Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.4, Aug. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.4.885

클라우드컴퓨팅 이용 신용카드사의 영세수탁자 개인신용정보 보호방안

김 시 인,† 김 인 석‡
고려대학교 정보보호대학원

Protection Plan of Trustee Personal Credit Information for Credit Card Company Using Cloud Computing

Shi-in Kim,† In-suk Kim‡
Graduate School of Information Security, Korea University

요 약

최근 금융권 해킹사례를 통해서 알 수 있듯이 공격자는 금융회사를 직접 해킹하기 보다는 보안관리가 허술한 수탁자를 대상으로 해킹공격을 시도하고 있다. 이로 인해 위탁자는 수탁자에 대한 보안점검 및 통제를 강화하고 있으나 영세 수탁자의 경우 전산설비 부족 및 보안장비 도입 시 과도한 비용 발생으로 인해 정보보호 투자에 미흡하다. 본 논문에서는 신용카드사들로부터 개인정보를 제공 받은 영세수탁업체의 보안강화를 위해 개인정보 라이프 사이클 기준으로 취약점에 대해 알아 보고자한다. 취약점 해결방안으로 클라우드 컴퓨팅 서비스에 소송관리시스템을 구축하여 사용하고 데이터 전송구간은 가상사설망을 설치하여 기밀성 및 무결성을 확보한다. 또한 사용자 보안강화를 위해 사용자PC에 PC방화벽, 출력물 보안등의 설치를 통한 개인신용정보 처리 보호방안을 제시하고자 한다.

ABSTRACT

As seen in recent cases of hacking in financial services, attackers are attempting to hacking trustee with poor security management, rather than directly hacking a financial company. As a result, the consignor is strengthening the security check and control of the trustee, but small trustee has difficulties to invest in information security with the lack of computer facilities and the excessive cost of security equipment. In this paper I investigate the vulnerability of personal information processing life cycle standards in order to enhance the security of small consignee that receive personal information form the credit card company. To solve the vulnerability the company should use litigation management system constructed on cloud computing service and install VPN to secure confidentiality and intergrity in data transfer section. Also, to enhance the security of users, it is suggested to protect personal credit information by installing PC firewall and output security on user PC.

Keywords: Trustee security, Consignor security, Cloud

I. 서 론

최근의 보안사고에서 공격자는 기업들을 대상으로 직접적인 공격보다는 이들 기업과 수탁계약을 맺은 업체를 통하여 우회하는 방법을 활용하고 있다. 공격자가 이러한 간접적인 방법으로 공격을 감행하는 이유는 수탁계약을 맺은 업체들이 침해사고에 취약하기 때문이다. 대표적인 사례로는 '17년 3월에 발생한

Received(04. 16. 2019), Modified(1st: 05. 21. 2019, 2nd: 06. 17. 2019), Accepted(06. 17. 2019)

† 주저자, shieni@naver.com
‡ 교신저자, iskim11@korea.ac.kr(Corresponding author)

국내 ATM기 회사의 백신 서버가 인터넷 망에 연결되어 있는 취약점을 이용해 전산망을 해킹한 뒤 ATM기 63대에 악성 프로그램을 유포시켰고 해당 ATM을 사용한 고객 금융정보 23만 여건이 유출된 사건이다. ATM 공격 사건 이후 금융보안원에서는 17년 하반기 금융회사 공동으로 수탁자 점검을 실시했다. 점검결과 공통적으로 취약한 사항은 중요 단말기의 안전조치에 대한 사항으로 중요 단말기가 별도로 지정되어 있지 않았으며, 인터넷 접속 가능한 일반 업무용 단말기에서 시스템 관리 업무를 수행하고 있는 취약점이 있었다. 또한 개인정보처리시스템에 대한 비인가 접근 탐지 및 대응사항으로 침입방지시스템 등의 이벤트를 모니터링하고 있으나, 전자적 침해시도에 대한 분석, 대응이 미흡했다. ATM을 관리하고 있는 VAN사는 해당 취약점에 대해 많은 시간과 비용을 투자하여 조치완료 하였다.

금융회사는 개인정보보호법 제26조(업무위탁에 따른 개인정보의 처리 제한)4항에 따라 수탁자에 대한 관리감독을 해야 하는 의무가 있다. 구체적으로 수탁자가 위탁자인 금융회사의 개인신용정보를 처리하면서 정보유출, 목적외 이용 등에 따른 문제가 발생할 경우 위탁자의 책임이 있으므로, 수탁자가 관련 규제를 준수하여 개인신용정보를 처리하도록 계약 등을 통해 강제할 수 있지만, 수탁자가 규제를 위반하지 않고 개인신용정보를 처리할 수 있는 환경을 위탁자가 제공하는 것이 더 필요할 수 있다. 수탁자가 안전한 절차 또는 환경에서 위탁자의 개인신용정보를 처리할 수 있도록 클라우드컴퓨팅을 이용하는 것이 하나의 방안이다.

금융회사의 전산시스템은 폐쇄적인 망에 독자적으로 구축되어 있었으나 국내 클라우드 활성화 정책[1] 및 전자금융감독규정(2016.10)이 개정되면서 금융권에서도 클라우드컴퓨팅을 도입할 수 있는 계기가 되었다. 하지만 모든 정보시스템이 아닌 비 중요정보시스템에 국한하여 허용[2]함으로써 금융회사에서 적용하기에는 한계가 있었다. 이에 2018년 7월 핀테크 활성화 방안의 일환으로 금융위원회에서 전자금융감독규정을 개정(2019.01)함으로서 고유식별정보 또는 개인(신용)정보가 포함되어 있어도 클라우드컴퓨팅을 사용할 수 있게 하였다. 이에 따라 금융회사들은 클라우드컴퓨팅을 적용하기 위해 여러 가지 방안을 모색 중이다. 본 연구는 신용카드사들이 업무를 영위하기 위해 위·수탁 계약이 빈번하게 발생하는 부분에 착안하여 클라우드컴퓨팅을 이용한 수탁자 중 소송관련 대행업체(이하 영세수탁자)가 업무처리 시 개인신용정보를 보호하는 방안에 대해 설명하고자 한다.

II. 신용카드사의 영세수탁자 현황

신용카드사와 같은 개인신용정보처리자가 자신의 목적과 이익을 위해 개인신용정보를 제3자에 제공하는데, 본인의 업무를 제3자에게 맡기는 것을 위탁이라 하고, 개인신용정보처리자를 위탁자, 그리고 제3자를 수탁자라고 한다.

일반적으로 수탁자를 구분하는 기준은 위탁자가 속한 업권, 위탁자 또는 수탁자의 자산규모, 수탁자의 기업유형, 수탁자가 계열사 및 관계사 등의 관계인지 여부, 위탁 업무의 특성 및 성격에 따라 상이하다. 본 논문에서는 수탁자의 자산규모 및 업종에 따라 수탁자를 구분하고, 이 중 영세수탁자에 해당하는 제3자에게 위탁자의 개인신용정보를 제공하였을 경우 이 개인신용정보를 어떻게 보호할 것인지에 대한 방안을 제시하고자 한다.

2.1 영세수탁자 정의

한국신용평가정보에서 제공되는 기업유형에 대한 정보를 기준으로 수탁자의 자산규모 및 기업유형에 따라 대기업, 중견기업, 중소기업, 공기업, 기타의 유형으로 구분할 수 있다.

논문에서는 중소기업과 기타에 해당하는 자 중에서 자본금이 1억원 미만의 회사를 영세수탁자로 정의하였다. 여기서 자본금을 1억으로 정한 이유는 신용정보 이용 및 보호 등에 관한 법률(이하 "신용정보법") 제17조제2항 및 동법 시행령 제14조에 따르면, 신용정보회사등은 수집된 신용정보의 처리를 자본금 또는 자본총액(대차대조표상의 자산총액에서 부채총액을 뺀 금액을 말한다)이 1억원 이상인 기업으로서 정보보호 관련 법률에 따른 정보보호책임자[1]를 지정한

1) 신용정보법 시행령 제14조(수집된 신용정보 처리의 위탁) ① 법 제17조제2항에서 "일정한 금액 이상의 자본금 등 대통령령으로 정하는 일정한 요건을 갖춘 자"란 자본금 또는 자본총액(대차대조표상의 자산총액에서 부채총액을 뺀 금액을 말한다)이 1억원 이상인 기업으로서 다음 각 호의 어느 하나에 해당하는 자를 말한다.
1. 법 제20조제3항 본문에 따라 신용정보관리·보호인을 지정한 자
2. 「개인정보 보호법」 제31조에 따라 개인정보 보호책임자

자에게 위탁할 수 있도록 규정하고 있는데, 이는 1억원 미만의 수탁자의 경우 상대적으로 정보보호의 수준이 낮을 수 있다는 점을 착안하였다. 참고로 본 논문에서는 회사의 신용정보법 법규 위반여부에 대해서는 별론으로 한다.

2.2 영세수탁자에 대한 자료제공 현황

본 논문을 위해 '18년 12월 11일 신용카드사의 홈페이지에 게시되어 있는 위·수탁 관리현황을 엑셀로 정리한 결과 조사된 신용카드사(이하 "대상 신용카드사")의 영세수탁자는 총 38개사(중복제외)이고, 위탁업무별 제공되는 자료의 현황은 Table 1.과 같다.

특히 Table 1.의 4번 항목은 민사소송 업무 등의 위임, 신용카드 매출채권 공탁업무를 대행하고 있는 ○○법무사무소는 법무사이고, 이 자가 제공받는 자료는 주민등록번호, 성명, 주소, 연락처, 계좌번호, 카드번호가 있다.

Table 1. Custodian data provision status

#	Purpose	Offer item
1	Service provision	name, mobile phone number, date of birth, gender
2	Marketing	mobile phone number, membership number, name, address, nickname
3	Sale of goods	name, mobile phone number, address, product name, number of products, note
4	lawsuit	resident registration number, name, address, contact, account number, card number
5	paying credit card	card number

를 지정한 자

3. 「전자금융거래법」 제21조의2에 따라 정보보호최고책임자를 지정한 자
4. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제27조에 따라 개인정보 관리책임자를 지정한 자

2.3 영세수탁자에 대한 보안관리 실태점검 결과

위탁자인 신용카드사는 수탁자를 대상으로 개인신용정보 보호를 위하여 주기적으로 점검을 실시하고 있다. 대상 신용카드사가 점검한 2018년도 상반기 점검결과[22]에 따르면 다음과 같다.

- 관리적 측면: 규정, 지침, 홈페이지 미 운영, 개인정보처리방침의 미 수립·미공개(부가상품), 이행실태에 대한 주기적인 관리·감독을 미시행하고 있다.

- 기술적 측면: 개인정보가 저장되어 있는 PC에 대한 보호조치가 적절하게 운영되지 않았다. 세부적으로 살펴보면 개인정보가 저장된 PC가 인터넷에 연결 되어 있지만 최신패치가 적용되어 있지 않거나, 백신이 미설치 되어 있어 악성코드에 대한 대비책이 전무한 상태다. 또한 침해사고 예방을 위한 침입탐지시스템 및 분산서비스공격에 대응하기 위한 대책도 미흡한 상황이다.

점검결과에 따른 개선방안을 도출하기 위해 수탁자들과 논의를 하였으나, 비용측면에서 합리적인 협의안을 도출하기에는 현실적인 한계가 있었다. 따라서 신용카드사인 위탁자가 자신의 개인신용정보를 보호하기 위해 현실적인 비용과 노력으로 수탁자를 관리적·기술적 측면에서 관리할 수 있는 방안으로 클라우드컴퓨팅 이용 방안을 고려하게 되었다.

2.4 설문조사를 통해 본 영세수탁자 정보보호 관리현황

설문조사를 통해 기존 하나의 수탁자가 몇 개의 금융회사로부터 업무를 위탁 받는지와 연간 정보보호 투자금액 및 위탁자의 정보보호 실태 점검 등을 확인하기 위하여 영세사업자 중 하나인 법무사무소 14곳을 대상으로 설문조사를 실시하였다. 설문조사는 2019년 5월 15일부터 19일까지 5일간 진행하였고, 구체적인 설문항목과 조사결과는 다음과 같다.

- 직무경력 : 법무사로 근무한 경력을 조사하여 설문작성자의 전문성을 확인하기 위함.
  - 3년이하: 14.3%
  - 5년이하: 21.4%
  - 9년이하: 0%

- 10년이상 64.3%
- 없음 0%

● 위탁자 수 : 현재 수탁자가 위탁받은 업체의 수를 확인하기 위함으로 하나의 수탁자가 보통 몇 개의 금융회사로부터 업무를 위탁받는지 확인하고자 함.
- 2개 업체이하: 14.3%
- 4개 업체이하: 28.6%
- 6개 업체이하: 21.4%
- 7개 업체이상: 28.6%
- 없음: 7.1%

● 정보보호담당자 지정 : 수탁자가 정보보호를 위해 노력하고 있는지 확인하기 위함.
- 지정: 14.3%
- 미지정: 85.7%

● 정보보호투자금액 : 연간 영세수탁자의 정보보호 투자금액을 통해 과도한 비용발생으로 인해 정보보호 투자에 미흡한지 여부를 확인하고자 함.
- 100만원 이하: 85.7%
- 500만원 미만: 14.3%
- 500만원 이상: 0%

● 위탁자 정보보호 실태점검 여부 : 수탁자에 대한 위탁자의 의무인 관리·감독이 잘 이뤄지고 있는지 확인하고자 함.
- 6개월 이내: 7.1%
- 1년 이내: 35.7%
- 2년 이내: 0%
- 3년 이내: 0%
- 없음: 57.1%

● 업무 목적외 자료수집 : 위탁자가 업무에 상관없는 개인신용정보를 제공하는지 확인하고자 함.
- 제공받지 않음: 92.9%
- 제공받음: 7.1%

● 제공받는 자료현황 : 수탁자가 제공받는 자료가 개인신용정보인지 확인하고자 함.
- 이름: 92.9%
- 핸드폰번호: 92.9%
- 생년월일: 35.7%
- 주소: 64.3%
- 주민등록번호 71.4%
- 계좌번호: 21.4%
- 카드번호: 28.6%
- 기타 7.1%

● 자료 수집방법 : 위탁자로부터 개인신용정보를 어떠한 방식으로 제공받는지 확인하고자 함.
- 전자메일: 28.6%
- 출력물: 78.6%
- 기타: 21.4%

● 자료 파기관리 : 소송이 완료된 건에 대해서 개인신용정보를 어떻게 파기하고 관리하는지 확인하고자함.
- 자체파기만 수행: 42.9%
- 자체 파기후 위탁자에게 증적제출: 7.1%
- 관리하지 않음: 50%

설문조사를 통해 알 수 있듯이 영세수탁자의 경우 연간 정보보호투자금액이 100만원 미만인 수탁자가 85.7%로 정보보호 투자에 미흡한 것을 알 수 있으며 위탁자 정보보호 실태 점검여부에서 점점 받지 않은 수탁사가 57.1%로 위탁자의 의무인 관리·감독이 소홀하다는 것을 알 수 있다. 자료수집 시에도 전자메일(28.6%) 또는 출력물(78.6%)로 제공받고 있어 자료유출 가능성이 있으며 자료에 대한 파기관리 또한 관리하지 않음 50%로 소홀하다.

본 논문에서 클라우드컴퓨팅 이용을 통한 영세수탁자 개인신용정보 보호 방안을 연구하고자 하는 사유는 설문조사에서 수탁자가 위탁받는 금융회사의 수가 3개 이상인 수탁자의 응답이 85.7%로 수탁자 한 곳이 여러 금융회사의 업무를 위탁받아 처리하는 것을 알 수 있다. 서론에서도 언급한 봐와 같이 위탁자가 수탁자를 관리·감독해야한다면 수탁자가 안전한 절차 또는 환경에서 위탁자의 개인신용정보를 처리할 수 있도록 신용카드사들이 클라우드컴퓨팅을 이용하여 클라우드 내에 공동으로 시스템을 구축하고 수탁자에게 제공함으로서 수탁자의 정보보호 수준을 높일 수 있기 때문이다.

2.5 관련 연구

이보성 외(2015)는 클라우드 서비스 유형별 개인

정보보호 방안 마련을 위해 클라우드 서비스 유형에 따른 개인정보 저장 방식의 차이를 분석하여 서비스별로 개인정보의 위·수탁 관계를 달리해야 하며 클라우드 서비스 유형에 따라 개인정보 처리 및 보호방안을 달리해야 한다고 시사하고 있다[3].

권오식 외(2016)는 수탁자의 정보 처리 및 관리를 담당하는 직원은 위탁자의 직원으로 간주하고 주기적이고 정기적인 정보보호 관리체계의 준수여부를 상시적으로 점검하고 개인 정보 보호에 대한 정기교육도 시행해야 개인정보 유출사고를 미연에 방지 할 수 있을 것이라 하고 있다. 여기서 시사점은 위·수탁 시 수탁자의 보안관리체계가 위탁자의 보안관체계 수준보다 낮다고 판단하여 위탁자의 수준만큼 강화해야 한다는 것을 의미한다[4].

손태현 외(2014)는 기업이 수탁자를 관리하고 있는 대부분의 부서가 계약을 담당한 현업부서이며 실질적 관리 감독 등의 책임지고 있다. 이러한 계약 주체에 따른 구조적 취약점 때문에 수탁자의 정보보호 수준 및 관리 감독 역량 저하의 요인으로 작용하고 있어 내부보다는 외부의 전문기관의 수행이 객관적 평가 관리를 제언했다. 수탁자 보안관리체계의 수준을 높이기 위해서는 내/외부 전문 인력이 관리 감독하는 것이 필요하다는 것을 시사하고 있다[5].

고영대 외(2015)는 개인정보 위·수탁 업무의 다양성, 개인정보의 처리를 위탁하는 위탁자 및 위탁받는 수탁자의 비즈니스 환경, 업체 규모 등의 현실적인 요소들의 고려하여 각 단계별 발생 가능한 보안위험에 대해 보안관리 프레임워이 필요하다는 것을 시사하고 있다[6].

박준현 외(2016)는 기업이 클라우드 기술 중 하이브리드 방식 활용 시 기술성, 경제성, 효율성에서 많은 이점을 지니고 있으며 해당 기술을 사용하기 위해서는 보안대책 마련 및 클라우드 기술을 정확히 파악하고 어느 분야에 활용하는 것인지가 중요하다는 것을 시사하고 있다[7].

위 관련 논문들을 보면 클라우드 서비스 유형에 따른 정보보호 및 수탁자의 보안수준을 높이기 위해서 위탁자의 관리·감독하는 부분을 많이 연구했다. 하지만 영세수탁자에 대한 정보보호 관리방안에 대한 연구는 많이 미흡하다. 이에 이 논문에서는 영세수탁자에 대한 개인신용정보 보호방안을 클라우드컴퓨팅 이용 및 가상사설망(VPN)을 통해 도출한다.

III. 클라우드컴퓨팅 기반 개인신용정보 보호 방안

먼저 영세수탁자들이 위탁자의 개인신용정보를 어떤 방식으로 처리하는지에 대해 설명하고, 이 과정에서 어떠한 보안위협이 있는지를 제시하며, 결과적으로 클라우드컴퓨팅을 이용해 영세수탁자의 개인신용정보 보호방안을 제시하고자 한다.

3.1 영세수탁자의 보안위협

영세수탁자가 가지는 보안위협을 도출하기 위하여 먼저 수탁자가 위탁자의 업무를 수행함에 있어 어떤 단계를 거치는지 확인할 필요가 있다. 이를 일반적으로 개인신용정보 라이프사이클로 구분되는데, 구체적인 내용은 Fig.1.과 같다.

Fig. 1. Personal (credit) information lifecycle

위 그림을 기준으로 영세수탁자가 가지는 보안위협은 간략히 정리하면 다음 페이지 Table 2.와 같다.

3.1.1 수집 단계에서의 보안위협

수탁자는 위탁자로부터 위탁자의 개인신용정보를 제공받고 이는 개인신용정보 라이프사이클에서 수집단계에 해당한다고 볼 수 있다. 수집단계에서는 위탁자가 전용선 또는 가상사설망(VPN)을 통해 전자적인 형태로 전송하거나, 이동형저장매체, 전자메일, 출력물을 통해 전달하는 방식이 있다. 현재 위탁자가 전자메일 또는 출력물로 자료를 제공하고 있으며 이

Table 2. Summary of security threat based on personal credit information lifecycle

Step	Security threats	
	Technical aspects	Administrative aspect
Collection	Eavesdropping, Messageforgery modulation, Senderrecipient modulation	Lack of management for data collection
Use	Other than the person in charge due to data sharing can read	Available for non-business purposes
Third party provision	Information leakage by trustees	
Delegation	Information leakage by the trustee and lack of supervision and supervision of the trustees	
Management	Security Solution and CERT Not Operated	Insufficient internal control procedures for data management
Destruction	Absence of destruction management system	There is nothing to destroy due to the mistake of the person in charge

에 따른 취약점 다음과 같다.

기술적인 측면에서의 위협으로는, 자료 수집단계에서 자료를 암호화하지 않고 전자메일로 제공함으로서 발생할 수 있는 취약점은 크게 3가지로 정리할 수 있다. 첫 번째는 도청이다. 도청은 전자메일 전송을 위한 통신이 공용인터넷을 통해 이루어지기 때문에 공격자가 전자메일에 대해 가로챌 수 있다. 송신자와 수신자 네트워크 구간에 여러 중간 시스템과 통신 링크를 통해 전자메일이 이동하게 되는데 이때 보안 통신 채널이 없어 공격자가 전송 중인 데이터를 검색할 수 있으며 수동으로 도청할 수 있다[8]. 두 번째는 메시지 위·변조이다. 공격자가 전자우편의 내용을 편취 또는 위조하거나 변조하여 수신자에게 메시지의 내용을 오인하도록 할 수 있다. 공격자는 송신자와 수신자 사이에서 전자메일 통신의 기본 개념을 손상시킬 수 있을 뿐만 아니라 전송 된 전자메일의 내용을 수정할 수 있기 때문에 무결성을 잠재적으로 손상시킬 수 있다. 또한 공격자는 편취한 전자메일을 수신자를 대상으로 릴레이하지 않거나 위·변조된 메시지를 전달할 수 있다[8][9]. 마지막으로 송·수신자 변조이다. 공격자가 노출 회피를 위해 합법적인 전자메일 사용자의 신원으로 명의 변경 후 악의적인 메시지를 송신할 수 있다. 대부분의 송·수신자는 합법적인 사용자로 보낼 때 누군가 자신의 신원을 가장 한 사실을 알 수 없다. 또한 전자 메일은 합법적인 전자메일과 악의적인 전자메일이 구별되지 않기 때문에 탐지하기가 매우 어렵다[8][9][10].

관리적 측면에서는 제공받은 자료에 대한 반입 및 자료 관리 프로세스가 존재하여야 하나 정산을 위한 문서 및 스캔 본만 관리되고 있다. 실제 제공받은 자료에 대한 제공처, 제공자, 수신처, 수신일시, 수신담당자 등 문서 관리를 위한 프로세스가 미흡하여 자료 분실 등으로 인한 유출가능성이 존재한다.

3.1.2 이용 단계에서의 보안위협

수탁자가 위탁자의 업무를 처리하기 위해 위탁자의 개인신용정보를 처리하는 단계에 해당한다. 수탁자는 수집한 자료를 담당자 업무PC 또는 공유PC에 저장함으로써 열람 권한이 없는 담당자가 문서를 열람할 수 있다.

기술적 측면에서는 소송을 위한 관리시스템이 구축되어 있지 않기 때문에 수집한 자료를 일반PC에 저장하고 공유하여 사용하고 있으며 파일에 대한 권한 관리가 이뤄지지 않아 권한이 없는 담당자도 열람이 가능하다. 열람 횟수 및 출력 횟수를 관리할 수 없으므로 출력 및 복사로 인한 유출 가능성이 존재한다.

관리적인 측면에서 위탁자의 개인신용정보에 대해 위탁받은 업무목적외 이용이 가능할 수 있다.

3.1.3 제3자 제공 단계에서의 보안위협

수탁자가 위탁자의 개인신용정보를 처리한 후 이를 또 다른 제3자인 법원 등에 제공하는 단계가 있다. 개인신용정보를 법원에 제출 시 제출과정에서 분실 및 복사에 대한 유출가능성이 존재한다.

관리적인 측면에서 위탁자의 개인신용정보가 업무목적에 따른 제3자가 아닌 다른 제3자에게 제공됨으로서 정보유출 가능성이 있다.

3.1.4 처리위탁 단계에서의 보안위협

수탁자가 위탁자의 개인신용정보를 처리함에 있어 필요할 경우 아르바이트인력 등 수탁자 소속 직원이 아닌 자를 통해 재위탁하는 단계가 있다. 3.1.3에서 살펴 본봐와 같이 법원에 제출 시 제출과정에서 분실 및 복사에 대한 유출가능성이 존재한다.

관리적인 측면에서 재수탁자에 대한 개인신용정보 처리에 따른 적법한 관리감독을 수행하는지 여부가 보안위협이 될 수 있다. 즉, 재수탁자에 대한 재위탁자로서의 관리·감독 의무를 준수할 필요가 있다.

3.1.5 보관 단계에서의 보안위협

수탁자가 위탁자의 개인신용정보를 처리한 결과, 처리에 필요한 자료를 출력물형태 또는 전자적인 형태로 보관하는 단계가 있다. 개인신용정보를 보관하는 업무PC가 인터넷에 연결되어 악성코드 및 지능형 위협공격을 통한 자료 유출 가능성이 존재한다.

기술적인 측면에서 출력물로 자료제공 시 신용카드사는 수탁자가 제공받은 자료에 대한 유출을 제어할 수가 없다. 수탁자는 위탁자로부터 제공받은 개인신용정보 자료를 스캔 받아 소송 및 비용정산을 위하여 사용자PC에 저장한다. 본 논문 2.3의 보안관리실태 점검에서 알아본 봐와 같이 PC가 인터넷에 연결 되어 있지만 최신패치가 적용되어 있지 않거나, 백신이 미설치 되어 있어 악성코드 및 지능형 위협공격을 통한 개인정보유출 가능성이 있다.

관리적인 측면에서는 수탁자가 개인신용정보 자료에 대한 유출 방지를 위한 선관의 의무를 다하는지 여부가 보안위협이 될 수 있다. 즉 개인신용정보 자료 유출방지 위한 회사 내의 내부통제 절차를 준수할 필요가 있다.

3.1.6 파기 단계에서의 보안위협

수탁자가 위탁자의 개인신용정보를 처리한 후 처리목적이 달성되거나 위탁자에게 처리결과를 제공하는 등을 통해 수탁자가 소유하는 위탁자의 개인신용정보를 파기하는 단계가 있다. 수탁자가 법원제출이나 오출력으로 인한 파기 시 위탁자는 개인신용정보가 실질적으로 파기되었는지 확인할 방법이 없다.

기술적인 측면에서는 파기관리시스템이 구축되어 있지 않기 때문에 실제 미파기에 따른 정보유출 가능성이 있다.

위탁받은 업무목적이 달성됨에 따른 위탁자의 개인신용정보를 파기하였는지 여부가 위협이 될 수 있다.

3.2 보안위협에 대한 대응 모델 제안

영세수탁자가 가지는 보안위협에 대해 3.1에서 개인신용정보 라이프사이클별로 살펴봤다. 보안 위협에 대한 대응방안을 간략하게 정리하면 Table 3.과 같으며 Fig.2.를 통해 영세수탁자의 보안위협에 대한

Table 3. Summary of Responding to security threats by Personal Credit Information Lifecycle

Step	Security threats	Countermeasures	Cloud computing technology
Collection	Eavesdropping, Messageforgery modulation, Sender recipient modulation	Securing confidentiality and integrity through virtual private network (VPN)	virtual network security appliance, Site-to-Site VPN, Client VPN
Use	Other than the person in charge due to data sharing can read	granting of access	virtual network security appliance, Multi-Factor Authentication(MFA), Identity and Access Management(IAM)
Third party provision	Information leakage by trustees	Copy protection with output security	Install and operate output security system in the cloud
Delegation			
Management	Security Solution and CERT Not Operated	Use of built-in security service	Security Center
Destruction	Absence of destruction management system	Construction of destruction management system	Operation of cloud destruction management system in the cloud

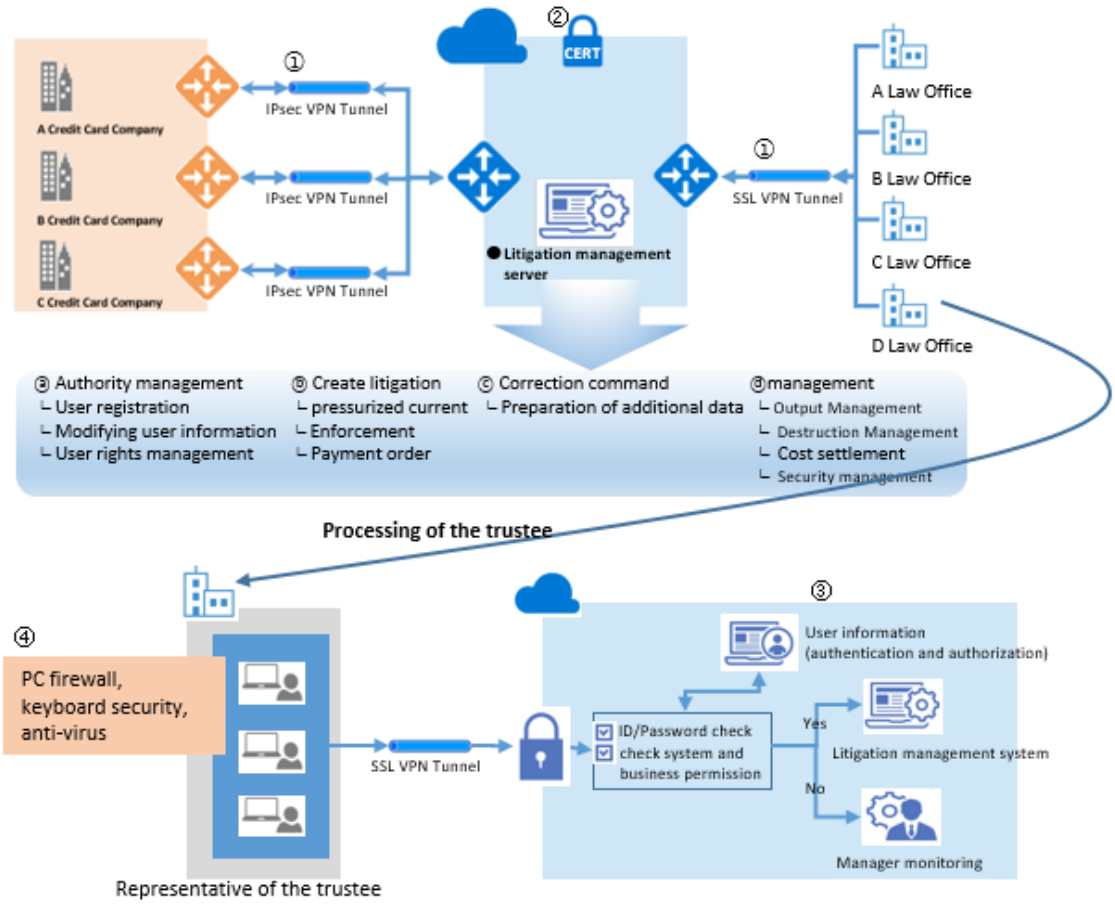

Fig. 2. Model for countermeasures against security threats

대응 모델을 제안하고 설명하고자한다.

3.2.1 수집 단계에서의 보안위협 해결방안

수집단계의 보안위협을 간략하게 정리하면 자료를 암호화하지 않고 전자메일로 제공함으로서 도청, 메시지 위·변조, 송·수신자 변조가 가능했으며 출력물로 제공함으로서 분실 등으로 인한 유출 가능성이 존재 했다. 이를 해결하기 위한 방법으로 Fig.2.의 ①에서 가상사설망(IPsec VPN, SSL VPN)[11][12][13]을 사용함으로서 기밀성과 무결성[14][15][16][17]을 확보하여 보안위협을 대응할 수 있다. 클라우드컴퓨팅에서 이를 적용하기 위한 기술로는 Virtual network Security Appliance[19]와 Site-to-Site VPN[20], Client VPN[20]를 통하여 구현할 수 있다.

3.2.2 이용 단계에서의 보안위협 해결방안

이용단계의 보안위협을 간략하게 정리하면 개인신용정보 자료에 대한 접근통제가 미흡하여 권한 없는 담당자가 문서를 열람할 수 있는 취약점이 존재했다. 보안위협에 대한 대응방안으로 Fig.2.의 소송관리시스템 → ⓐ권한관리에서 부여한 권한관리를 ③에서 사용자 인증 시 사용자별 접근권한이 부여된 메뉴 및 문서에 한하여 접근가능토록 함으로서 담당자외 접근을 통제할 수 있다. 또한 Fig.2.의 ④PC방화벽, 백신, 키보드 보안을 설치하여 수탁자의 업무용 PC의 안전성을 확보한다. 이를 적용하기 위한 기술로는 Virtual network Security Appliance[19]와 MFA(Multi-Factor Authentication)[19], IAM(Identity and Access Management)[20]

를 통해 구현할 수 있다.

3.2.3 제3자 제공 및 처리위탁 단계에서의 보안위협 해결방안

제3자 제공 및 처리위탁 단계에서의 보안위협을 간략하게 정리하면 개인신용정보가 업무목적에 따른 제3자가 아닌 다른 제3자에게 제공됨으로서의 정보유출 가능성 및 재수탁자에 의한 정보유출 가능성이 존재한다. 보안위협에 대한 대응방안으로는 Fig.2.의 소송관리시스템 → ⓓ관리 → 출력물관리에서 출력물 횟수를 부여한다. Fig.2.에서 사용자 인증 시 사용자별 접근권한이 부여된 문서에 접근가능하게하고 해당문서의 출력 횟수를 관리함으로서 통제할 수 있으며 문서에 대한 통제는 Fig.2.의 소송관리시스템에 문서보안솔루션[18]을 설치·운영함으로서 통제가 가능하다. 다만 출력된 문서의 분실 또는 복사에 대해서는 통제가 불가능하다.

3.2.4 보관 단계에서의 보안위협 해결방안

보관단계의 보안위협을 간략하게 정리하면 개인신용정보를 보관하는 업무PC가 인터넷에 연결되어 악성코드 및 지능형 위협공격을 통한 자료 유출 가능이 존재한다. 업무PC에 개인신용정보를 보관하지 않고 Fig.2.의 소송관리시스템에 저장함으로써 개인신용정보를 보호할 수 있으며 개인신용정보에 접근하는 PC는 Fig.2.의 ④를 통해 안전성을 확보한다. 또한 Fig.2.의 ②에서 보안전문인력 및 보안관제서비스를 통해 모니터링 함으로써 악성코드 및 지능형 위협공격에 대응할 수 있다.

3.2.5 파기 단계에서의 보안위협 해결방안

파기단계의 보안위협을 간략하게 정리하면 수탁자가 법원제출이나 오출력으로 인한 파기 시 위탁자는 개인신용정보가 실질적으로 파기되었는지 확인할 방법이 없다는 것이다. 보안위협에 대한 대응방안으로는 수탁자가 소송관련 자료를 법원에 제출했을 경우 접수증을 스캔 받아 등록하거나 오출력으로 인한 파기의 경우 파기 동영상을 촬영하여 등록함으로서 출력건수와 파기등록건수를 Fig.2.의 소송관리시스템 → ⓓ관리 → 파기관리에서 관리할 수 있다.

3.3 기대효과

제안한 모델이 기존 작업방식의 대한으로 가능한지, 영세수탁자 입장에서 정보보호가 강화되면서 소요되는 비용의 절감효과가 있는지, 영세 수탁자가 작업을 함에 있어 시간과 공간의 제약이 없는 편이성이 있는지 등에 대해 확인하기 위하여 본 논문 2.4에서와 마찬가지로 설문 조사를 실시하였고, 설문항목 및 설문조사 결과는 다음과 같다.

- 클라우드 사용에 따른 효과 : 클라우드 사용 시 수탁자에 미치는 효과를 확인하고자 함.
  - 편의성 증대(언제 어디서든 접근가능): 78.6%
  - 비용절감 효과(업무처리를 위한 위탁사방문 등): 50%
  - 업무의 효율성(업무자동화): 78.6%
  - 정보보호 수준 향상(클라우드 내 보안서비스 사용): 71.4%
  - 기타: 14.3%

클라우드컴퓨팅 이용에 따른 효과로 언제 어디서든 시간과 공간에 제약을 받지 않고 업무를 할 수 있는 편의성에 대해 78.6%로 긍정적으로 답하였으며, 업무자동화를 통해 위탁자에 방문하거나 수작업 서류관리 등 비용절감효과에 대해서는 50%로 실제 구축되지 않아 체감효과를 느끼지 못한 것으로 판단된다, 업무자동화를 통한 업무의 효율성 증대는 78.6%, 수탁자는 위탁자가 클라우드 내 구축한 시스템에 접근하여 업무처리 시 클라우드 서비스에서 제공하는 보안관제 등을 사용함으로써 정보보호가 향상 될 것이라는 응답이 71.4%로 해당 모델이 효과적일 것으로 나타났다.

위 설문조사 결과 수탁자가 클라우드컴퓨팅을 이용함으로서 정보보호 수준 향상 및 업무프로세스 개선을 통한 업무 효율화에 도움이 된다는 것을 알 수 있다. 또한 위탁자 입장에서도 수탁자가 클라우드컴퓨팅을 이용함으로서 수탁자에 대한 관리·감독을 클라우드에서 할 수 있기 때문에 관리·감독에 대한 시간과 비용도 줄일 수 있고 각기 다른 수탁자의 정보보호 수준을 일정한 수준으로 향상 시킬 수 있어 해당 제안모델은 다른 수탁자에 대해서도 확대 가능할 것으로 판단된다.

IV. 결 론

본 논문에서는 신용카드사들이 업무를 영위하기 위해 많은 업체와 위·수탁 계약을 체결하고 있다는 것을 살펴봤다. 글로벌 보안컨설팅 전문업체 포네몬 인스터튜트 2017년 조사보고서에 따르면 '외부업체 때문에 해킹 사고가 발생한 적이 있다'고 대답한 기업 비율이 세계에서 56%에 달했다고 한다[21]. 이 보고서에서 의미하는 것은 공격자는 기업들을 대상으로 직접적인 공격보다는 이들 기업과 수탁계약을 맺은 업체를 통해 우회하는 방법을 활용하고 있다는 것을 알 수 있다.

침해사고를 예방하기 위해 위탁자는 수탁자를 관리·감독해야 하는 법적 의무가 있으나 수탁자 중 영세수탁자는 전산설비 부족 및 보안장비 도입 시 과도한 비용으로 인해 합리적인 협의안을 도출하기에는 현실적인 한계가 있다. 따라서 신용카드사인 위탁자가 자신의 개인신용정보를 보호하기 위해 현실적인 비용과 노력으로 수탁자를 관리적·기술적 측면에서 관리할 수 있는 방안으로 클라우드컴퓨팅 이용 방안을 제시하였다.

신용카드사들이 위·수탁계약을 맺어 업무를 영위할 수밖에 없는 것이 현실이라면 각기 다른 수탁자의 보안수준에 맡기기 보다는 전문인력 및 변화하는 위협에 빠르게 대처할 수 있는 클라우드컴퓨팅을 이용함으로서 보안이 강화되길 기대한다.

References

[1] Seung Ik Baek and Ji Yeon Shin and Jong Woo Kim, "Exploring the Korean Government Policies for Cloud Computing Service," The Journal of Society for e-Business Studies, 18(3), pp. 2, Aug. 2013

[2] Hye-Ji Do, "A Study on Cloud Computing for Financial Sector limited to Processing System of Non-Critical Information: Policy Suggestion based on US and UK's approach," The Journal of Society for e-Business Studies, 22(4), pp. 40, Nov. 2017

[3] Bosung Lee and Beomsoo Kim, "Protection of Personal Information on Cloud Service Models," Journal of The Korea Institute of Information Security & Cryptology 25(5), pp. 1245-1255, Oct. 2015

[4] O-shik Kwon, "A study on consignee/consigned party management system enhancement for information technology outsourcing," Conference on Information and Communication Equipment, pp. 1-3, Sep. 2016

[5] Taehyun Son and Jungsun Park, "A Study on Improving Information Security Implementation of IT Brokerage Company," Korea Safety Management Science Conference Fall Conference, pp. 357-365, Sep. 2014

[6] Youngdai-dai Ko and Sang-jin Lee, "A Proposal of Enhanced Personal Information Security management Framework of Consigning of Personal Information," Journal of The Korea Institute of Information Security & Cryptology, 25(2), pp. 383-393, Apr. 2015

[7] Jun Hyun Park and Jae Sung Park, "Enterprise Hybrid Cloud Technology and Security Trends," Journal of The Korea Institute of Information Security & Cryptology, 26(1), pp. 81-91, Feb. 2016

[8] Ignacio Sanchez, Apostolos Malatras, Iwen Coisel, "A security analysis of email communications," JRC TECHNICAL REPORT, pp. 33-38, Dec. 2015

[9] Hang Hu and Gang Wang, "Revisiting Email Spoofing Attacks," arXiv: 1801.00853v1 [cs.CR] 2, pp. 2, Jan. 2018

[10] Korea Internet Security Agency, "In-depth analysis of new vulnerability of convergence industry," pp. 26-27, Dec. 2017

[11] Tripti Sharma and Rahul Yadav, "Security in Virtual private network Computer," International Journal of Innovations & Advancement in Computer Science IJIACS ISSN 2347 - 8616, Vol. 4, special issue, pp. 669-675, Mar. 2015
[12] Ritika kajal and Deepshikha Saini and Kusum Grewal, "Virtual Private Network," International Journal of Advanced Research in Computer Science and Software Engineering Vol. 2, no. 10, pp. 428-432, Oct. 2012
[13] Baljot Kaur Chawla and O.P. Gupta, B. K. Sawhney, "A Review on IPsec and SSL VPN," International Journal of Scientific & Engineering Research, Vol. 5, no. 11, pp. 21-24, Nov. 2014
[14] Jemal Mohammed Tahir, "Testing Virtual Private Network (VPN) Interoperability," Metropolia university of applied sciences, pp. 35, May. 2015
[15] S. Kent, "IP Authentication Header," https://tools.ietf.org/html/rfc4302, Dec. 2005
[16] S. Kent, "IP Encapsulating Security Payload (ESP)," https://tools.ietf.org/html/rfc4303, Dec. 2005
[17] Munhui Kang and Taemung Jung, "VPN technology overview," Conference Proceedings of the Korea Institute of Information Security and Cryptology, 9(4), pp. 6, 1999
[18] Korea Internet Security Agency, "Client Service Security," pp. 18, 2017
[19] Microsofte Azure, "Azure Security documentation," https://docs.microsoft.com/ko-kr/azure/security/, May. 2019
[20] AWS, "Identity and Access Management for AWS Security Hub," https://docs.aws.amazon.com/securityhub/latest/userguide/security-iam.html, May. 2019
[21] "60% of companies hacked through business partners...Launched BitSite service to confirm security to partner companies," TECH M, Jun. 2019
[22] "Report on site inspection results of consignors in the first half of 2018," Jun. 2018.

〈저자소개〉

김 시 인 (Shi-in Kim) 정회원
1999년 2월: 한서대학교 전산정보학과 졸업(학사)
2017년 9월~현재: 고려대학교 정보보호대학원 석사과정
2015년 4월~현재: (주)우리카드 정보보호부 재직
〈관심분야〉 전자금융보안, 전자금융법규, 보안위험분석

김 인 석 (In-Seok Kim) 정회원
1973년 2월: 홍익대학교 전자계산학과 졸업(학사)
2003년 2월: 동국대학교 정보보호학과 졸업(석사)
2008년 2월: 고려대학교 정보경영공학과 졸업(박사)
2009년~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 전자금융보안, IT감사, 전자금융법규