 암호화 및 제어를 벗어나 정보유출이 가능하며 문서를 암호화하고 권한을 부여할 때 문서의 내용에 기반을 두어 권한을 부여하는 것이 아니라 문서 생성자에 의해 권한이 부여되거나 생성자가 속한 부서, 직급, 직책 등 사용자 분류에 따라 권한이 부여되므로 개인정보가 많이 포함된 중요 문서임에도 불구하고 낮은 권한의 사용자가 열람하거나 인쇄할 수 있는 권한이 부여되는 등의 문제점을 가지고 있으며 DRM솔루션이 도입되지 않은 외부 관계사와 업무를 공유하기 위해서는 해당 문서를 복호화해서 전달해야 하므로 일부 사용자에게는 복호화 권한을 부여하게 되며 복호화 권한을 가진 사용자에 의해서 복호화되어 유출되는 문서에 개인정보 등 중요한 정보가 포함된 경우에도 확인없이 유출될 수 있다. DB보안 솔루션의 경우 개인정보가 저장되어 있는 데이터베이스에 대한 접근제어, 쿼리 실행권한 제어, 데이터베이스 내에 저장된 데이터에 대한 암호화 및 로깅 기능을 제공하고 더불어 접근이 허용된 사용자가 업무에 필요한 최소한의 데이터에만 접근하도록 제한하여 보안을 강화시켜주는 기능을 제공하지만 업무 수행자가 실제 데이터베이스가 설치된 서버에서 업무를 수행하는 것이 아니라 데이터베이스에 접근가능한 사용자가 PC를 통해 접근하고 PC로 데이터가 이동된 이후에는 해당 데이터를 여러 가지 방법으로 파일형태로

작성하여 유출시킬 경우 쉽게 유출 가능한 한계를 가지고 있다.

네트워크 발신통제 솔루션의 경우 네트워크 단에 설치되어 이동되는 데이터를 패킷 레벨에서 다양한 네트워크 프로토콜을 분석하여 메일, 메신저, 웹게시판을 통해 전송되는 데이터를 관리자가 설정한 키워드, 패턴매칭 검색을 통해 본문 및 첨부파일의 내용을 검사하여 중요정보가 유출되는 것을 차단하는 기능을 제공하지만 근본적으로 발신통제 솔루션이 적용된 네트워크만을 감시하게 되므로 이동성을 갖춘 PC 또는 노트북을 사외로 유출하는 경우, 다양한 이동형 저장장치를 통한 유출, 감시대상이 아닌 무선통신을 통하는 경우 등 다양한 우회경로를 통해 데이터가 유출되는 것을 막을 수 없는 한계점을 가지고 있다.

프린터 보안의 경우 출력을 통한 유출만을 제어하는 솔루션이므로 단지 출력을 통한 정보 유출을 제어하거나 출력물을 통한 유출 사고 발생 시 사후 추적의 기능만 제공할 뿐이다.

개인정보 검출/삭제/암호화 솔루션의 경우 각 PC에 흩어져 있는 개인정보를 검출하여 현황을 파악하고 삭제 및 암호화를 수행할 수는 있으나 업무를 위해 사용하는 개인정보를 포함한 파일이 온라인, 오프라인 경로를 통해 유출되는 것을 실시간으로 탐지하고 차단할 수 있는 기능을 제공하지 못하고 있어 개인정보 유출 차단 솔루션으로서는 한계를 가지고 있다.

이와 같이 기존 제품의 한계점을 요약해서 정리하면 각자 자신의 솔루션이 보안할 수 있는 영역이 제한적이라 우회경로를 통한 유출이 가능하다는 점과 내용 검사를 기반으로 데이터를 통제하는 것이 아니라 사용자의 분류에 의해 각종 매체를 차단하거 문서에 대해 강제 암호화를 통하여 정보 유출을 차단함으로써 기존 업무환경을 변화시키거나 또는 유출되지 않아야 할 정보는 유출되는 반면 보안이 중요하지 않은 정보의 활용에도 자유롭지 못하게 하는 영향을 미치고 있다.

5. 향후 개인정보보호 기술의 방향

개인정보는 기업의 입장에서는 상품이나 서비스 등에 대한 정보를 더 많이 고객에게 전달하고, 그에 대한 고객의 문의사항이나 요구사항 등을 보다 빠르고 편리하게 응대하여 고객을 만족시키고 더 나아가 향후의 신상품이나 서비스 등에서도 자사의 상품이나 서비스를 이용토록 하는 영구고객화 전략 등을 위해서는 최대한 활용하여야 하는 중요한 정보임과 동시에 유출 시에는 기업에 경제적 피해와 신뢰성에 엄청난 피해를 야기하고 또한 강화되고 있는 개인정보보호와 관련된 법규를 지켜야하는 복잡한 문제이다. 따라서 기업 입장에서는 업무에 활용하는데 지장을 주지 않으면서도 내부자에 의해 고의 또는 실수로 개인정보가 유출되는 것을 효과적으로 막을 수 있는 솔루션이 필요하게 되었다. 즉 최대한 개인정보를 활용할 수 있도록 허용하되 유출이 의심되는 경우에는 차단하여 유출되지 않도록 하기 위해서는 단순히 사용자 분류를 기반으로 하는 매체제어, 암호화 만으로는 최대한 활용과 보안의 두가지 효과를 거둘 수 없다.

따라서 데이터의 내용 검출(컨텐트 인스펙션)을 기반으로 데이터의 이용 중 또는 이동 중에 내용검사를 기반으로 로깅, 경고, 암호화, 차단 등 여러 액션을 통해 정보 유출을 차단할 수 있는 기술이 필요하게 되었고 이를 DLP(Data Loss Prevention or Data Leakage Prevention)이라고 정의하고 있다. DLP라는 용어는 불과 몇 년 전부터 해외에서 사용되기 시작하였지만 국내의 경우 이미 오래 전부터 컨텐트 보안이라는 이름으로 여러 솔루션들이 출시되었고 내부정보유출방지솔루션 또는 개인정보보호 솔루션으로 불려왔다. 해외의 경우 기존 대형 보안업체들이 DLP 솔루션 벤더를 M&A하는 경향이 두르러 졌다. EMC는 Tablus를, McAfee는 Onigma를, Symmantec은 Vontu를, 그리고 최근에는 CA가 Orchestria를 합병하는 등 활발한 M&A가 이루어졌는데 이는 두 가지 측면에서 시사점을 가진다. 하나는 엔드포인트 솔루션 벤더들이 DLP솔루션을 확보함으로써 통합적인 DLP솔루션을 확보하려 한다 할 수 있다. 또한 기존의 방화벽, IPS, IDC업체들이 통합적인 네트워크 보안 솔루션을 지향하는 움직임으로도 볼 수 있다. 국내의 경우에도 기존 내부정보유출 솔루션의 한계점을 극복하기 위해서 여러 정보보안업체들이 협력을 하거나 자신이 가지고 있는 솔루션의 영역을 확장해 나가고 있는 추세이다. 최근 언론에 보도된 내용에 따르면 국내 DRM 3사의 경우도 DRM의 암호화 기술에 DLP의 중요 데이터 감사 기술을 도입하여 융합시킴으로써 한층 강화된 내부정보유출방지 솔루션을 제공할 것이라고 발표하고 있다.

그럼, 개인정보보호 솔루션의 요구사항을 정리하면 다음과 같이 볼 수 있다.

1) 개인정보의 보유현황 조사, 분석
   서버 및 PC에 저장된 파일을 다각도로 검색하여 결과 제공

개인정보 파일의 보유현황에 따른 위험인물/위험부서 정보 제공
개인정보가 포함된 주요 파일에 대한 암/복호화 및 완전삭제 기능 제공

2) 개인정보 유출시 실시간 차단, 경보
온라인 또는 오프라인 경로에 의한 각종 유출 시 내용을 기반으로 실시간 차단 및 경보
사용자가 개인정보가 포함된 파일을 유출 시도 시 적법한 절차를 통할 수 있도록 유도

3) 개인정보 변경, 반출 추적
개인정보 파일의 추가, 삭제, 변경, 반출 등의 감시, 추적

4) 개인정보 보호정책 설정
개인정보 보유현황, 반출회수 등에 대한 사용자별 개인정보 관련 행위 분석 자료를 참조하여 개인정보보호 정책을 효율적으로 설정, 관리

6. 결 론

대다수 기업이 외부로부터의 공격이나 악의적인 내부 직원, 잘못된 비즈니스 프로세스, 단순한 실수와 같은 위협요소로부터 기업의 주요 정보를 보다 안전하게 보호하기 위해 다양한 보안 툴과 기술을 이용하고 있다. 그러나 네트워크 보호나 정보 이용 제한을 목적으로 하는 기존 보안 솔루션의 경우 정보가 어디에 저장돼 있으며 어떻게 이용되는지, 손실방지를 위한 최선의 방법은 무엇인지 등의 근본적인 질문에 대한 해답을 갖고 있지 않다. 따라서 이 같은 질문에 해답을 제시하고 보다 효과적인 정보보호를 위해 DLP, 즉 데이터 손실 방지 솔루션이 등장했으며, 경제위기와 함께 정보유출로 인한 기업의 금전적·사업적 피해가 커지는 상황에서 이 솔루션에 대한 관심이 갈수록 증대되고 있다. 이제 기업은 비즈니스의 새로운 위협으로 떠오르는 개인정보 유출을 방지하고 기업의 기밀 데이터를 검색, 모니터링해 포괄적인 보호방안을 제공할 수 있는 전략적인 솔루션이 필요하게 되었다.

이를 위해서는 기존 내부정보유출방지 솔루션들의 한계점인 사용자 기반 네트워크, 다양한 매체에 대한 단순한 허용, 차단을 통한 통제의 방법에서 벗어나 데이터의 내용 검출을 기반으로 데이터의 이용 중 또는 이동 중에 내용검사를 기반를 통해 로깅, 경고, 암호화, 차단 등 여러 액션을 통해 정보 유출을 차단할 수 있는 기술이 필요하게 되었으며 이를 위해 기존 내부정보유출방지 솔루션 업체들은 각자가 가진 기반기술에 모자란 부분을 보강하여 DLP제품으로 발전해 나가는 모습을 보여주고 있다.

참고문헌

[1] "공공기관의 개인정보에 관한 법률", 법률 제8871호, 제2조, 제2호, 2008.2.29

[2] "정보통신망 이용촉진 및 정보보호 등에 관한 법률", 법률 제8778호, 제2조, 제6호, 2007.12.21

[3] "초고속인터넷서비스 영업망에서의 개인정보 침해 개선을 위한 소고", KISA

[4] 중앙일보 보도자료, http://article.joins.com/article/article.asp?total_id=3293075, 2008. 9

[5] 국가정보원 (2007. 2.). "첨단 산업기술 보호동향" (제7호).

[6] 삼성경제연구소, SERI 경영 노트, 제 10호, 2009. 6. 11, 4page-7page

[7] 박문석, 사이버공간에서의 프라이버시권에 관한 비교법적 연구, 2009. 2

[8] 권영관, 컨택센터에서의 고객의 개인정보 보호 모델, 2009. 2

[9] 박병호, 유비쿼터스 사회에서의 개인정보보호에 대한 기술적인 접근 연구, 2008. 2

[10] 송지훈, 내부정보유출 방지 솔루션 보안성 평가, 2009. 9

김 상 진

1996 성균관대학교 물리학 학사
1999 성균관대학교 컴퓨터공학 석사
2008 소프트캠프(주) 연구소장
문서보안, 도면보안 솔루션 개발
현재 닉스테크(주) 연구소장
통합PC보안, 보안USB, 개인정보보호 솔루션 개발

E-mail : sjkim@nicstech.com