情報保護學會論文誌
第 22 卷 第 2 號, 2012. 4

개인정보 오·남용 방지 및 보호를 위한 정보공유센터 프레임워크

고 유 미,† 최 재 원, 김 범 수‡
연세대학교 정보대학원

Protecting Individuals from Secondary Privacy Loss using Breached Personal Data Information Center

Yumi Ko,† Jaewon Choi, Beomsoo Kim‡
Graduate School of Information, Yonsei University

요 약

최근 빈번히 발생하고 있는 개인정보 유출사고로 인하여 사회적으로 개인정보보호 관리에 대한 경각심이 높아지고 있다. 본 연구는 개인정보 유출 사고 시, 개인정보 오·남용으로 발생할 수 있는 2차 피해를 적극적으로 방지할 수 있는 체계를 제안한다. 특히, 유출된 개인정보 데이터베이스를 공유 및 관리할 수 있는 개인정보 공유분석센터의 체계와 역할에 집중하였다. 공유된 개인정보 데이터베이스는 유출된 기업과 유사한 산업군에 있는 기업들이 보다 높게 활용할 수 있고 이를 통하여 동일한 ID와 패스워드를 사용하는 이용자들에게 적절한 정보보호 조치를 취할 수 있다. 개인정보 공유분석센터는 개인정보 데이터베이스 제공에 있어 유출된 기업의 자발적 또는 의무적 제공과 서비스 형태에 따라 그 효과가 달라질 수 있다. 개인정보 데이터베이스를 의무적으로 제공하고 센터가 적극적으로 매칭 서비스를 제공할 때, 단일 채널화된 데이터베이스의 구축 및 매칭 기술 활용 가능으로 매칭 정확도가 상승할 수 있고, 질 높은 서비스를 통하여 2차 개인정보 오남용의 피해 축소와 효과적인 관리 지원이 가능하다.

ABSTRACT

This study focused on the role of the center for private information, which can manage and share the personal data from data breach incidents. Especially, this study addresses on the importance of establishing information management systems for preventing secondary misappropriation of breached personal data and private information. The database of breached personal data can be used for reducing privacy worries of potential victims of secondary misuse of personal data. Individuals who use the same IDs and passwords on multiple websites may find this service more effective and necessary. The effectiveness of this breached data center on reducing secondary privacy infringement may differ depending on the extend of data being shared and the conditions of data submission. When businesses experienced data breach and submission of data to this center is required by the law, the accuracy and effectiveness of this service can be enhanced. In addition, centralized database with high quality data set can increase matching for private information and control the secondary misappropriation of personal data or private information better.

Keywords: personal data, private information, privacy, data breach, data breach information center, framework

접수일(2012년 2월 29일), 게재확정일(2012년 4월 20일)
† 주저자, ymko@yonsei.ac.kr
‡ 교신저자, beomsoo@yonsei.ac.kr

I. 서 론

정보통신 기술의 발달로 온라인 환경에서 인터넷 이용자 활동의 증가는 원하는 정보를 공유하고, 전자상거래 활성화와 같은 오프라인의 시·공간적 제약을 해소하는데 긍정적인 영향을 주었다. 그러나 온라인 환경에서 이용자들의 개인 정보는 매우 쉽게 수집, 저장, 활용될 수 있다는 점에서 정보화 시대의 주요 이슈로 다루어지고 있다. 특히, 2011년 금융권 및 대형 포털 사이트의 개인정보 대규모 유출 사건이 발생하면서 사회 전반적으로 개인정보보호에 대한 경각심이 일었다. 한국인터넷진흥원 인터넷침해대응센터의 통계에 따르면 2011년 개인정보권 침해 신고 상담건수는 전년대비 54,832건에서 122,215건으로 67.3% 증가하였다. 또한 개인정보 유출 및 관련된 권리의 침해 상담 내용 중에서 약 57%가 '주민등록번호 등 타인 정보의 훼손·침해·도용'에 관한 것으로 개인정보 유출에 대한 예방 및 관리의 중요성이 점차 부각되고 있다.

최근, 국내외를 막론하고 개인정보권 침해 사고는 빈번하게 발생하고 있다. 고유식별정보를 포함한 유출된 개인정보는 범죄에 악용될 수 있다. 특히, 불법적으로 유출된 개인신상정보를 이용하여 온라인 명의도용 등으로 인한 피해가 확산되고 있다. 미국에서 2005년 개인정보 유출로 인한 피해액은 560억 달러에 이르렀지만, 개인정보 유출통지 법(Data Breach Notification Law)의 도입과 다양한 노력으로 명의도용(identity theft) 피해는 평균 6.1% 감소 효과가 있는 것으로 나타났다[20]. 우리나라 역시 「개인정보보호법」,「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 개정안(2012.2.17)에서 개인정보 유·누출 사고시 기업은 관련 기관에 신고할 뿐만 아니라 정보주체에게 이 사실을 공지할 것을 의무화하여 피해를 줄이기 위한 노력을 기울이고 있다.

개인정보 유출 사고에 따른 2차적 피해는 개인의 경제 활동 및 신용도 등에 부정적 영향을 미치므로 미연에 방지하기 위한 적극적 노력이 필요하다. 온라인 개인정보 유출 등의 위험이 매우 높은 상황에서 데이터보호와 개인정보의 침해를 방지하기 위하여 기술적 해결책과 정보보호 관리방안이 필요하다[3,13]. 특히 온라인에서 개인 정보 유출로 인한 개인의 2차적 피해를 차단할 수 있는, 보안 위협에 대한 개인행동이나 보안 기술을 사용하는 조직에 대한 관리를 통한 문제 발생 요소들의 통제가 필요하다[22].

현행법에 따른 신고 및 통지는 실질적으로 2차 피해를 방지하는데 한계가 있다. 개인정보 유출사고의 직·간접적 피해는 정보주체의 권리 보호를 위해 필요하며 보다 실질적인 추가 피해방지를 위한 방안이 필요하다. 본 연구에서는 개인정보 유출 사고 발생 시 유출된 개인정보를 공유하여 개인정보 오·남용으로 인하여 추가적으로 발생 가능한 2차 피해를 방지할 수 있는 개인정보 공유분석센터 모델이 필요함을 제안한다. 또한 개인정보 유출 사고 시 개인정보에 대해 관련 산업, 기업 차원에서 정보를 공유함으로써 정보주체의 피해가 추가로 확산되는 것을 방지할 수 있는 관리체계의 일환으로 몇 가지 대안을 제시하고, 이에 대한 장단점을 분석하였다.

II. 이론적 배경

2.1 개인정보 보호와 활용실태

2.1.1 정보보안과 개인정보 보호

다양한 정보 기술의 활용은 다수의 정보를 효율적으로 관리하고 사용함으로써 개인에 대한 관리의 강화 및 신용 기반의 거래를 가능하게 하였다. 특히 개인정보의 보호에 대한 인식이 점차 증가하는 환경에서 개인정보의 가치는 점차적으로 향상되고 있으며 기업의 개인화 서비스를 통한 마케팅 광고 등을 통해 폭넓게 이용되고 있다.

웹이 데이터베이스와 연동되어 정보 관련 서비스를 제공하는 환경에서, 각 데이터베이스와 서비스 주관 기관의 정보 흐름을 관리하기 위하여 개인정보 유출을 막기 위한 통합적 관점의 정보 보안 관리방식이 필요하다. 다시 말해서 정보 보안과 관련하여 정보 유출을 효율적으로 예방 및 관리하는 기능은 각 이해관계자들이 공유하고 있는 정보가 쉽게 유출 가능하고 그에 따른 피해를 보호할 수 있다는 점에서 중요성을 인지할 필요가 있다.

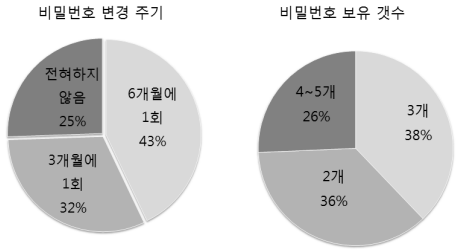
정보 보안의 관점에서 사용자의 정보를 관리하고 정보 유출을 관리할 수 있는 절차는 다양하지만 이러한 절차를 최소화하고 통합된 관리를 진행하는 것은 사용자의 정보 유출에 대한 위협을 줄여 줄 수 있다[21]. Hoffman 등[17]에 따르면 전자 거래 확산의 장애 요인의 하나로 많은 연구들이 개인 정보를 관리하기 위한 보안 관리를 중요한 요소로 언급하고 있다. 그 이유는 전자상거래를 하는 소비자들은 온라인 탐색 과정에서 누군가가 자신의 개인정보에 대해 접근한다

고 하더라도 이를 통제 할 수 없기 때문이다. 전자상거래에서 이용자가 지속적으로 사이트를 이용하기 위해서는 기본적으로 이용자의 개인정보를 필수적으로 제공하여야 한다. 이 때 이용자가 개인정보를 제공하는 것에 대하여 신뢰를 확보하기 위하여 서비스 제공자는 경쟁적 이점을 형성하기 위해 웹 페이지에 고객의 가입과 지속적 관계를 위한 신뢰 형성을 통해 위협을 감소시킬 필요가 있다.

2.1.2 인터넷과 개인정보 활용 행태

'2011년 인터넷이용실태조사'에 따르면 만12세 이상 인터넷 이용자 중에서 '인터넷을 통해 개인정보, 금융정보 등이 유출될까봐 걱정된다'는 64%에 이르렀다. 또한 인터넷을 이용하면서 경험하는 주된 불편, 피해 사항으로 '개인정보의 오용 및 사생활 침해'가 32.6%로 스팸메일, 원치 않는 광고 다음으로 높았다. 또한 만12세 이상 인터넷 이용자의 과반수가 인터넷을 통해 야기되는 사회문제 중 '개인정보 유출 및 도용'이 53.2%로 가장 걱정된다고 응답하였다[4]. 이처럼 개인정보와 관련된 이용자들의 인식 및 우려는 높은 수준인데 반해, 현재 인터넷 이용자는 커뮤니케이션활동(SNS, e-mail 등), 경제활동(인터넷쇼핑, 인터넷뱅킹 등) 등에 참여하면서 주민등록번호와 같은 고유식별정보를 포함한 개인정보를 여러 웹사이트에 제공하고 있다. 특히, 해외 서비스와 비교하여 국내 인터넷서비스사업자들은 고유식별정보를 포함한 개인정보를 과도하게 수집하는 경향이 있으므로 개인정보가 유출될 경우, 정보주체는 2차 직·간접적 피해를 입을 가능성이 큰 위험을 안고 있다. 이에 인터넷서비스 제공 기업에서는 개인정보권 침해사고를 예방하기 위한 방안의 일환으로 이용자들의 개인정보 보호를 위해 비밀번호를 일정주기로 변경하도록 권고하고 있다. 그러나 '2010 정보보호실태조사(개인편)'에 따르면 2010년 10월 만12~59세 인터넷 이용자 중 현재 웹사이트에서 사용하고 있는 비밀번호 종류가 3개라는 응답이 30.8%, 2개는 29.7%, 4~5개는 20.9%로 3개 이하가 과반수 이상을 차지하고 있다. 또한, PC 및 웹사이트 비밀번호 변경 주기 역시 '6개월에 1회 정도'가 24.2%로 가장 많았고, '3개월에 1회 정도'는 17.8%, '전혀 하지 않는 응답' 역시 14.4%로 나타났으며 이는 그림 〔그림1〕과 같다[5].

2009년, 국내에서는 해커가 악성 바이러스를 유포하는 방법으로 230만명의 ID와 패스워드를 해킹하고



〔그림 1〕 인터넷 이용자의 웹사이트 비밀번호 이용행태

네이버와 동일한 ID와 패스워드를 사용하는 15만명의 개인정보를 빼내, 이 중 9만개를 도용하는 사건이 발생했다[8]. 방영석 등[7]에 따르면 여러 웹사이트에 동일한 ID를 사용하는 이용자 행태를 해커들이 악용함으로써 발생하였다. 개인정보 유출 사건의 경우를 보더라도 해커들은 동일 ID를 사용하는 이용자를 중심으로 더 많은 정보를 불법적으로 수집하여 추가적인 범행에 이용해왔음을 알 수 있다. 또한 인간의 인지 채널 용량 이론 등에 따르면 인간의 인지 및 기억 능력의 한계로 인해 대다수의 인터넷 사용자는 사용하는 ID와 패스워드 개수는 몇 가지로 제한되어 사용할 수밖에 없는 것 또한 현실이다. 이러한 사용자들의 행태가 개인정보 유출 시 악용되고 있으므로 이를 효과적으로 해결하거나 관리할 수 있는 대책이 필요하다.

2.2 정보공유시스템

2.2.1 지식관리시스템

과거 지식관리차원의 연구의 결과를 통하여 개인정보의 효과적 관리에 유용한 시사점을 찾고자 한다. 정보를 공유함에 있어서 정보시스템의 역할은 매우 다양하다. 특정 시스템이 획득한 지식을 다른 사람과 공유하거나 상호 교환을 통하여 지식을 제공하고 재사용하는 공유 시스템은 전체 지식 관리 단계를 관장할 수 있는 핵심요소이다. 지식 관리는 특정 정보의 획득, 저장, 공유 그리고 사용의 과정으로 정의된다[16]. 특히 정보공유 활동은 개인 또는 별개의 조직에 내재된 정보를 전체적인 수준으로 확산시킴으로써 조직과 조직 간의 연결을 제공하고 경제적인 가치를 가져올 수 있다는 점에서 중요하다.

다양한 지식을 소유한 집단 간의 상호작용은 집단의 능력을 초과한 수준으로 전체 집단의 능력을 강화시킬 수 있다. 개인정보를 관리하고 정보 유출 단계 전후의 정보를 관련 기업들 간에 통지함으로서, 개인

정보 유출과 관련된 정보로부터 2차적인 정보 유출을 방지할 수 있는 시스템적 접근이 가능하다.

지식관리와 관련하여 한 집단의 정보를 다른 집단으로 공유하는 행위는 특정 지식을 관련 공동체에 직·간접적으로 공유할 수 있다는 점에서 공동의 목적에 부합하는 정보 제공을 통하여 성과를 향상시킬 수 있다[14]. 특히 공동의 목적 및 성과를 향상시키기 위하여 IT 기반의 지식 및 정보를 관리하는 것은 지식의 공유와 응용력을 향상시키며 이렇게 향상된 지식의 응용은 공동의 목적을 가진 집단 전체의 성과에 도움이 될 수 있다[15]. 기존 연구들은 공식적, 비공식적으로 개인 또는 팀 간의 지식 공유를 통하여 정보이용의 효율성을 향상시킬 수 있다는 점을 시사함으로써 IT 시스템의 지원을 통한 지식관리가 중요함을 제시하고 있다[12,15,19]. 특히 각 집단에게 개인정보의 유출을 공지하고 2차적 피해를 막기 위한 정보의 공유는 해당 정보를 다루는 기업들의 학습을 도울 수 있는 등의 효과를 기대할 수 있다.

기업의 지식관리시스템 연구와는 달리 개인정보 유출과 관련된 기존 연구와 관련하여 정보공유를 위한 정보시스템의 지원 및 관리 방식에 대하여 연구는 극히 적다. 따라서 본 연구에서는 개인정보유출과 관련하여 정보 공유 시스템을 관리할 수 있는 정보 공유 센터의 역할을 제안하고, 보다 효과적인 정보 공유 및 2차적 피해의 예방에 대한 체계를 제시하고자 한다.

2.2.2 정보공유시스템의 국내외 사례

앞서 언급한 바와 같이 정보 공유를 통하여 정보관리 및 보호가 가능하므로 국제적, 국가적으로 또는 특정 산업의 여러 분야에서의 정보공유시스템에 대한 필요성이 제기되었다. 반테러를 위한 국제 정보 공유 협력과 같은 국제간 정보공유 시스템뿐만 아니라, 국가 전반에 걸쳐 특정 산업군에 관계없이 공익을 증진하기 위한 목적으로 운영되는 공유시스템이 있다. 또한 신용정보를 분석하여 금융 산업의 활성화에 기여하는 특정 산업군내의 정보공유, 대기업 계열사 간 비즈니스 프로세스 효율성 증진을 위한 지식정보공유시스템 등의 기업간 지식정보 공유시스템 등이 그것이다. 이처럼 정보공유시스템은 다양한 분야에서 구축, 활용되고 있으며 구분하여 이를 정리하면 〔표 1〕과 같다.

〔표 1〕 정보공유시스템의 구분

구분	내용	실제 사례
국제	국가간 글로벌 협력·공조 체제	반테러 국제정보 공유 협력, 아태침해사고대응팀협의회 (APCERT)
국가	국가차원의 공익증진 목적	국가사이버보안안전센터 (국가정보원)
특정 산업	특정 산업군 내 관련 정보 공유 및 활용 시스템	금융결제원 (금융부문 정보공유분석센터), 금융정보분석원, 계약정보공유시스템 (생명,손해보험사), 신용평가정보시스템 (코리아크레딧뷰로), 통신정보공유분석협회 (통신부문 정보공유분석센터)
기업 간	기업간, 기업 계열사, 부서 간 업무 정보 등의 지식정보공유시스템	기업간 IT 협업시스템, 조직간 관리회계시스템

금융산업 등 특정산업군에서 비교적 활발하게 공유시스템이 활용된다. 예로 금융기관을 이용한 범죄자금의 자금세탁 방지 및 외화의 불법유출을 막기 위해 설립된 금융위원회 산하 금융정보분석원이 있다. 「특정금융거래정보의 보고 및 이용 등에 관한 법률 시행령」에 따라 금융기관으로부터 보고 받은 의심스러운 금융거래 정보를 분석하고 그 관련 정보를 상위 기관에 제공하는 역할을 한다. 또한 국내 K신용평가정보 시스템은 연체정보, 채무불이행 정보 등의 불량정보 위주의 한정된 부정(Negative) 정보뿐 아니라 카드 사용실적, 대출상환실적과 같은 긍정적(Positive) 정보를 분석하여 신용을 평가한다[1]. 이와 같은 시스템을 이용하면 관련 정보가 공유됨으로써 보다 효과적인 신용평가가 가능하게 된다. 국내뿐만 아니라 해외에서도 정보공유시스템의 필요에 대한 공감대가 형성되고 있다. 미국 은행들은 온라인 해킹범죄 공동대응 강화 방안의 일환으로 정보공유분석센터를 구축하고자 하였다. 해커들의 사이버테러 공격과 같은 외부 위협은 은행들이 기존의 독자적 관리활동에 병행하여, 보유 정보의 공유를 통한 공동대응 방식을 지향하도록 하는 압력 요인으로 작용한 것이다[11].

또한 최근 정보보호 분야에서는 복잡화되는 사이버 공격에 대응하기 위하여 정보공유분석센터(Information Sharing and Analysis Center, ISAC), 사이버위협정보공유시스템 등을 구축하여 공동 대응하는 노력을 보이고 있다. 「정보통신기반보호법」 제16조에 의거하여 금융 ISAC을 비롯하여 침해사고에 대비하고 보안 정보의 공유를 위한 센터를 설립하였다. ISAC은 사이버테러 대응 정보 등을 제공하고 침해사고 발생 시 실시간 경보 및 분석 업무를 수행한다. 특

정 산업, 분야별 여건을 고려한 침해사고 대응체계 구성 및 운영을 통하여 관련 기관에서 침해사고가 발생할 경우 주요 정보 사항을 공유하고 공동으로 대응하고 있다[9]. 이들 사례에서 볼 수 있듯이 개인정보 유출 사고 시, 개인정보의 효과적 관리와 유관 산업 간에 발생할 수 있는 2차 피해를 감소시키기 위한 중앙에서 통제 가능한 공동 대응의 필요성과 가능성이 제기된다. 또한 일부기업에서는 암시장을 통하여 유출된 개인정보를 구매하고, 이를 통한 개인정보보호 수준을 높이려는 노력이 행하여지고 있다. 따라서 본 연구는 개인정보 공유 분석 센터를 구축하여 관련 이해관계자들이 개인정보 관리에 대한 협업적 프레임워크를 공유하는 것이 필요하다고 보았다.

2.3 개인정보 공유 시스템 법적 프레임워크

개인정보 외 타 분야 정보공유분석센터로는 의심되는 금융정보 등과 같은 거래정보에 대해서 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 제3조, 제4조, 제4조2, 제8조(2011.5.19.)에 따라 금융위원회 소속 금융정보분석원을 설립하여 정보를 수집 분석할 수 있다. 또한 금융이나 통신 등 분야별 정보통신기반시설을 보호하기 위한 정보공유분석센터 구축 운영에 관한 「정보통신기반보호법」 제16조(2009.5.22.)에 따라 정보공유분석센터를 설립하여 운영할 수 있도록 하고 있다. 따라서 개인정보 유출 사고 시에도 정보주체의 피해 확산을 방지하기 위하여 개인정보 공유 분석의 필요함을 제시하고 구체적으로 관련 법·제도의 개선이 필요하다.

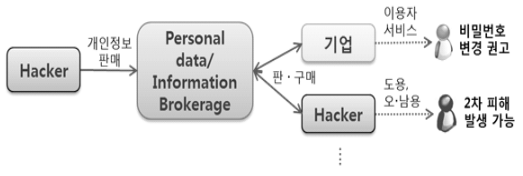
국내에서 개인정보권 침해와 관련하여 한국인터넷진흥원의 인터넷침해사고대응지원센터(KISC: Korea Internet Security Center), 국가정보원의 국가사이버안전센터 등의 다양한 기관에서 그 역할을 수행하고 있다. 그러나 개인정보 데이터베이스가 대량으로 유출되는 사건이 발생할 시에 이용자가 이용하는 다수의 웹사이트 정보를 공유 및 침해 위험도를 분석하기 위해서는 통합된 기관의 정보 관리가 필요하다. 개인정보 유출 시, 이를 효과적으로 통제하고 2차적 피해가 발생하지 않도록 통합 관리할 법·제도적 장치의 구축이 우선시 되어야 한다. 개인정보 공유 시스템의 법적근거의 출발점은 개인정보 유·누출 사고 시 정보주체에 통지하고 해당 기관에 신고하도록 하도록 하는 조항으로, 「개인정보보호법」 제34조(2011.3.29.), 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제27조의3(2012.2.17.)이 해당된다. 개인정보 공유분석센터 구축 및 운영과 관련하여 법적인 요건의 정비가 필요하다.

III. 개인정보 유출 시 개인정보 공유분석시스템 모형

3.1 개인정보 관리 현황

관련 전문가에 따르면 개인정보가 유출되었을 때, 개인정보 브로커를 중심으로 개인정보 거래가 이루어지고 유출된 개인정보는 다시 악의적 목적을 가진 사용자에게 재판매된다. 이 과정에서 명의도용 등과 같은 제2,3차 피해가 발생할 수 있다. Otto 등[18]에 따르면 개인정보 브로커 단계에서 많은 정보가 집중되어 있고 이를 다양한 채널로 재배포하게 되므로 개인정보 유출 위험에 노출될 경우, 정보주체의 개인정보 통제권에 위협을 가져올 수 있으므로 보다 철저한 관리가 필요하다.

[그림 2]와 같이 개인정보가 유출되면 개인정보 브로커 단계에서 거래가 발생하고 정보주체의 프라이버시 및 통제권에 위협을 가하게 된다. 이때, 이용자의 금전적·실질적 피해를 방지하기 위하여 유출된 개인정보를 활용하고자 하는 유관기업들은 유출 기업에서의 자발적 공유 또는 블랙마켓의 브로커를 통하여 이를 입수할 수 있다. 이와 같은 시스템에서는 중앙 관리센터가 부재하더라도 유출사고 기업 및 관련 기업들간의 데이터 공유는 가능할 수 있다. 그러나 기업 간 자발적 개인정보 공유는 사회적 공감대 및 업계의 필요성이 수반되어야 하는데 그렇지 않을 경우, 정보를 공유하지 않는 현 시스템과 비교할 때 블랙마켓 거래 비용이 발생하는 등 효과성이 크게 높지 않을 것이다. 그러므로 악의적 개인정보 브로커가 개입할 수 있는 현 정보공유실태를 고려한다면, 이를 전체적으로 관리하고 향후 위험을 통제할 수 있는 중앙 관리 기관 운영에 대하여 개별적 기업의 노력에 비해 더 많은 이점을 부여할 수 있다.



[그림 2] 개인정보 유출 사고 시, 개인정보 유통 흐름도

3.2 개인정보 공유 분석 시스템 모델

개인정보 유출 사고 시, 유출된 개인정보 관련 지식을 안전하게 공유할 수 있도록 하는 분석 센터를 구축하고 자발적 또는 의무적으로 공유하는 방식으로 유출된 자료와 자사 데이터베이스와의 대조를 통해 2차 피해를 방지하고자 하는 기업들이 이용할 수 있도록 한다. 개인정보 공유분석센터(이하 "센터")는 유관 산업간, 기업 간에 있어 역할에 따라 적극적 또는 단순 중개역할을 담당하게 된다. 개인정보를 유출한 기업은 센터로 신고하고, 센터에서 이러한 서비스의 제한적인 활용이 가능하다. 유출된 자료 및 정보는 정보주체의 유출방지를 위한 목적에 한해 이용할 수 있다.

3.2.1 개인정보 공유분석 센터의 기본 모델

〔그림 3〕의 A회사는 개인정보 유출 사고 기업으로 유출사고에 대하여 지정기관에 신고 시, 개인정보를 센터에 제공한다. 이렇게 구축된 개인정보 데이터베이스는 B,C회사와 같은 유관업계, 금전적 피해로 직결될 수 있는 회사들이 계약에 의하여 이용가능하다.

센터는 통합 개인정보 데이터베이스 운영을 통하여 개인정보를 분석 및 평가하고, 고위험 또는 저위험군으로 분류된 이용자별로 그에 맞는 조치를 취할 수 있도록 하는데 필요한 기초 정보를 기업에 제공한다. 이를 통해 유출된 정보와 동일한 아이디와 비밀번호를 쓰는 고위험군의 이용자는 2차 피해 및 신분 도용에의 위험성이 높으므로 기업은 임시 비밀번호를 생성, 부여하고 이용자가 재변경하는 것과 같은 강제 변경 조처를 취할 수 있다. 또한 금전적 피해로 직결될 수 있는 금융 정보인 경우, 피싱과 같은 사회공학적 위협에 노출 될 수 있으므로 이에 대한 사전 경고를 통해 2차 피해를 미연에 방지한다. 저위험군 이용자인 경우, 자발적·주기적 비밀번호 변경 권고 등의 조처를 취할 수 있다. 이러한 차별적 보완조치의 활용은 2차 피해를 막기 위한 노력의 실질적 효과를 증대할 수 있다.

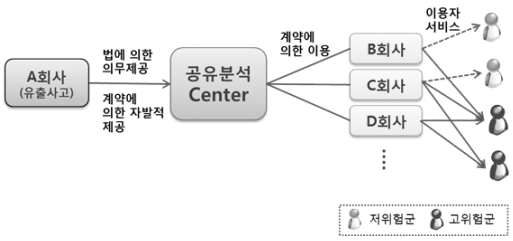
또한, 현행법에 따라 유출사고 기업은 개인정보 유출사고와 관련된 내용을 해당 기관에 신고하고 이용자에게 관련 내용을 알리는 유출 통지 절차를 진행하는데, 이때 2차 피해방지를 위한 안내문에 이용자로 하여금 개인정보 공유분석 센터를 활용하여 동일 아이디를 활용하는 사이트를 검색하고 변경 가능하도록 하는 등의 서비스를 제공할 수 있다.

3.2.2 개인정보 공유분석 센터의 확장 모델

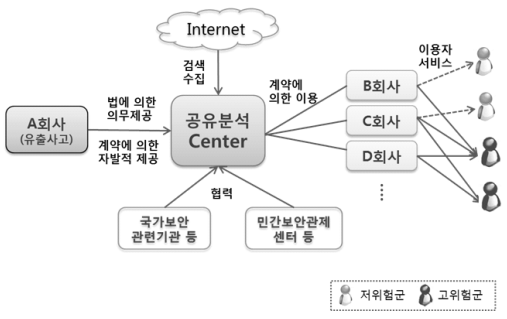
인터넷침해사고대응지원센터는 인터넷망의 상시 모니터링을 통한 보안위협 및 이상 징후를 조기에 탐지하여 인터넷침해사고를 사전에 예방하고 피해확산을 방지하는 역할을 수행하는데 있어 국내 정보통신서비스제공자, 백신업체, 보안관제업체 등과 상시적인 정보 공유, 신속한 공동대응체계를 통하여 인터넷 망에 대한 안전성 및 신뢰성을 확보한다〔6〕.

〔그림 4〕에서 제시하는 확장 형태의 센터는 유출사고 기업의 개인정보 뿐 아니라, 기존 인터넷에 유포된 불법 개인정보를 검색·수집을 통하여 유출된 개인정보에 대한 통합 데이터베이스를 구축한다. 또한 정보보호 관련 전문기관들의 협력 체제를 구축하여 보다 적극적인 기능을 수행하는 것이다.

개인정보 공유 분석센터에서 전문 기관의 협조를 받아 진행할 때, 연계 협조 비용이 발생할 수 있다. 여러 기관의 정보가 집적될 경우, 정보 보안에의 위협이 생길 수 있으므로 직접적으로 연계효과에 대한 분석이 추후에 필요하다. 하지만 국가적 차원에서 사이버대응센터를 구축하여 운영하고 있고, 민간 역시 보안관제센터를 설립하는 등 적극적으로 정보보호 노력을 기울이고 있는 만큼 관련 공조체제를 구축한다면 시너지 효과가 기대된다. 특히, IT 시스템은 민간영역에 다수



〔그림 3〕 개인정보 공유분석시스템(기본)



〔그림 4〕 개인정보 공유분석시스템(확장)

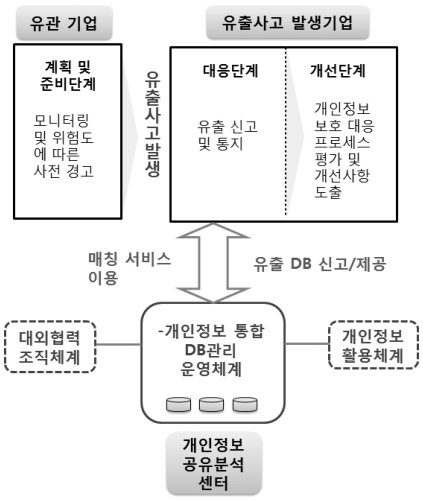
분포되어 있으므로 정부주도의 센터가 설립된다고 하더라도 민간영역의 협조가 필수적이며, 보다 효과적인 대응 협력이 이루어질 수 있다.

IV. 개인정보 공유분석 센터의 효과성

4.1 개인정보 공유분석 센터의 서비스 구성

이충훈 등[10]에 따르면 개인정보가 유출되었을 때, 기업대응 프로세스는 계획 및 준비단계, 대응단계, 개선단계의 3단계로 구분된다. 기업은 발생가능한 개인정보 유출사고의 효과적인 대응을 위해 사전에 구체적인 대응 계획을 수립한다. 실제 사고가 발생한 경우에는 대응단계에서 그 사실을 지정 기관에 신고하고 관련 자료를 개인정보 공유분석센터에 제공한다. 기타 기업에서는 센터의 정보와 서비스를 이용하여 정보보호 수준을 강화할 수 있다. 마지막으로 대응단계에서 개인정보 보호 대응 프로세스의 객관적 평가를 통해 개선 사항을 도출하여 반영함으로써 대응프로세스를 고도화 할 수 있다.

[그림 5]와 같이 센터는 대외협력조직체계 및 기존의 개인정보 활용체계와 연계하여 개인정보 데이터베이스를 고도화할 수 있으며, 개인정보 통합관리체계는 개인정보 분석, 평가에 대한 체계와 통합 개인정보 데이터베이스 운영체계를 포함한다. 대외협력체계는 개인정보 수집을 위하여 국내외 다양한 개인정보보호 기관, 보안관제 센터, 소프트웨어 벤더, 보안전문가, 국내 CERT 등과 협력체계를 구축하는 것과 같이 개인



[그림 5] 개인정보 공유분석센터 서비스 모형

정보 공유분석센터 역시 부문별 보안관제 센터와의 협력을 추진할 수도 있다[2]. 이들 체계와의 유기적인 협력관계를 통하여 기업은 유출사고에 사전 대비할 수 있고, 사고가 발생하더라도 정보주체의 피해 확산 방지에 대하여 적극적인 조처를 취할 수 있게 된다.

4.2 서비스 형태에 따른 장단점

개인정보 공유분석시스템 구축시 서비스 이용자와 운영자로 구분될 수 있다. 이용자 및 운영자는 센터의 취지를 이해하고 동의하는 관련 이해관계자들로서, 센터의 주요 서비스 대상이자 주 이용자는 유출 사고 기업의 유관분야의 기업으로 통칭할 수 있다.

개인정보 유출사고 기업은 센터에 관련 자료를 의무 또는 자발적으로 제공할 수 있다. 이에 따라 비용과 효과는 달라질 수 있으며, 공유 및 서비스 형태에 따른 효과성에 대해서는 [표 2]에 제시하였다. 기업 또는 특정산업군내의 자발적 제공에 맡겨 계약에 의해 운영할 경우, 센터의 적극성에 따라 단순중개 또는 적극적 서비스 기관으로의 역할을 수행할 수 있다. 유출사고 기업의 데이터베이스를 의무적으로 제공하여야 하는 강제성이 없으므로 참여 기업의 부담이 감소한다. 그러나 자발적 제공이 원활하지 않을 경우 관련 산업군 내 기업은 비교·분석 서비스를 받기 어려워 센터의 실질적 효과는 미약할 수 있다. 이에 반해 자발적 제공을 바탕으로 적극적인 서비스를 제공할 경우 개인정보 비교·분석 서비스의 투명성, 신뢰성 확보가 가능하다. 이때 정보주체의 2차 피해를 방지하기 위한 기업들의 적극적인 참여 의지가 필요하다.

유출 정보 제출이 의무화되는 경우, 해당 자료를 반드시 제공하여야 한다. 이때 센터의 기능 역시 적극성 및 개입성에 따라 단순히 중개역할을 수행하거나 또는 보유하고 있는 데이터베이스로 이용을 원하는 기업과 계약을 맺어 B2B 형태로 서비스를 제공할 수 있다. 단순 역할을 할 경우에 센터는 중립적으로 운영되며, 서비스를 필요로 하는 기업들은 이용 계약을 맺어 이용 가능하다. 센터는 중개 역할을 수행하므로 사고 유출 기업 및 타 기업 간의 적극적인 참여의지가 수반되어야 한다. 반면, 센터에서 적극적인 서비스를 제공할 시에는 센터는 정보 처리의 투명성을 확보하고 중립성, 높은 보안성을 유지하여야 한다. 고객정보는 보유기업에서 상당히 중요한 자산으로 인식하고 보호하고자 하는 등의 관점을 고려하여야 할 것이다. 이 경우, 결과적으로 단일 채널화된 서비스의 구축 및 매칭 기

〔표 2〕 개인정보 공유분석센터의 제공형태 및 기능에 따른 효과

제공 형태	기능	효과	
자발적 제공	단순 중개	장점	개인정보 관리에 대한 기업인식 강화, 기업 내 자체적인 자발적 정보관리기술개발
		단점	개인정보 제공 기업 및 유관 기업의 적극적인 의지 필요. 서비스를 원하는 유관 기업이 있어도 유출 자료 수집이 제한되면, 실질적 효과 미약
	적극 매칭	장점	센터 중립성을 통하여 기업 간 신뢰도 확보 가능, 기업들의 참여 독려
		단점	개인정보 제공 기업 및 유관 기업의 적극적인 의지 필요. 유관기관의 적극적인 매칭 의사가 있어도 개인정보 DB 구축이 잘 안될 경우, 효과 미약
의무적 제공	단순 중개	장점	수집 투명성 향상, 매칭 서비스를 필요로 하는 유관 기업 참여 촉진
		단점	유관기업의 적극적인 2차 피해 방지 의지 필요
	적극 매칭	장점	단일 채널화된 데이터베이스의 구축 및 매칭 기술 활용 가능으로 ID 정확도 상승. 2차 개인정보 오남용에 대한 강력한 관리 지원 가능
		단점	센터 서비스의 투명성이 없을 경우 신뢰성 문제로 인한 기업 참여 수준 저하, 의무적·적극적으로 서비스 제공 시 매칭기술의 오류 등으로 인한 문제 발생, 센터 보안위험 수준 높음

술 활용하여 개인정보 ID 정확도 상승으로 질 높은 서비스를 제공할 수 있고, 제2차 개인정보 오·남용에 대한 보다 효과적 보호 및 관리 지원이 가능하다.

유출된 개인정보 데이터베이스를 의무적으로 제공할 경우의 효과적인 개인정보 비교·분석을 통하여 정보주체의 제2차 피해 규모를 감소시킬 수 있다. 자발적일 경우, 정보센터 참여와 정보제공, 정보서비스 이용에 대한 합리적 정책 비용이 발생하고, 개인정보 공유에 따른 효과는 의무적 제공보다 효과가 크지 않을 수 있다.

V. 결 론

최근 개인정보 대규모 유출 사고가 빈번히 발생하면서, 이를 방지하기 위한 개인정보 유출 및 누출 통지제도가 법에 의해 마련되었다. 기업은 사고유출 처리와 관련된 계획을 수립하고 유출사고 발생 시에는 지체없이 그리고 정확한 통지를 제공하여야 한다. 또한 프라이버시를 보호하기 위한 고객 정체성을 확보하고 정기적인 보안 감사를 시행하고, 개인정보 저장 시 반드시 암호화하며 회사의 프라이버시 정책을 명확하게 표현할 것을 권고하고 있다〔18〕. 또한, 개인정보 유출사고에 대하여 정보주체에게 통지할 때에 2차 피해 방지를 위한 보다 적극적인 방안이 필요하고, 이에 관련된 여러 가지 방안이 연구되고 있다.

이 연구에서는 유출된 개인정보를 관계기관 및 개인에게 통지할 뿐만 아니라 별도의 유출정보 처리 및 공유센터를 마련하여 제2차 피해를 줄이기 위한 보다 적극적 대응방안을 제시한다. 개인정보권 침해 사고가 발생할 경우, 신속하게 대응할 수 있도록 하기 위한 법과 제도 등도 포함되어야 한다. 현재까지 유출된 개인정보의 분석 및 조처는 관련 기업 간, 산업 간의 협력체계가 미비한 상황에서 블랙마켓 등을 통하여 개별적으로 이루어졌기 때문에 그 효과성 등에 대한 문제점과 또 다른 위험에 노출될 가능성이 있다. 이러한 문제나 위험 등을 고려한 보다 적극적인 방안으로 국가차원의 개인정보 통합관리기관이 필요하다.

본 연구에서 제시한 개인정보 공유분석센터의 장점은 유출사고가 발생한 개인정보 데이터베이스를 공유하고 유관 기업의 데이터베이스와 비교·분석 할 경우, 정보주체에게 효과적인 개인정보 유출 방지 맞춤 서비스를 제공할 수 있다. 기업은 다수의 웹사이트에 동일 ID와 패스워드를 사용하는 이용자를 고위험군으로 분류하여 비밀번호 강제변경 조치의 근거로 활용가능하고, 금전적 피해의 확률이 높은 금융 관련정보일 경우에는 계정 접근 제한 등의 적극적인 조처를 취할 수 있다. 저위험군일 경우 자발적 변경 권고를 함으로써 2차 유출 피해를 미연에 방지하는 효과가 있다. 또한 정보공유분석센터를 통해 관련 기업들은 유출된 개인정보 통합·관리함으로써 블랙마켓에의 노출 위험을 저하시킬 수 있다.

기존 개인정보 브로커 등을 통해서 불법적으로 거래되는 개인정보 공유를 법과 계약에 의해 양성화함으로써 정보주체의 유출 피해 확인 및 적극적인 대처가 가능해진다. 이는 기업의 입장에서 이용자 중심의 개인정보 유출 피해 방지 대책을 수립하고 보다 적극적인 대처를 함으로써 개인정보 유출 사고 발생 시 소요되는 비용을 줄일 수 있다. 또한 사회 전체적으로 개인정보의 불법 유통, 유출된 개인정보가 불법으로 오·남용을 사전에 예방하고 기타 개인정보권 침해대응방법과의 시너지 효과를 발생시킬 수 있다. 그에 따라서

본 연구는 개인 정보 유출을 관리하기 위한 제도적, 실무적 개선점을 확인하고 이를 통하여 개인정보 보안 수준을 향상할 수 있는 관점을 개선하고자 하였다.

그러나 개인정보 공유분석센터를 운영할 경우, 정보가 집적되는 만큼 또 다른 유출 사고에 대비한 철저한 보안정책이 수반되어야 할 것이며 개인정보 DB 공유 기간을 설정하여 일정기간 동안 서비스하는 방안 등을 활용할 수 있다. 공유기간은 통상적으로 해커가 개인정보 DB를 수집하여 다른 곳에 악용 가능한 기간을 추산하여 제시할 수 있다. ID 외에도 고유식별정보(주민등록번호 등)를 함께 사용함으로써 매칭 정확률이 높아지는 등의 구체적인 효과에 대해서는 추후 실제 데이터를 통한 연구가 필요하다. 사고 예방비용 대비 실질적인 2차 피해로 인한 배상금액, 기업의 이미지 실추, 신뢰성 상실 등에 대한 직간접적인 비용이 향후 계속 상승한다면 이러한 센터의 운영효과도 지속적으로 높아질 수 있다.

참고문헌

〔1〕 권영준, 남재현, 조민정, "개인신용평가에서의 비금융정보의 경제적 효과." 한국경제연구 29(2),pp. 81-107, 2011년 4월.

〔2〕 김동진, 조성제, "국가 DB기반의 국내외 보안취약점 관리체계 분석." Internet and Information Security 1(2), pp.130-147, 2010년 11월.

〔3〕 김범수 외, 스마트 시대 정보보호 전략과 법제도Ⅰ, 한국학술정보, 2011년 12월.

〔4〕 방송통신위원회, 한국인터넷진흥원, 2011년 인터넷 이용실태조사, 2012년 1월.

〔5〕 방송통신위원회, 한국인터넷진흥원, 2010 정보보호 실태조사-개인편, 2011년 5월.

〔6〕 방송통신위원회, 행정안전부, 지식경제부, 2011 국가정보보호백서, pp.17-18, 2011년 5월.

〔7〕 방영석, 이동주, 배윤수, 안재현, "인터넷 사용자들의 아이디/패스워드 사용실태에 대한 실증적 연구." 한국경영정보학회 춘계학술대회 논문집 2009(1), pp. 859-864, 2009년 6월.

〔8〕 보안뉴스, "230만명 개인정보 해킹, 도박광고에 활용 일당 구속.", 2009년 4월 16일 http://www.boannews.com/media/view.asp?idx=15506.

〔9〕 이근영, 박태형, 임종인, "스마트 모바일 오피스 보안을 위한 CERT와 ISAC의 역할." 정보보호학회논문지 21(5),pp.109-127, 2011년 10월.

〔10〕 이충훈, 고유미, 김범수, "개인정보 유출 시 통지·신고 프레임워크 및 가이드라인." 정보보호학회논문지 21(5), pp.169-179, 2011년 10월.

〔11〕 한국금융연구원, "미국 은행들의 온라인 해킹범죄 공동대응 강화." 주간 금융브리프 21(5), 2012년 2월.

〔12〕 Alavi, M., and Tiwana, A., "Knowledge Integration in Virtual Teams: The potential Role of KMS." Journal of the American Society for Information Science and Technology, vol.53, no.12, pp.1029-1037, Oct. 2002.

〔13〕 Bélanger, F., and Crossler, R. E., "Privacy in the Digital Age: A review of Information Privacy Research in Information Systems." MIS Quarterly, vol.35, no.4, pp.1017-1041, Dec. 2011,

〔14〕 Bock, G. W., Zmud, R. W., and Kim, Y. G., "Behavioral Intention Formation in Knowledge Sharing: Examing the Roles of Extrinsic Motivators, Social-Psychological Forces, and Organizational Climate." MIS Quarterly, vol.29, no.1, pp.87-111, Mar. 2005.

〔15〕 Choi, S. Y., Lee, H., and Yoo, Y., "The Impact of Information Technology and Transactive Memory Systems on Knowledge Sharing, Application, and Team Performance: A Field Study." MIS Quarterly, vol.34, no.4, pp.855-870, Dec. 2010.

〔16〕 Davenport, T. H., and Prusak, L., Working Knowledge, 2nd Ed., Boston: Harvard Business School Press, May. 2000.

〔17〕 Hoffman, D. L., Novak, T. P., and Peralta, M., "Building Consumer Trust in Online Environments: The Case for Information Privacy." Communications of ACM, vol.42, no.4, pp.80-85, Apr. 1999.

〔18〕 Otto, P. N., A. I. Anton, and D. L. Baumer, "The ChoicePoint dilemma - How data brokers should handle the privacy of

personal information." IEEE Security & Privacy, vol.5, no.5, pp.15-23, Sept.-Oct. 2007.
〔19〕 Pee, L. G., Kankanhalli, A., and Kim, H. W., "Knowledge Sharing in Information Systems Development: A Social Interdependence Perspective." Journal of the Association for Information systems, vol.11, no.10, pp.550-575, Nov. 2010.
〔20〕 Romanosky, S., R. Telang, et al., "Do Data Breach Disclosure Laws Reduce Identity Theft?" Journal of Policy Analysis and Management vol.30, no.2, pp.256-286, Mar. 2011.
〔21〕 Sheehan, K. B., and Hoy, M. G., "Dimensions of Privacy Concern among Online Consumers." Journal of Public Policy and Marketing, vol.19, no.1, pp.62-73, Spring. 2000.
〔22〕 Wiant, T. L., "Information Security Policy's Impact on Reporting Security Incident." Computers and Security, 24, pp.448-459, Sep. 2005.

〈著者紹介〉

고 유 미 (Yumi Ko) 학생회원
2008년 2월: 연세대학교 문헌정보학과
2011년 3월~현재: 연세대학교 정보대학원 지식서비스보안과정
소만사 Research Fellow
〈관심분야〉 정보보호, 프라이버시, 개인정보

최 재 원 (Jaewon Choi) 정회원
2004년 2월: 가톨릭대학교 경영학과 졸업
2006년 2월: 가톨릭대학교 경영학과 석사 (경영정보학)
2010년 8월: 가톨릭대학교 경영학과 박사 (경영정보학)
2010년 8월~2011년 8월: 한국과학기술원(KAIST) 테크노경영연구소 연수연구원
2011년 9월~현재: 연세대학교 정보대학원 박사후연구원
〈관심분야〉 웹개인화, 정보보호, 지능형의사결정시스템, 소셜네트워크분석, 데이터마이닝

김 범 수 (Beomsoo Kim) 종신회원
1999년: 미국 University of Texas at Austin, Ph.D.
1999년~2002년: 미국 University of Illinois at Chicago, 조교수
2002년~현재: 연세대학교 정보대학원 교수
2011년~현재: 지식서비스보안과정 및 ITMS과정 주임교수, ISACA Korea 부회장
2012년~현재: 연세대학교 정보대학원 부원장
〈관심분야〉 정보보호정책 및 제도, 프라이버시 권리, 개인정보 보호, 전자상거래, 정보경제학