情 報 保 護 學 會 誌
第21卷 第5號, 2011. 8

정보유출방지와 프라이버시 침해에 대한 고찰

김 진 형*, 김 형 종**

요 약

네트워크 등의 환경에서 정보의 사용 범위가 확대됨에 따라, PC 및 다기능의 단말 등을 사용하여 내부 정보에 접근 가능하도록 하는 기능적 요구가 확대되고 있다. 그러나 이러한 요구에 따라 내부 정보 접근이 용이 해 지면서 내부 정보 유출의 가능성이 증가 하게 되었다. 실제로 최근 발생한 정보유출 사건들은 단순 정보유출이나 일회성 공격에 지나지 않고, 자산의 유출로 인해 기업의 존폐를 흔들 만큼 그 영향이 커지고 있다. 이러한 정보유출사고 발생이 증가함에 따라 정보를 취급하는 정부기관 및 기업은 이를 막기 위하여, 정보유출방지시스템을 운영한다. 그러나 정보유출을 방지하기 위한 솔루션이 확인 하는 데이터에는 정보유출방지시스템에 연결되어있는 사용자들의 개인정보가 포함되어있다. 개인의 프라이버시는 어떠한 경우에서도 반드시 보호되어야 한다는 관점으로 볼 때, 정보유출탐지시스템 설계 시 사용자들의 프라이버시 보호가 가능한 솔루션이 필요한 상황이라고 볼 수 있다. 본고에서는 정보유출 방지를 위한 기술이 갖는 프라이버시 침해 관계에 대해 살펴보고, 이를 막기 위한 요소기술들을 제시하고자 한다. 본고는 정보유출과 개인정보보호에 대한 상관관계 분석에 대한 연구 내용을 요약하는 형태로 작성되었다.

Ⅰ. 서 론

2011년도 상반기에는 개인정보가 유출되는 주목할 만한 사건이 여러 건 발생하였다. 예전에 발생 했던 인터넷 포털 사이트 메일시스템에서의 개인정보유출사건(55만 명), 1000만 명 이상의 회원정보가 유출된 쇼핑몰 사건, 고객 600만 명의 개인정보를 텔레마케팅업체에게 유출시킨 텔레콤 업체 사건들은 기업의 정보를 유출시키거나 획득하기 위한 공격에 의한 것이었다. 비록, 정보통신 기술의 발달 등으로 전자 거래와 같은 개인정보를 활용하는 전자적 활동 영역이 넓어지면서, 정부 및 기업의 개인정보의 수집 및 보관이 의무화 되는 분위기 속에서 오히려 정보 관리자 또는 취급자에 의한 정보유출 발생 가능성은 매우 높을 것으로 미리 예상되었으나, 내부 시스템 구축 시 이러한 점을 간과하였기에 공격뿐 아니라 내부자의 정보유출 사건이 발생하게 되었다[5].

이러한 사건에 대한 대응책으로 정보를 수집하고 보관 하는 정부 및 기업은 정보유출방지시스템을 도입하여 운영한다. 개인정보 수집 시 정보 제공 및 보관에 대한 개인의 동의를 받은 경우를 제외한 무분별한 개인정보 수집을 막기 위해 정보유출방지시스템을 운영해야할 필요성이 증가하였다. 특히 민감한 개인정보의 경우, 정부 기관에서의 신원 조사 및 기타 확인 사항을 위한 검색, 또는 기업의 마케팅 등의 경제적 이유 등에, 개인의 동의와 함께 정당하게 제공되는 경우 이외의 상황은 불법적인 제공으로 인한 개인정보의 유출로 판단하고, 이러한 솔루션을 통해 개인정보유출 시도를 차단하는 방법을 적용 한다. 정보유출방지시스템에서는 패킷 내 포함되어있는 개인정보를 삭제 하거나 개인정보가 포함되어있는 네트워크 패킷을 차단하는 방법 등으로 정보유출을 방지한다. 비단 개인정보 뿐 아니라 내부 중요정보 또한 유출되면 안 되는 정보이므로 이러한 외부로의 정보 이동에 대한 차단 기술이 필요하게 되었다.

정보를 취급하는 정부 기관 및 기업은, 더욱 강력한 정보유출탐지를 위해 내부와 통신하는 모든 패킷을 모

본고는 2009년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구과제 "프라이버시를 보장하는 정보유출탐지 기술 연구"(2009-0068361)의 결과 논문들을 요약한 내용을 담고 있음

* 서울여자대학교 정보미디어대학 정보보호학과 (jinny@swu.ac.kr)
** 서울여자대학교 정보미디어대학 정보보호학과 (hkim@swu.ac.kr)

니터링 하고자 한다. 그러나 이러한 과정에서 모든 패킷의 내용을 확인 하는 행위 및 내부정보 유출을 막기 위해 제시되고 있는 기술들은 정보유출방지시스템과 연결되어 있는 직원들의 프라이버시 침해의 위험을 가지고 있다. 필요한 영역의 모니터링 이외의 직원의 개인 정보를 무분별하게 확인 하는 상황이 발생할 수 있다. 본고에서는 이와 같은 정보유출 방지를 위한 기술이 갖는 프라이버시 침해에 대해 살펴보고, 이를 막기 위한 요소기술들을 제시하고자 한다. 특히, 본고는 저자들의 최근 정보유출과 개인정보보호에 대한 상관관계 분석 연구 내용을 요약하는 형태로 작성되었다.

Ⅱ. 정보유출방지와 프라이버시

2.1 정보유출방지 기술을 반영한 시스템

정보유출방지(DLP: Data Leakage Prevention)시스템은 기업에서 보관하고 있는 중요정보에 대한 정보의 흐름을 효과적으로 관리하기 위해 운영하는 시스템이다. 이러한 시스템은 기업의 목적에 맞추어 수립하고 운영하는 보안 정책에 따라, 보관하고 있는 정보에 적용하여 중요 자산을 보호하고자 사용하는 것이다[5]. 정부기관 및 기업은 자산의 보호를 위해 내부 네트워크 환경에서의 이동 중인 데이터, 저장 형태로 보관되어있는 데이터에 대해 외부로의 유출 방지 목적을 가지고 이러한 시스템을 운영한다. 정보유출방지시스템은 내부에서 외부로 이동하는 네트워크 패킷을 기관 내 정의되어있는 보안 정책에 따라 모니터링 하여 외부로 나가는 패킷에 대한 차단 또는 중요정보를 포함하고 있는 패킷 중에서 중요정보를 임의로 삭제 하는 방법을 사용한다. 또한 온라인을 통한 파일 등의 정보유출방지기능 뿐 아니라, 이동저장장치 또는 프린터 등의 매체를 통한 유출 시도에 대해서도 모니터링을 수행한다. 네트워크 로그데이터 분석을 통해 사후 유출탐지 기능도 수행하게 되는데 이러한 이유로 정보유출탐지시스템이라고도 불린다[3].

2.2 개인정보 정의 및 보호의 중요성

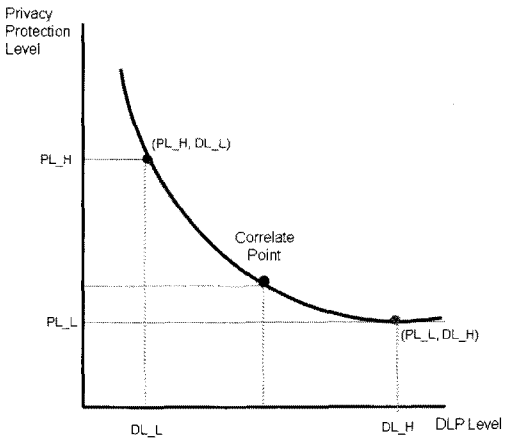
국내 몇 가지 법률에서는 개인정보를 다음과 같이 정의 하고 있다. 정보통신망이용촉진 및 정보보호등에관한법률과 개인정보보호법에서는 생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호, 문자, 음성, 음향 및 영상 등의 정보라고 정의한다. 이러한 개인정보는 어떠한 경우에도 보호 되어야 하고 이러한 정보의 사용은 통제되어야 한다. 또한, 개인이나 조직의 권리, 개인이나 조직이 소유하는 자료, 개인이나 조직에 관한 정보는 허가 없이 타인에게 수집되어 사용되면 안 된다. 조직에 속하는 개인 신상정보는 인사나 고용, 작업, 서비스 등과 관련이 없는 다른 개인이나 조직 사이에서 부당하게 수집, 배포되거나 사용되면 안 된다. 그러나 정보유출방지시스템을 통한 내부 정보 유출 방지를 위한 모니터링 과정 중 이러한 정보에 접근할 수 있는 권한이 없는 시스템 관리자들이 정보를 수집 및 접근하게 되어 직원의 프라이버시 침해가 발생할 수 있다.

Ⅲ. 프라이버시를 보호하는 정보유출방지

본 장에서는 프라이버시와 정보유출탐지 사이의 관계를 보고 프라이버시를 보호하는 정보유출방지 기술에 대해 소개 하고자 한다.

3.1 정보유출탐지 과정에서 발생 가능한 개인정보 침해 (Trade-off관계)

정보유출에 대한 탐지수준 및 프라이버시의 보호 수준은 아래 [그림 1]과 같이 Trade-off 관계를 갖는다.

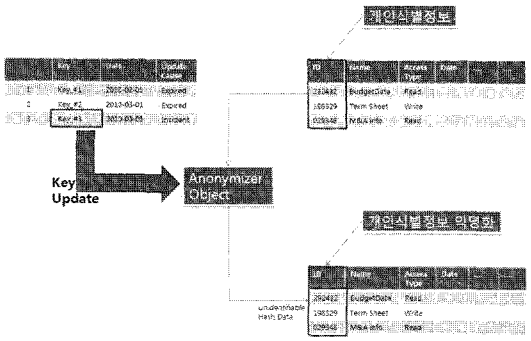


〔그림 1〕 프라이버시보호와 정보유출탐지등급의 상관관계(2)

현재 대부분의 기업들은 정보유출 탐지수준을 최고로 높이는 방향으로 정책을 가져가고 있으나, 이는 내부

직원의 프라이버시의 침해를 가져오고 있다. 적절한 합의점을 찾는 문제는 단순히 위의 [그림 1]에서의 중앙점을 찾는 데에 있지 않고, 기업의 업무의 특성과 다루는 정보의 유형에 따라 정책적으로 결정된다. 본 연구진이 제시하는 지수화 된 상관관계 모델[1][3]은 정보유출탐지 수준을 정했을 때 해당 수준이 갖는 프라이버시 침해 정도의 추상적 지수와 함께, 구체적인 침해 데이터를 제시하는 것을 목표로 한다.

3.2 정보유출탐지 과정에서 프라이버시 보호 가능한 익명화 방안



〔그림 2〕 개인식별정보 익명화 프로세스〔2〕

정보유출탐지 과정에서 발생하는 프라이버시 침해에 대해 이를 막기 위한 요소기술이 있다. 정보유출방지시스템이 확인 하는 데이터 중 민감한 데이터 또는 개인식별 데이터에 대해 익명화 하여 보관 하는 것이다. 원래 익명화 기술은 로그의 장기적인 보관 또는 로그정보를 외부에 전달하고자 할 때 개인 또는 기관이 식별할 수 없도록 하기 위한 기술적 접근이었으나, 이러한 기술을 프라이버시 보호에 적용할 수 있다[2][7]. 익명화 방법은 크게 개인식별정보에 대한 삭제와 해쉬함수를 활용한 난독화 방법을 사용할 수 있다. [그림 2]와 같이 향후 행위자 추적이 가능한 개인식별정보의 난독화 방법을 적용하여 개인식별정보를 익명화할 수 있다.

익명화를 위한 난독화 기법에 해쉬 함수를 선정 및 키 관리 방법을 정의 하여야 한다. 난독화 기술을 적용하기 위해 해쉬 함수에 사용되는 여러 가지 암호기술 중 간편하고도 안전한 기술을 선정 하여야 하며, 효율적이고 개인 식별이 좀 더 어렵게 하기 위한 키 관리 방안을 제시하여야 한다. 특히 키의 경우, 주기적으로 일정시간이 지나면 폐기 변경 되도록 정의 되어야 하며, 특정한 사고가 발생한 경우 키는 반드시 갱신되어야 한다[8].

3.3 정보유출방지시스템에서 개인정보보호와 정보유출탐지 정도의 조절 기준을 지수로 제시

앞의 3.1장에서 정보유출탐지시 적용되는 탐지 강도가 프라이버시 침해를 가져올 수 있으며, 이들 사이에 Trade-off 관계가 있음을 제시하였다. 여기서는 간단한 예시를 통해 어떤 형태로 이러한 관계가 나타날 수 있는 지를 살펴보고자 한다.

〔표 1〕 시나리오 예시〔1〕

<시나리오>

A회사에서 정보유출방지시스템을 사용하여 Bob이라는 사원의 email발송에 대한 모니터링을 수행한다.

1. Bob(bob@mail.com)이 Alice(alice@host.com)에게 메일을 보낼 때의 패킷을 캡처하여 모니터링을 수행하고자 한다.
2. 캡처한 패킷 중 Email과 관련된 패킷의 모니터링을 시작한다.
3. 내부정보유출 방법으로 가장 많이 사용 되는 방법은 첨부파일에 기밀문서를 첨부하는 형태이므로, 기본적으로 헤더의 내용은 확인 하고, 본문의 내용은 확인하지 않더라도, 첨부 파일의 내용은 열어서 확인한다.
4. 모니터링 수행 시 확인 한 내용을 위에서 제시한 모델에 따라 정리 하여 점수를 계산 해 본다.

확인 Data	*확인*	*10개*
총 15개 중	*미확인*	*5개*

본 장에서는 3.2장에서 제시한 익명화 기술을 적용하지 않고 단순히 정보를 확인 하는 것에 대한 지수화에 대해 정의 해 보고 [표 1]과 같은 시나리오를 통해 확인해보고자 한다.

정보유출탐지를 위해 정보를 확인 한다면, 정보유출을 탐지하는 측면에서의 데이터의 등급이 높은 등급이 나오게 된다. 그러나 프라이버시 보호 측면에서는 정보를 확인 한 것이며, 데이터 보호 등급은 낮게 나오게 된다. 즉, 정보유출탐지시스템의 하나의 행위에 DLP와 프라이버시 보호 등급은 반비례 관계가 성립 된다[1][4].

[표 1]의 예시는 [1]에서 이미 분석 제시한 것과 같이 총 15개의 정보 중에서 정보유출탐지를 위해 10개의 정보를 확인 하였다. 가중치 없이 확인하는 정보의 개수를 기준으로 비율을 계산해 본다면, 정보유출탐지 측면에

서는 0.67이라는 값을 계산할 수 있으며, 프라이버시 보호 측면에서는 0.33이라는 값을 계산할 수 있다. 위의 경우는 정보유출탐지 측면에 더 비중을 둔 경우로 볼 수 있다. 이러한 단순한 상관관계뿐만 아니라, 좀 더 자세한 상관관계 예시는 본고의 참고문헌들에 제시되어 있다.

Ⅳ. 결 론

본고에서는 내부정보유출을 막기 위해 운영되고 있는 정보유출방지시스템을 통해 시스템 관리자들이 직원들의 행위 정보를 확인하게 됨으로써 시스템에 연결되어있는 직원들의 프라이버시 침해가 발생 한다는 문제 제기를 하였다. 이에 대한 대응 방안으로 프라이버시를 보호하면서 정보유출방지가 가능 하도록 익명화 기술 중 정보유출방지 솔루션이 확인 하는 정보에 난독화 기법을 활용하여 개인 식별정보를 보호 하는 방안을 제안하였고, 정보유출방지시스템의 결과를 지수로 산출 하여 정보유출탐지 정도와 프라이버시 보호의 수준에 대한 비교 및 적정 수준 확보 방안을 제시한 기존 연구 내용 중 일부를 소개 하였다.

이러한 방안을 활용하여 구현한 정보유출방지시스템에 정보보호에 대한 정책을 정의 한다면 일정 수준의 자산의 보호와 직원에 대한 프라이버시 보호가 가능하다고 판단된다.

참고문헌

[1] J. H. Kim and H. J. Kim, "The Data Modeling considered Correlation of Information Leakage Detection and Privacy Violation," ACIIDS 2011 : 3rd Asian Conference on Intelligent Information and Database Systems, LNAI 6592, pp. 165-170

[2] J. H. Kim and H. J. Kim, "A Study on Privacy Preserving Data Leakage Prevention System," DEIT 2011 : International Conference on Data Engineering and Internet Technology, 2011. 03.

[3] J. H. Kim and H. J. Kim, "Design of Internal Information Leakage Detection System Considering the Privacy Violation," ICTC 2010 : International Conference on ICT Convergence, 2010. 11.

[4] J. H. Kim, H. J. Kim et al., "A Knowledge Representation for Personal Information Leakage Scoring System," ISIS 2009 : 10th International Symposium Advanced Intelligent System, Aug, 2009.

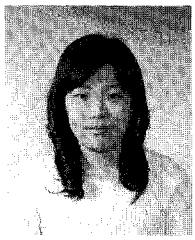
[5] 김진형, 김형종 외 3인, "프라이버시 침해 및 보호 상관관계 모델 연구," 보안공학연구논문지, Vol. 8, No. 2, pp.215-226, 2011.04

[6] Jason (Seok In) Jung, 김형종 외 1인, "Adjusting The Circumstance Between Levels of Protection of Internal Information and Employees' Privacy," 2010 한국인터넷정보학회 추계학술대회, pp63-64 , 2010. 10.

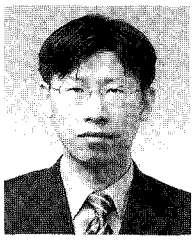
[7] 김진형, 김형종 외 2인, "프라이버시를 보호하기 위한 요소 기술 연구", 2010 한국인터넷정보학회 추계학술대회, 2010. 10.

[8] 김진형, 김형종, "개인정보 데이터 접근 비정상행위 탐지 기법을 활용한 개인정보 보호 기법 연구," 정보과학회지, 27(12), pp.60-67, 2009. 12.

〈著者紹介〉



김 진 형 (Jinhyung Kim)
학생회원
2006년 2월 : 서울여자대학교 정보보호공학과 공학사
2008년 2월 : 서울여자대학교 대학원 컴퓨터학과 이학석사
2008년 3월 ~ 현재: 서울여자대학교 대학원 컴퓨터학과 박사과정
관심분야 : 개인정보보호, 클라우드 컴퓨팅 보안



김 형 종 (Hyung-Jong Kim)
종신회원
1996년 2월 : 성균관대학교 정보공학과 공학사
1998년 2월 : 성균관대학교 정보공학과 공학석사
2001년 2월 : 성균관대학교 전기전자 및 컴퓨터공학과 공학박사
2001년 ~ 2007년 : 한국정보보호진흥원 수석연구원
2004년 ~ 2006년 : 미국 카네기멜론대학 CyLab Visiting Scholar
2007년 3월 ~ 현재 : 서울여자대학교 정보보호학과 조교수
관심분야 : 인터넷전화 보안, 취약점 분석 및 모델링, 이산사건 시뮬레이션 방법론, 개인정보보호