금융회사의 고유식별정보 암호화 규제·감독에 대한 실효성 확보 방안

이 승 윤*, 김 인 석**

요 약

본 연구의 목적은 금융기관 대상 고유식별정보 암호화 규제 및 감독에 대한 효과적인 대응방법을 제시하고, 현재의 문제점 그리고 앞으로 나아가야 할 방향을 제시하는 것이다. 금융기관에서는 법규준수를 위하여 다수의 개인정보처리시스템 중 DB시스템을 중심으로 대응하고 있어 그 외 다수의 어플리케이션시스템 내 고유식별정보를 포함하고 있는 데이터 파일의 경우 암호화 등 추가적인 조치가 필요한 것으로 조사되었다. 본 연구에서는 제도적, 관리적, 기술적 실효성 확보 방안을 결론에서 제시 하였다.

Effective measures for the regulation and supervision of encryption of unique identification information of financial companies

Seung Yun Lee*, In Seok Kim**

ABSTRACT

The purpose of this study is to propose effective countermeasures against the regulation and supervision of unique identification information for financial institutions and present the present problems and future directions. In financial institutions, it is investigated that DB system of many personal information processing systems is in order to comply with the law, and additional measures such as encryption are required for data files containing unique identification information in many other application systems. In this paper, the conclusions of institutional, administrative, and technological feasibility are presented.

Key words : Unique identification information, DB system, File system, Encryptoin

접수일(2018년 10월 10일), 게재확정일(2018년 12월 14일)

* 고려대학교/금융보안학과(주저자)

** 고려대학교/금융보안학과(교신저자)

1. 서 론

사물인터넷, 빅데이터, 인공지능, 클라우드 등의 핵심기술로 대변되는 4차산업혁명 시대는 초연결(hyper-connected)성을 바탕으로 다양한 분야에서 개인정보를 수집, 활용하고 있으며, 정보제공자가 인지하지 못하는 정보들도 실시간으로 수집 및 활용될 수 있다. 따라서 이렇게 수집된 개인정보의 경우 관련법규에 따라 잘 관리되어야 하나 지속적으로 해킹, 내부 관계자 등을 통해 개인정보 침해 및 유출이 발생하고 있어 개인정보보호의 중요성과 필요성이 높아지게 되었다. 그 중에서도 금융회사의 경우는 금융거래의 특수성으로 수집되는 정보가 상대적으로 타 산업에 비해 가치가 높아서 더욱더 엄격한 기준으로 개인정보를 관리해야 하며, 개인정보의 유출 시 기업 이미지실추, 소비자 단체 불매운동, 집단손해배상청구등 기업경영에 큰 타격을 받게 된다[1]. 2018년 1월 1일부터 개인정보보호법 제 24조 3항에 의거 일정규모 이상의 금융회사는 고유식별정보 암호화 조치를 준수해야 한다. 따라서 금융회사는 법규사항을 이행해야 하나, 금융회사의 현실은 다수의 복잡 다양한 형태로 개인정보처리시스템을 운영 및 보유하고 있어 의도하지 않거나 또는 관리상의 실수로 고유식별정보를 암호화 등 안전성 확보에 필요한 조치를 이행하지 못하는 경우가 발생할 수 있어 이에 대한 실질적인 이행조치가 필요한 상황이다. 본 연구의 목적은 실제 금융회사에서 고유식별정보 암호화 대응방안을 살펴보고 현재의 문제점을 파악하고, 실효성 있는 법이행 조치를 위한 효과적인 방안을 제시하고자 한다.

2. 고유식별정보 암호화 규제·감독 사항 및 금융회사 이행 현황

2.1 고유식별정보 암호화 대상 및 규제·감독 사항

2.1.1 고유식별정보 암호화의 법적배경 및 규제목적

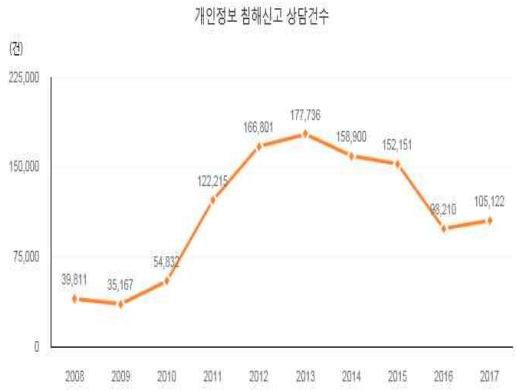
개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호하기 위하여 2011년 3월 29일 제정 및 동년 9월 30일 개인정보보호법이 시행 되었다 [2]. 이 법 시행 시 개인정보처리자는 정보주체에게 별도 동의를 받은 경우 또는 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우를 제외하고 처리할 수 없도록 하였으며, 개인정보처리자가 고유식별정보를 처리하는 경우에는 암호화 등 안전성 확보에 필요한 조치를 하도록 하였다. 그러나 2011년 싸이월드 개인정보 유출사건, 2014년 KT 고객정보 유출사건, 2014년 카드3사 개인정보 유출사건 등 지속적으로 대규모 개인정보 유출사건이 발생하자, 이로 인하여 사회문제가 되고 있고 특히 카드3사 개인정보 유출 사건을 계기로 금융회사의 개인 신용정보에 대한 과도한 수집·활용 및 허술한 전산보안에 대한 우려가 제기 되어 관계부처 합동으로 금융분야 개인정보 유출 재발방지 종합대책이 발표(2014년 3월)되었으며, 재발방지를 위한 대책으로 주민번호 과다노출 관행 개선을 위해 보관방식을 금융회사는 수집한 주민번호를 외부망은 물론 내부망에도 암호화하여 보관· 이용하도록 하였다[6]. 그리고 암호화 적용 시기는 개인정보보호법 제24조2제2항 및 동법 시행령 제21조의2에 의거 100만명 이상의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자는 2018년 1월 1일부터 암호화를 적용하도록 개정(2014년 3월) 되었다[2].

따라서 일정규모 이상의 민간분야 즉 인터넷서비스 제공업체(ISP)와 금융분야의 금융기관이 해당 한다.

또한, 개인정보처리자가 주민등록번호 등 고유식별정보를 법에서 정한 것 과 같이 안전하게 보관하고 있는지를 확인하기 위해 개인정보보호법 시행령 제21조(고유식별정보의 안전성 확보조치)에 따라 공공기관 또는 5만명 이상의 고유식별정보를 처리하는 자는 행정안전부장관으로 하여금 동법 제24조제4항에 따른 안전성 확보에 필요한 조치를 하였는지 2년마다 1회 이상 조사하도록 개정(2016년 3월)하였다.

2.1.2 고유식별정보 안전조치 미이행에 따른 피해 사례

2008년부터 2017년 까지 고유식별정보를 포함한 개인정보 침해신고 건수는 2013년 177,736건으로 가장 높게 나타났으며, 이후 2014년부터 2016년 까지 조금씩 낮아지다가 2017년 105,122건으로 다시 증가추세로 돌아서고 있음을 알 수 있다.



(Fig 1) Number of personal information infringement notification counseling [10][12].

또한, 전체 침해사고 신고 건수 중 고유식별정보에 해당하는 주민등록번호 등 타인 정보의 도용에 관한 건수가 전체 침해 건수에서 차지하는 비율이 2013년 72.6%, 2017년 60.1% 등으로 매년 가장 높음을 알 수 있다. 이는 개인정보가 해킹 등을 통해 유출되었을 경우 주민등록번호를 포함하는 고유식별정보를 이용하거나 타겟으로 범죄에 악용됨을 알 수 있으며, 이를 방지하기 위하여 고유식별정보의 안전성 확보조치가 무엇보다도 중요한 것임을 알 수 있다.

<Table 1> Ratio of the number of theft of other information such as resident registration number [10][12]

Year	Total number (A)	Number of theft of personal information such as resident registration number (B)	Ratio (B/A)
2017	105,122	63,189	60.1%
2016	98,210	48,557	49.4%
2015	152,151	77,598	51.0%
2014	158,900	83,126	52.3%
2013	177,736	129,103	72.6%

고유식별정보 안전조치 미이행에 다른 피해사례로는 2017년 9월 하나투어 개인정보 유출사건이 있으며, 기술적·관리적 안전조치를 위반으로 인해 약 49만명의 개인정보가 유출되었으며, 이중 42만명의 주민등록번호가 포함된 것으로 개인정보보호법 제정이래 최초로 과징금(3억2,725만원)이 부과되었으며, 이는 정부가 개인정보 유출사고에 대한 국민의 불안감을 해소하고 기관의 보안의식 제고를 위해 지속적으로 개인정보 계도활동과 실태점검을 강화해 나가기위한 조치로 볼 수 있다.[7]

2.2 금융회사 고유식별정보 암호화 이행 현황

2.2.1 금융회사 암호화 추진 방안과 적용범위

금융회사 암호화 추진은 2014년 카드3사 개인정보 유출사건으로 발단된 금융분야 개인정보 유출 재발방지 종합대책과 개인정보보호법 개정으로 인하여 2015년도부터 본격적으로 시작하여 2017년 말까지 모두

<Table 2> Examples of damages resulting from the implementation of unique identification information safety measures since 2014 [7][8][9].

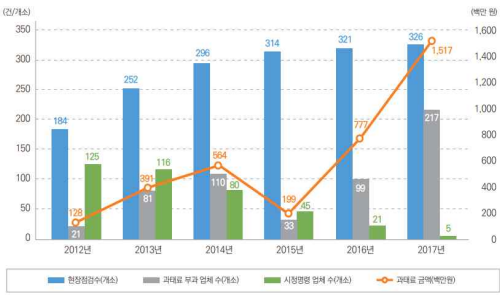
Division	Time	Spill information	Punishment
Hana Tour personal information leakage accident	September 2017	420,000 resident registration number leaked	Penalty of 327.25 million won Fines paid 18 million won
East Soft Personal Information Leak Incident	September 2017	1.66 million account information leakage and secondary damage occurred	Penalty of 112 million won Fines paid 10 million won
Personal information leak through KT homepage hacking	February 2014	12 items including 11.7 million resident registration numbers leaked	Penalty of 70 million won Fines paid 15 million won

완료하였다[17]. 금융회사는 통상 10년 주기로 차세대 프로젝트를 추진해 오고 있어, 프로젝트 시기가 빠른 금융사(전북은행, 경남은행, 신한은행)의 경우 암호화 적용시기가 빠르며, 개별 금융사별 차세대프로젝트 시기에 암호화를 포함하여 추진(농협은행, 하나은행, 우리은행)하거나, 암호화를 위한 자체 TFT를 구성(기업은행)하여 추진하였다[16][17].

금융회사의 고유식별정보 암호화 방안은 첫째 고유식별정보 대신 대체번호(고객번호)로 대체하는 방안, 둘째 DB암호화 솔루션을 적용하는 방안, 셋째 자체 업무별 암호화 알고리즘을 이용하는 방안 중 업무별 특성을 고려하여 선택하여 적용할 수 있다. 그리고 암호화를 적용 할 때에는 암호화에 따른 성능저하를 최소화 할 수 있도록 현 시스템의 자원사용률 및 네트워크 응답속도 등 현황을 사전에 파악하여 서비스 적용 시 업무 영향도를 최소화해야 한다[13].

금융회사의 암호화 적용범위에 대한 해석은 신용정보와 관련하여「신용정보의 이용 및 보호에 관한 법률」정보통신서비스와 관련하여「정보통신망 이용촉진 및 정보보호 등에 관한 법률」그 외 개인정보와 관련하여 일반법인「개인정보보호법」의 적용을 받게 되며, 좀 더 세부적으로는 개인정보의 안전성 확보조치 기준, 개인정보의 기술적·관리적 보호조치 기준, 전자금융감독규정에서 각각 요구하는 사항을 충족할 수 있도록 하여야 한다[3][4][5]. 정보보호와 관련된 유사한 법률 및 고시와의 적용방법이나 순서의 불투명, 관련 법령간의 관계 등으로 체계적으로 고유식별정보를 안전하게 관리하기에 어려움이 많다[14]. 2018년 1월 1일부터 고유식별정보에 대하여는 내부망, 외부망에 상관없이 모든 구간에서 안전한 암호화 조치가 필수사항이 되었다. 행정안전부에서는 2011년 9월 개인정보 보호법 시행 이후 안전한 개인정보 이용환경 조성을 위해 개인정보 관리실태 현장점검을 실시하고 법 위반 시 행정처분을 실시하는 등 점점 규제를 강화해 나가고 있음을 알 수 있다[11].

(Fig. 2) 2012~2017 On-site inspection, penalty charge and correction order change.[11].



따라서 금융회사는 2017년 연말까지 완료한 고유식별정보 암호화 추진사항이 잘 이행되었는지 여부를 점검해 볼 필요가 있다. 점검대상은 DBMS의 컬럼 내 데이터에 대한 암호화 뿐 만 아니라 데이터베이스 시스템과 함께 개인정보처리시스템을 이루고 있는 어플리케이션시스템 내의 로그파일, 송수신파일, 백업파일 등으로 확대하여야 할 것이다.

2.2.2 A금융회사 고유식별정보 암호화 이행 현황

본 연구에서는 A금융회사를 대상으로 개발시스템과 DMZ(Demilitarized Zone, 이하 'DMZ'라 한다) 구간 내 시스템을 대상으로 개인정보 검색솔루션(Enterprise Recon)을 이용하여 총 903대의 파일시스템을 대상으로 고유식별정보에 대한 안전성 확보조치가 되어 있는 지를 조사하였다.

개발시스템 744대를 검색한 결과 극히 일부파일에서 암호화가 적용되지 않고 검출된 고유식별정보 중 개발시스템 내 테스트용 주민등록번호가 검출된 건수 대비 42%로 가장 높은 비율을 보였으며, 시스템 로그(26%), 파일전송용 데이터(17%), 미사용 파일 등 기타(13%)순으로 조사 되었다.

<Table 3> Percentage by type of encryption non-action in development system

NO	TYPE	RATIO
1	Resident registration number for test	42%
2	System Log	26%
3	Data for file transfer	17%
4	Data for backup	1%
5	Business related files	1%
6	Etc(end of work, unused)	13%

DMZ 구간 내 시스템 총 159대를 대상으로 검색한 결과 극히 일부파일에서 암호화되지 않고 검출된 고유식별정보 중 Log file에서 검출된 주민등록번호가 78%로 가장 높은 비율을 보였으며, 미사용 백업데이터(20%), 웹서버 내 첨부파일(2%), 미사용 HTML 또는 화면스크립트 파일 또는 소스파일이 1%미만 비율로 암호화되지 않은 것으로 조사 되었다.

<Table 4> Percentage by type of encryption non-action in DMZ section system

NO	TYPE	RATIO
1	Log file	78%
2	Unused backup data	20%
3	Attachments file	2%
4	Unused HTML file	Less than 1%
5	Unused screen scrip file	
6	Source file	

암호화되지 않고 보관 된 파일 중 대부분을 차지하는 로그파일의 경우 고유식별정보를 포함하지 않도록 로그생성 로직을 변경하여 조치 완료하였으며, 기타 불필요한 미사용 파일의 경우에는 삭제 처리하여 모두 조치 완료하였다. 로그파일의 경우 업무담당자가 해당파일에 고유식별정보가 남아 있는지 모르는 사례가 있었으며, 대부분의 미사용 파일은 오래된 파일로 담당자 변경 등으로 인지하지 못하는 경우, 해당업무가 종료된 이후 삭제 처리가 안 된 경우였다.

3. 금융회사 고유식별정보 암호화 실효성 확보방안

3.1 제도적 실효성 확보방안

고유식별정보 암호화와 관련하여 관련 법규, 규정, 해설서 등에 따르면 고유식별정보를 안전한 알고리즘을 이용하여 암호화해야 한다 라고만 표현되어 있으며, 행정안전부의 고유식별정보처리자 안전성 확보조치 관리실태 조사 및 방송통신위원회 점검 시 개인정보처리시스템의 DB시스템을 위주로 점검하고 있어, 내부시스템 내 다른 어플리케이션 시스템에 저장·보관 되고 있는 파일은 방치될 수 있는 리스크가 있다.

이는 고유식별정보를 포함한 개인정보 유출사고의 원인이 내부 DB시스템을 타켓으로 불법적인 DB 접속을 통해 정보를 해킹하는 경우도 있으나, 일부는 내부자와 공모하여 접근통제가 강화된 DB시스템이 아닌 다량의 중요정보를 포함한 파일을 타켓으로 유출을 시도할 수 있다.

따라서 고유식별정보 처리에 따른 보호조치 대상을 확대 반영하여 DB에 저장된 데이터뿐 아니라 개인정보처리시스템을 이루고 있는 어플리케이션 시스템 전체를 대상으로 해야 하며, 관계기관 감독 및 점검 시에도 비정형화된 파일시스템까지 고려되어야 할 것이다.

3.2 관리적 실효성 확보방안

금융회사의 경우 서비스를 제공하기 전 다양한 형태의 테스트 목적으로 개발시스템을 별도로 운영하고 있으며, 이러한 목적의 개발시스템 경우 일반적으로 운영시스템에 비해 상대적으로 접근통제 및 보안정책이 동일하게 관리되지 않거나, 해당 데이터의 경우 암호화 추진 이전에 생성된 것으로 장기간 방치 될 수 있어 개인정보 유출 관점에서는 리스크가 더 크다고 할 수 있다. 따라서 금융회사는 개발시스템을 통한 개인정보유출 리스크를 해소하기 위해서 개발시스템을 운영시스템과 동일한 수준으로 관리 될 수 있도록 내부관리체계를 수립하여야 하며, 업무 담당자는 개발시스템 내 암호화되지 않은 불필요한 고유식별정보가 있는지 지속적으로 확인할 수 있도록 해야 한다.

3.3 기술적 실효성 확보방안

금융회사의 경우 개인정보처리시스템을 이루는 수많은 다양한 형태의 어플리케이션 시스템들이 존재하며, 앞서 조사한 결과에서 알 수 있듯이 로그파일, 백업파일, 송수신파일 등 다양한 형태로 고유식별정보를 포함하는 데이터 파일이 존재하고 있다. 따라서 안전하게 보관되지 않고 있는 고유

식별정보가 있는지 여부를 담당자가 자체적으로 확인하고 조치하기에는 많은 인력과 시간을 필요로 하며 그 실효성 또한 매우 낮을 수밖에 없다[15]. 따라서 개인정보를 포함하여 고유식별정보 보관여부를 효율적으로 검색해 주는 보안솔루션을 이용하여 안정적으로 시스템 영역까지 확대하여 주기적으로 고유식별정보 보관여부를 검색 할 수 있으며, 식별된 데이터파일은 불필요한 경우 삭제 처리하며 불가피한 경우에는 안전하게 암호화하거나 또는 대체번호로 변경함으로써 고객의 중요한 정보를 안전하게 관리 할 수 있으며, 설령 해킹으로부터 정보가 유출되더라도 타인명의 인터넷 회원 가입, 스팸메일, 신분증 위조와 같은 2차 피해를 방지 할 수 있을 것이다[13].

4. 결 론

본 연구에서는 금융회사의 개인정보 안전성 확보조치에 대한 규제·감독사항, 현황, 문제점을 도출하였으며, 금융회사의 개발시스템과 DMZ구간 내 시스템을 대상으로 암호화 등 안전성 확보조치가 미흡할 수 있는 유형에 대한 조사를 진행하였으며, 본론에서는 제도적, 관리적, 기술적 실효성 확보방안을 제시하였다. 개인정보보호법 개정에 따라 법규 준수 이행여부를 확인하기 위해 행정안전부 등 관련기관의 실태조사는 더욱 확대되고 강화되고 있으므로, 금융회사는 본 연구에서 제안하는 고유식별정보 암호화 실효성 확보방안을 통하여 금융고객의 개인정보를 안전하게 보관 할 수 있을 것이다.

하지만 좀 더 다양한 금융회사를 대상으로 운영시스템 전반으로 확대하여 연구를 진행한다면 좀 더 객관적이고 합리적인 방안을 제시할 수 있을 것으로 기대한다.

참고문헌

[1] Nam seon-mo, Effective Measures for Damage Prevention of Leakage of Personal Information, Research on Victims' Studies, Vol. 23, No. 3, pp.75-97, December 2015.

[2] National Law Information Center(www.law.go.kr), Personal Information Protection Act, October 19, 2017. Act on the Use and Protection of Credit Information, August 18, 2014. Act on Information Network Promotion and Information Protection, etc., September 18, 2018.

[3] Ministry of Public Administration and Security Notification No. 2017-1, Standards for Securing Personal Information Security, July 27, 2017.

[4] Broadcasting Commission Notice No. 2015-3, Technical and Administrative Protection Measures of Personal Information, May 19, 2015.

[5] Financial Services Commission Notice No. 2016-37, Electronic Financial Supervisory Regulation, October 5, 2016.

[6] Relevant department joint "Comprehensive measures to prevent recurrence of personal information leaks in financial sector" March 2014.

[7] Press release (Ministry of Public Administration and Security)(www.mois.go.kr) Decision of administrative disposition by Hana Tour private information leakage accident, February 6, 2018.

[8] Korea Communications Commission (KCC) press release (www.kcc.go.kr), security company East Soft personal information leak accident prevention, March 28, 2018.

[9] Korea Communications Commission (KCC) press release (www.kcc.go.kr), KT's violation of personal information protection regulations, June 26, 2014.

[10] Korea Communications Commission e-Nara Index, "Number of Personal Information Infringement Complaints", July 15, 2018.

[11] Ministry of Public Administration and Security, Korea Internet & Security Agency, 2013 ~ 2017 Personal Information Survey and Administrative Disposition Casebook, April 2018.

[12] Kim, Yong Ho, "A study on strengthening security management to secure personal information security", Graduate School of Information Communication, Konkuk University, August 2018.

[13] Han Se-jin, An Impact and Problem by the Personal Information Protection Act. on the Financial Sector, Convergence Security Journal, Vol. 13, No. 1, pp. 32-26, March 2013.

[14] Kang Yoon-woo, Problems and Improvement of Personal Information Protection Law in Bank, Graduate School of Law, Korea University, June 2013.

[15] Jeong-Min Lee, In-Seok Kim, Design and Implementation of Financial Security Automatic System for Privacy Information of Financial Institution, The Journal of The Institute of Internet, Broadcasting and Communication, Vol. 15, No. 6, pp.25-30, December 2015.

[16] Jung Ki-suk, "A Study on Prevention of Personal Information Leakage in Financial Institutions," Convergence Security Journal, Vol. 14, No. 4, pp110-116, June 2014.

[17] Gil jae-sik, "100% encryption of financial sector, resident registration number", electronic newspaper, December 14, 2017.

〔저자소개〕

이 승 윤 (Seung-yun Lee)
2002년 2월
부경대학교 전자정보통신공학과 학사
2017년 3월~현재
고려대학교 정보보호대학원 금융보안학과 석사과정
email : yunny1lsy@gmail.com

김 인 석 (In-seok Kim)
1973년
홍익대학교 전자계산학과 학사
2003년
동국대학교 정보보호학과 석사
2008년
고려대학교 정보경영공학과 박사
2009년~현재
고려대학교 정보보호대학원 교수
email : iskim11@korea.ac.kr