情 報 保 護 學 會 誌
第23卷 第1號, 2013. 2

금융권 개인정보 활용 실태와 개인정보보호법 시행에 따른 IT컴플라이언스 준수방안 연구

이 병 수*, 황 지 상**, 황 동 욱***, 최 봉 철****, 홍 용 진*****

요 약

국내 시중에는 약 304개 금융회사가 금융 및 보험 상품 서비스를 제공하고 있으며, 최근 금융감독원에서는 국내 304개 금융회사(생·손보 39개사)를 대상으로 한 개인정보수집·이용제공 동의서 운영실태 점검 결과 총 49개 금융회사에서 문제점이 발견되었다.[1] 2012. 2. 17일 개정된 정보통신망 이용촉진 및 정보보호 등에 관한법률에서는 본인인증확인기관, 법령에서 별도로 수집·이용하는 경우와 방송통신위원회가 고시하는 경우 이외에는 주민등록번호의 사용을 제한하고 있다. 본 연구에서는 국내 개정된 정보보호 관련 법률 관점에서 현 금융회사의 개인정보 활용 및 그에 따른 보안 실태를 연구하고 관련 결과에 따른 법적 IT컴플라이언스를 준수할 수 있는 개인정보 치환 및 관리 방법론 등 관련 법률과 기업의 사회적 책임(CSR)[2]을 만족시킬 수 있는 방안을 제언하고자 한다.

Ⅰ. 서 론

국내 시중에는 다양한 금융상품을 온/오프라인에서 가입할 수 있도록 인터넷 서비스를 제공하고 있으며, 이에 대한 상품을 이용하기 위해 서비스 소개 및 판매, 사은 행사 및 판촉 행사에 이용한 개인정보 활용에 대한 가입 동의서를 받는다. 관련 기업이나 기관은 이러한 정보를 바탕으로 가입자의 성향분석을 통해 이메일을 이용한 사용자 타깃 마케팅(Target Marketing)을 수행 한다. 금융회사는 발송된 이메일 내부에 포함된 관련 상품 및 데이터를 인구통계학적 분석 기법을 토대로 개개인이 가지고 있는 관심분야에 대한 맞춤 서비스 제공하고 자동 수집된 정보를 분석하여 방문자 대비 구매율(CVR)[3] 제고를 목표로 하고 있다.

국내 카드社에서는 아래 [그림1]과 같이 타깃 마케팅(Target Marketing)을 위한 광고 홍보메일을 전송하고 있으며, 본 분석 결과에 따르면 해당 메일 본문에는 국내법에 저촉되는 내용을 포함하고 있다. 본 논문에서는 금융회사(신용카드, 보험사)에서 발송하는 이메일에서 개인정보 수집과 관련하여 개인정보 활용의 적법성과 운영 실태에 관한 연구 수행하고, 2.1장에서는 국내 신용카드 현황을 소개, 2.2장에서는 개인 정보 수집 방법론, 2.3장,2.4장에서는 2012년 8월 18일부터 시행되는 정보통신 이용촉진 및 정보보호 등에 관한 법률, 개인정보보호법 관점에서 대응 방안을 모색하고자 한다.

〔그림1〕 광고홍보 메일의 예

* SK플래닛 IT팀 (bscry@sk.com)
** 아주IT 정보전략기획팀 (jshwang@aju.co.kr)
*** 딜로이트 안진회계법인 리스크자문본부 (donghwang@deloitte.com)
**** 중앙경찰학교 (mikorea@hotmail.com)
***** 윈스테크넷 침해사고분석팀 (yad2nus@wins21.co.kr)

Ⅱ. 본 론

2.1 금융회사 광보홍보 실태에 관한 연구

2.1.1 금융회사의 경제활동인구 수 및 신용카드 수

금감원 조사결과 국내에는 304개 금융회사(생·손보 39개사)가 금융 및 보험 등의 서비스를 제공하고 있다. 통계청, 금융감독원 보고 자료에 따르면 2010년 기준 신용카드를 이용한 경제활동 인구수는 24,784명[4]에 달하며 금융감독원 기준 11년 말 有실적 카드 기준(無실적 휴면카드 제외)으로 9,103만매[5]에 달하는 신용카드가 사용되고 있다. 국내 1인당 신용카드 보유 개수는 평균 4.7개로서 금융회사에서는 약 1,936만 명의 개인정보를 수집·보유·활용하고 있음을 알 수 있다. 이 자료를 토대로 각 금융회사 및 기업의 개인정보활용 실태를 점검 한다.

통계청 기준 신용카드 매수는 아래 [그림 2]와 같으며, 경제활동 인구 1인당 신용카드 소지 수가 4.7매임을 알 수 있다.

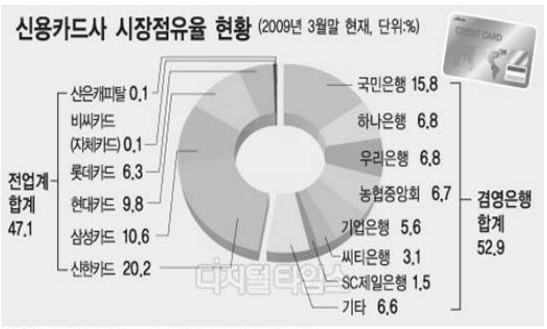
연도	추계인구(A) (천 명)	경제활동인구(B) (천 명)	신용카드 수 (천 매)	경제활동인구 1인당 신용카드소지 수 (매)	가맹점 수주) (천 점)
1990	42,869	18,539	10,384	0.6	–
1991	43,296	19,109	12,099	0.6	–
1992	43,748	19,499	14,705	0.8	–
1993	44,195	19,806	19,401	1.0	–
1994	44,642	20,353	25,314	1.2	–
1995	45,093	20,845	33,278	1.6	–
1996	45,525	21,288	41,113	1.9	–
1997	45,954	21,782	45,705	2.1	–
1998	46,287	21,428	42,017	2.0	–
1999	46,617	21,666	38,993	1.8	–
2000	47,008	22,134	57,881	2.6	–
2001	47,353	22,471	89,330	4.0	–
2002	47,615	22,921	104,807	4.6	1,479
2003	47,849	22,957	95,220	4.1	1,547
2004	48,082	23,417	83,456	3.6	1,495
2005	48,294	23,743	82,905	3.5	1,529
2006	48,497	23,978	91,149	3.8	1,611
2007	48,692	24,216	89,565	3.7	1,749
2008	48,606	24,347	96,248	4.0	1,853
2009	48,747	24,394	106,993	4.4	1,871
2010	48,874	24,748	116,589	4.7	2,082

주) 가맹점으로부터의 매출전표 매입건수 1건 이상(연간) 발생기준(2002년부터)
자료 : 통계청, 금융감독원(카드사 제출 업무보고서), 여신금융협회

〔그림 2〕 금융회사의 경제활동인구 수 및 신용카드 수 - 통계청

2.1.2 신용카드社 별 시장점유율 및 개인정보 수집현황 분석

다음으로, 신용카드社 시장점유율 현황[6]을 보면 신한카드 20.2%, 국민카드 15.8%로 1, 2위를 점유하고 있으며, 금번 연구대상인 BC카드(자체카드 만)와 현대해상, 롯데카드의 시장 점유율은 각 각 0.1%, 9.8%, 6.3%로 전체시장의 16.2%를 점유하고 있는 것으로 보이지만 BC카드社의 지불결제서비스를 이용하고 있는 11개 회원사(우리은행, Standard Chartered, 하나SK카드, NH농협카드, IBK기업은행, KB국민카드, 대구은행, 부산은행, 경남은행, Citibank, 신한카드)를 포함할 경우 약 58.2%의 시장점유율(Standard Chartered, 하나SK, 대구은행, 부산은행, 경남은행 제외)을 나타내고 있다. 실제 BC카드의 경우 2012년 8월 기준 4,240만 명의 고객을 보유[7] 하고 있음을 알 수 있으며, 전 국민의 84%의 개인정보를 활용하여 영업활동을 수행하고 있음을 알 수 있다.



〔그림 3〕 신용카드社 시장점유율 디지털타임즈 보도자료

상기 분석결과를 토대로 일부카드사와 통계자료에는 포함되지 않는 생보기업을 대상으로 개인정보의 활용범위와 개인정보 노출 여부에 대한 연구 분석결과를 다루도록 한다.

2.1.3 신용카드社 별 개인정보 노출 취약점 현황

2.1.2 항목에서 살펴본 바와 같이 국내 최대 시장점유율 및 개인정보 보유현황을 토대로 개인정보의 노출여부를 아래 [표 1]과 같이 확인 하였다.

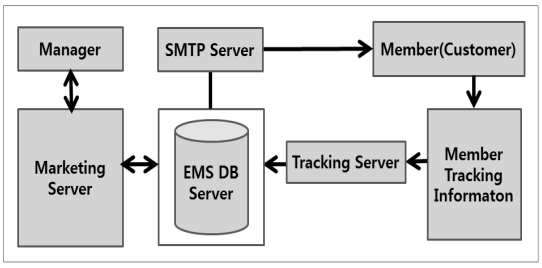
분석 결과 국내에서 다수의 개인정보를 보유하고 있는 A社에서 “정보통신망 이용촉진 및 정보보호 등에 관한 법률”제23조의 2 (주민등록번호의 사용 제한) 항에 위법사항이 적용되고 있으며, 개인의 주민등록 번호를 타깃 마케팅(Target Marketing)의 구분자로 활용하고 있는 것으로 확인된다.

〔표 1〕 기업별 개인정보 노출여부 분석 결과

조사대상	유출 유무	비 고
A社	O	BASE64로 인코딩된 주민등록번호
B社	X	발견되지 않음
C社	X	발견되지 않음
D社	X	발견되지 않음
E社	X	발견되지 않음
F社	X	발견되지 않음
G社	O	BASE64로 인코딩된 주민등록번호
H社	X	발견되지 않음
I社	X	발견되지 않음
J社	O	BASE64로 인코딩된 주민등록번호

2.1.4 금융회사 광고홍보를 위한 홍보메일 발송/분석시스템의 구조

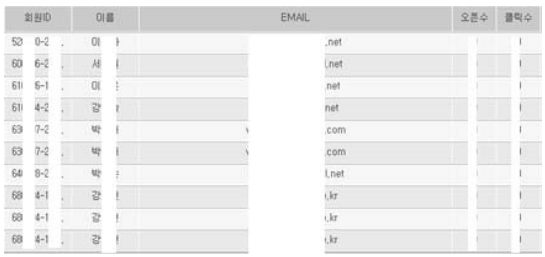
2.1.3 장에서 언급한 A社와 G社, J社에는 국내에서 개발된 홍보메일 발송/분석 시스템(EMS, e-Mail Marketing Solution)을 이용하고 있으며, 그 구조는 아래 [그림 4]와 같다.



〔그림 4〕 홍보메일 발송/분석 시스템의 구조

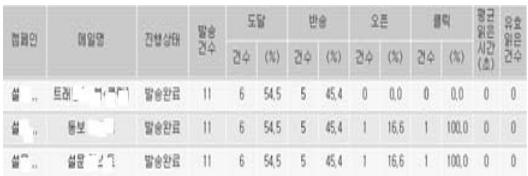
① 마케팅 서버 : 마케팅 관리자를 위한 사용자 UI(User Interface)를 제공하며, 마케팅 활동에 필요한 메일 등록, 대상자 맵핑, 발송 스케줄 등을 설정한다.
② 트래킹서버 : 트레킹 서버는 발송된 마케팅 메일에 대해 사용자의 응답에 대한 내용을 홍보 메일 발송/분석 시스템 DB에 저장한다.
③ SMTP서버 : 메일 발송에 필요한 작업을 수행한다.
④ 홍보 메일 발송/분석 시스템 DB 서버 : 각 서버들에서 사용되는 정보를 저장하는 역할을 수행한다.

홍보메일 발송/분석 시스템은 기업에서 진행하는 이벤트 및 홍보에 대한 기획을 진행하고 개인정보 중 변하지 않는 개인식별정보 값(Key, 주민등록번호)을 선정한다. 발송 시스템은 마케팅 서버에 식별한 키(Key, 주민등록번호) 값과 수신되는 고객의 메일 주소 간 상관관계를 설정함으로서 E-Mail A가 주민등록번호 B임을 설정하여, 향후 고객이 E-Mail을 열람하였을 경우 개인을 식별할 수 있도록 아래 [그림 5]와 [그림 6]과 같이 구성되어 있다.



〔그림 5〕기업별 개인정보 노출여부 연구 결과

기업은 위와 같이 설정된 정보를 가진 수신분석용 Key값을 포함하여 전체 고객을 대상으로 메일을 전송하고, 해당 메일을 수신한 고객은 해당 메일의 내용을 열어 메일에 포함된 사이트나 이미지 링크를 클릭하여 정보를 확인한다. 이 과정에서 고객이 마케팅 메일에 포함된 사이트나 이미지를 누르는 경우 해당 메일 내에 포함된 키 값과 광고 유형을 분석서버로 전송하며, 서버는 해당 고객을 식별하게 되고 이에 대한 정보를 Tracking서버로 전달하여 홍보메일 발송/분석 시스템 DB에 저장한다. 홍보메일 발송/분석 시스템서버에는 발송 고객이 메일을 수신하였는지, 해당 링크를 클릭하였는지에 대한 정보를 확인하여 향후 마케팅 자료로 사용된다.



〔그림 6〕 메일 열람여부 확인 및 클릭 분석

2.2 카드社 광고홍보 시스템 취약점 및 개인정보 유출 연구

1장에서 살펴본 홍보메일 발송/분석 시스템은 시중

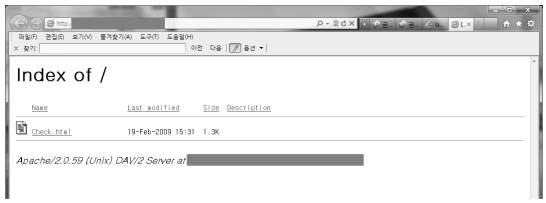
금융회사 중 3개 기업에서 사용하는 것으로 확인되었으며, 상세 내역은 아래 [표 2]과 같다. 주목할 점은 B社의 경우 개인식별정보인 주민등록 번호를 사용하지 아니하고 자체 식별 정보를 생성하여 내부 DB에서 개인을 식별하도록 구성되어 있어 안전한 것으로 확인 되었다.

〔표 2〕 기업별 개인정보 노출여부 연구 결과

조사대상	EMS사용여부	비고
A社	O	
B社	X	자체생성 식별정보 활용
C社	X	
D社	X	
E社	X	
F社	X	
G社	O	
H社	X	
I社	X	
J社	O	

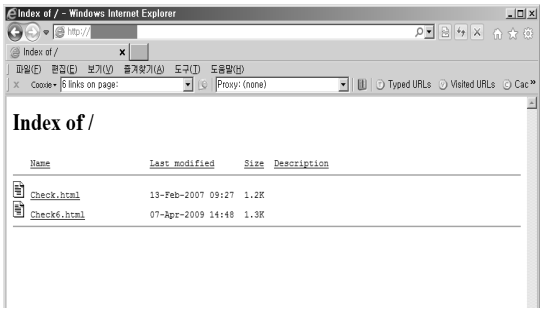
2.2.1 홍보메일 발송/분석시스템의 취약점을 이용한 개인정보 유출 공격

분석 결과 A社, G社, J社에서 사용하는 홍보메일 발송/분석시스템의 취약점이 아닌 “전자금융감독규정시행세칙 제13조(홈페이지 등 공개용 서버 관리대책)”에서 규제하고 있는 공개용 웹 서버에 대한 보호조치가 아래 [그림 7]과 같이 이루어지지 아니한 것으로 확인되었다.

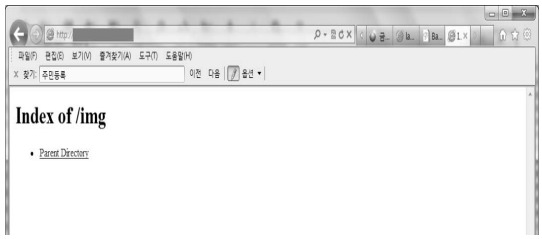


〔그림 7〕 G社의 공개용 웹 서버의 디렉터리 취약점

악의적 공격자는 각 카드社 홍보메일 발송/분석 시스템 웹 서버에 존재하는 자체 취약점을 이용하여 개인정보의 유출을 시도할 수 있으며, 해당 시스템이 위치하고 있는 동일한 네트워크 대역의 서버에 침투하여 카드社의 주요 정보를 수집할 수 있는 가능성이 확인되었다.



〔그림 8〕 J社의 공개용 웹 서버의 디렉터리 취약점

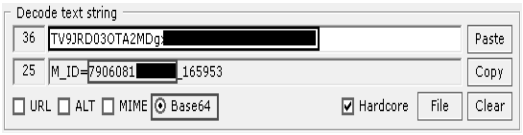


〔그림 9〕 A社의 공개용 웹 서버의 디렉터리 취약점

2.2.2 홍보메일 발송/분석시스템의 취약점을 이용한 개인정보 수집 증명

연구를 위해 A社의 E-Mail 메시지를 분석하고 포함된 개인식별정보(주민등록번호)를 Decoding 하여 분석하고, 대량으로 개인정보 수집 가능성을 증명한다. 카드社는 아래 [그림 10]와 같은 구조로 홍보 메일 전송한다. 광고 또는 메일 본문 내부에는 광고클릭에 대한 정보를 수집서버로 전송되는 링크와 Key값이 포함되어 있다. 해당 링크에는 어떠한 사용자가 해당 링크를 사용하였는지 식별하기 위한 목적으로 주민등록번호가 Base64로 인코딩 되어 사용된다. 다음은 메일 내용 중 일부이다.

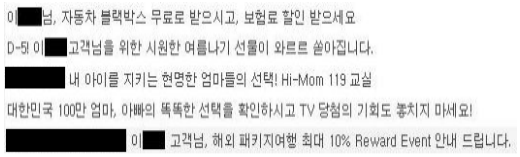
〔그림 10〕 A社의 광고메일 내용 일부 발췌



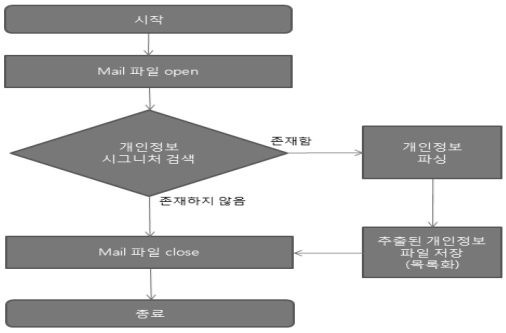
〔그림 11〕 디코딩된 주민등록 번호

[그림 10]에서 붉은색으로 표시된 부분이 바로 주민등록 번호이며, 인코딩 방식으로 되어 있어 본 메시지를 획득하면 누구나 손쉽게 디코딩이 가능한 취약한 방식을 이용하고 있다. 아래 [그림 11]은 메일내용에서 획득한 개인식별정보를 디코딩한 결과이다.

[그림 11]에서 붉은색으로 표시된 부분이 주민등록 번호이며 790618-1xxxxxx 으로 디코딩 된 것을 확인할 수 있다. 또한 메일 상·하단부에 포함되는 개인의 이름을 획득하여, 1개의 메일을 통해 개인의 성명과 주민등록번호를 획득 할 수 있다. 연구 활동 중 조사된 광고메일에서는 사용자 이름을 별도의 조치 없이 평문 그대로 포함되어 있는 것으로 확인되었다. 아래 [그림 12]은 사용자의 이름을 포함된 이메일 화면이다.

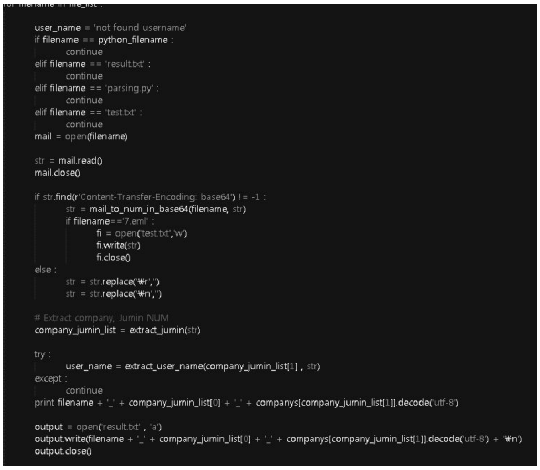


〔그림 12〕 평문으로 전송되는 사용자 이름 정보



〔그림 13〕 개인정보수집 흐름도

지금부터 확인된 메일 정보를 이용하여 개인정보 수집가능성을 증명하도록 한다. 아래 [그림 13]는 개인정보를 수집하기 위한 순서도로서 공격자가 전송한 악성코드를 사용자가 실행하였을 경우를 구현하였다. 위 흐



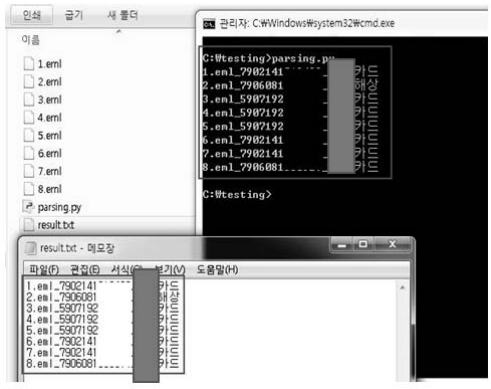
```
    user_name = 'not found username'
    if filename == python_filename :
            continue
    elif filename == 'result.txt' :
            continue
    elif filename == 'parsing.py' :
            continue
    elif filename == 'test.txt' :
            continue
    mail = open(filename)

    str = mail.read()
    mail.close()

    if str.find('Content-Transfer-Encoding: base64') != -1 :
            str = mail_to_num_in_base64(filename, str)
            if filename=='7.eml' :
                    fi = open('test.txt','w')
                    fi.write(str)
                    fi.close()
    else :
            str = str.replace('\r','')
            str = str.replace('\n','')

    # Extract company, Jumin NUM
    company_jumin_list = extract_jumin(str)

    try :
            user_name = extract_user_name(company_jumin_list[1] , str)
    except :
            continue
    print filename + '_' + company_jumin_list[0] + '_' + companys[company_jumin_list[1]].decode('utf-8')

    output = open('result.txt' , 'a')
    output.write(filename + '_' + company_jumin_list[0] + '_' + companys[company_jumin_list[1]].decode('utf-8') + '\n')
    output.close()
```

〔그림 14〕 개인정보수집용 악성코드 작성

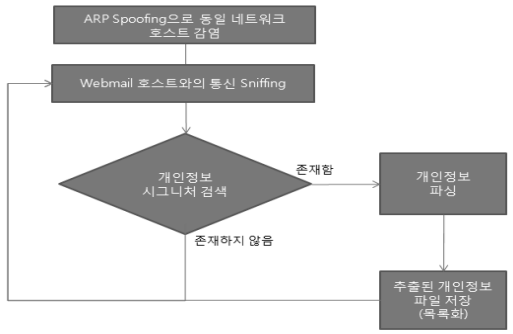
름도에서 개인정보 수집을 위해 작성 가능한 처리 함수는 다음과 같다. 아래 스크립트에는 각 카드社에서 사용하는 광고 클릭 이벤트 수집 서버URL을 기준으로 가장처음 적용되는 24글자의 Base64 인코딩 문자열을 파싱 하며, 파싱된 문자열을 Base64 디코딩하여 해당 사용자의 주민등록 번호를 반환 하도록 한다.

위 [그림 14]은 개인정보 수집을 위한 악성 스크립트로서 본 논문의 목적을 위해 작성되었으며, 어느 금융회사에서 발송된 것인지 확인하기 위한 Flag(company_flag변수)를 포함하여 반환하게 된다.

사용자의 PC에서 상기 스크립트를 실행하면 아래 [그림 15]와 같이 개인정보수집 스크립트를 통해 실제 메일 데이터에서 개인정보 수집이 가능한 것이 확인 되었다. 본 연구에 사용된 스크립트는 별첨으로 첨부 되어 있다. 아래 790214-101xxxx으로 시작하는 붉은색부분



〔그림 15〕 개인정보수집 성공 화면



〔그림 16〕 G社의 네트워크 모니터링을 통한 개인정보 수집 공격 흐름

이 추출된 개인정보이며 “주민등록번호_카드社명” 순으로 출력된 화면이다.

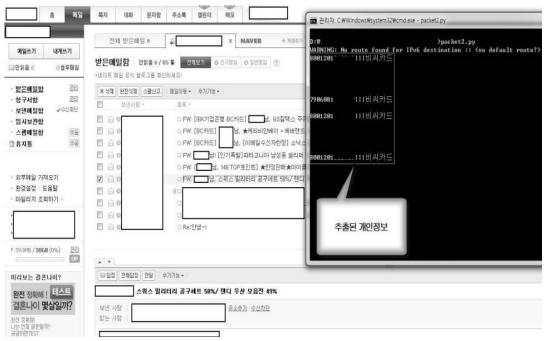
2.2.3 네트워크 기반을 이용한 개인정보 수집공격

2.2.1 장 개인정보를 취급하고 있는 홍보메일 발송/분석 시스템의 직접적 취약점을 공격하는 기법과, 2.2.2 장에서 언급한 악성코드 유포를 통한 방법 이외에도 네트워크를 이용한 개인정보 수집 가능성도 확인 되었다. 이는, 각 기업에서 전송하는 개인식별정보(주민등록번호)를 암호화 하거나 일방향성 HASH함수를 사용하지 않음으로서 발생되는 문제점으로서, 악의적인 공격자는 ARP Spoofing을 이용하여 사용자의 외부(인터넷)통신을 가로채어 해당 내용을 도청할 수 있는 공격과 병행하여 개인정보 수집이 가능하다. 공격자는 Sniffing된 통신 패킷의 데이터를 조합 한 뒤 해당 내용에서 개인정보를 추출 한다. [그림 16]은 ARP Spoofing 이후 사용자의 네트워크 활동을 모니터링 함으로서 사용자의 개인정보를 추출하는 흐름이다.

〔그림 17〕 네트워크 개인정보 수집용 공격코드 일부

공격자는 수집 효율성을 높이기 위해서 다수의 사용자가 이용하는 특정 네트워크 대역 또는 회사, 아파트 등을 도청 거점으로 이용하여 단시간 내 대량의 개인정보를 수집할 수 있다. 본 연구에서는 아래 [그림 17]과 같은 공격 코드를 작성하여 실제 한 기업 내 네트워크를 거점으로 이용하여 주민등록번호 수집이 가능하다.

아래 [그림 18]은 네트워크 기반에서 실제로 획득한 개인정보 목록이다.



〔그림 18〕 네트워크 개인정보 수집용 공격코드로 확보한 개인정보

2.3 개인정보보호법과 금융회사의 홍보 방식에 따른 법률적 고찰

2.2장에서 살펴본 바와 같이 국내 금융회사의 개인정보의 활용 범위와 그에 따른 개인정보 유출 가능성에 대하여 증명하였다. 본 2.3장에서는 기업 또는 기관이 준수하여야 하는 관련 법률 및 제도와 위법성에 대하여 고찰한다.

2.3.1 금융회사 광보홍보 방식에 따른 법률적 고찰

개인정보의 수집· 활용에 대한 법률은 정보통신망 이

용촉진 및 정보보호 등에 관한 법률, 시행령, 시행규칙과 개인정보 보호법, 시행령, 시행규칙 그리고 전자금융거래법, 시행령, 시행규칙으로 이루어져 있다. 관련 법률에는 아래 [표 3]와 같이 개인정보의 수집·활용을 규정하고 있으며, 상기 분석결과와 상관분석 결과 대부분의 법규를 위반하고 있는 실정이다.

〔표 3〕 개인정보보호 관련법규와 분석결과 간 상관분석 결과

관련법규	대분류	소분류	위법여부
정보통신망 이용촉진 및 정보보호 등에 관한 법률	제23조의2(주민등록번호의 사용제한)	① 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 이용자의 주민등록번호를 수집·이용할 수 없다. 1. 제23조의3에 따라 본인확인기관으로 지정받은 경우 2. 법령에서 이용자의 주민등록번호 수집·이용을 허용하는 경우 3. 영업상 목적을 위하여 이용자의 주민등록번호 수집·이용이 불가피한 정보통신서비스 제공자로서 방송통신위원회가 고시하는 경우	시행일 : 2012년 08월 18일
		② 제1항 2호 또는 제3호에 따라 주민등록번호를 수집·이용할 수 있는 경우에도 이용자의 주민등록번호를 사용하지 아니하고 본인을 확인하는 방법(이하 "대체수단"이라 한다)을 제공하여야 한다.	
전자금융감독규정 시행세칙	제13조(홈페이지 등 공개용 서버 관리 대책)	①금융기관 또는 전자금융업자는 공개용 서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다. 1. 공개용 서버를 내부 망과 분리하여 내부 망과 외부 망 사이(DMZ)에 설치하고 침입차단시스템으로 보호할 것 4. 안전진단프로그램 등을 이용하여 서버의 취약성 또는 무결성을 수시로 점검하고 원 내용과 상이 여부를 주기적으로 점검할 것	4절 위반
		②금융기관 또는 전자금융업자는 공개용 웹서버에 게재된 내용에 대하여 다음 각 호의 사항을 준수하여야 한다. 4. 개인정보의 유출, 위·변조 방지를 위한 보안조치 5. 직원 등이 운영하는 홈페이지에 대한 통제 강화	4절 위반
		③금융기관 또는 전자금융업자는 공개용 웹서버가 해킹공격에 노출되지 않도록 다음 각 호의 취약점에 대하여 적절하게 대응 조치하여야 한다. 1. 악의적인 명령어 주입 공격(SQL Injection) 2. 업로드 취약점 3. 취약한 세션 관리(Cookie Injection) 4. 악의적인 명령 실행(XSS) 5. 버퍼 오버플로우 6. 부적절한 파라미터 7. 접근통제 취약점 8. 부적절한 환경설정(서버 설정관련) 취약점 등	8절 위반
		④금융기관 또는 전자금융업자는 개인용 컴퓨터(PC) 등에서 음란, 도박 등 업무와 무관한 인터넷 사이트 접근에 대한 통제대책을 강구하여야 한다.	
개인정보보호법	제16조(개인정보의 수집제한)	① 개인정보처리자는 제15조제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.	
	제24조(고유식별정보의 처리제한)	① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 “고유식별정보”라 한다)를 처리할 수 없다. 1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우 2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우	1절 위반
		② 대통령령으로 정하는 기준에 해당하는 개인정보처리자는 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입할 경우 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.	
		③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.	3항 위반
		④ 행정안전부장관은 제2항에 따른 방법의 제공을 지원하기 위하여 관계 법령의 정비, 계획의 수립, 필요한 시설 및 시스템의 구축 등 제반 조치를 마련할 수 있다.	
	28조(개인정보의 보호조치)	① 정보통신서비스 제공자등이 개인정보를 취급할 때에는 개인정보의 분실·도난·누출·변조 또는 훼손을 방지하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다. 1. 개인정보를 안전하게 취급하기 위한 내부관리계획의 수립·시행 2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제장치의 설치·운영 3. 접속기록의 위조·변조 방지를 위한 조치 4. 개인정보를 안전하게 저장·전송할 수 있는 암호화기술 등을 이용한 보안조치 5. 백신 소프트웨어의 설치·운영 등 컴퓨터바이러스에 의한 침해 방지조치 6. 그밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치	4절 위반
		② 정보통신서비스 제공자등은 이용자의 개인정보를 취급하는 자를 최소한으로 제한하여야 한다.	
	제29조(안전조치의무)	개인정보처리자는 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.	기술적 조치 위반
	제30조(개인정보의 안전성 확보조치)	① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다. 1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치 3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 5. 개인정보에 대한 보안프로그램의 설치 및 갱신 6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치	3절 위반
		② 행정안전부장관은 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다.	
		③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 행정안전부장관이 정하여 고시한다	
개인정보의 안전성 확보조치 기준 행정안전부 고시 제2011-제43호	제7조(개인정보의 암호화)	① 제21조 및 영 제30조 1항 3호에 따라 암호화하여야 하는 개인정보는 고유식별정보, 비밀번호 및 바이오정보를 말한다.	고유식별정보의 암호화 위반
		② 개인정보처리자는 제1항에 따른 개인정보를 정보통신망을 통하여 송, 수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.	
		③ 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화 되지 아니하도록 일방향 암호화하여 저장하여야 한다.	
		④ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.	암호화 위반
		⑤ 개인정보처리자가 내부 망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다. 1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보영향평가의 결과 2. 위험도 분석에 따른 결과	
		⑥ 개인정보처리자는 제1항에 따른 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.	
		⑦ 개인정보처리자는 제3항, 제4항 및 제5항에 따른 개인정보 저장시 암호화를 적용하는 경우, 이 기준 시행일로부터 3개월 이내에 다음 각 호의 사항을 포함하는 암호화 계획을 수립하고, 2012년 12월 31일까지 암호화를 적용하여야 한다. 단 인터넷 구간 및 인터넷구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우 위험도 분석과 관계없이 암호화를 적용하여야 한다. 1. 개인정보의 저장 현황분석 2. 개인정보의 저장에 따른 위험도 분석절차(또는 영향평가 절차) 및 방법 3. 암호화 추진 일정 등	
		⑧ 개인정보처리자는 업무용 컴퓨터에 고유식별정보를 저장하여 관리하는 경우 상용 암호화소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.	

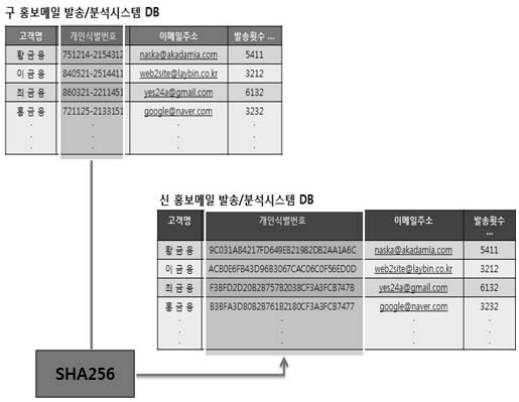
위 상관관계 분석결과를 보면 대부분 기술적 조치에 미흡한 것으로 해석되었으며, 이는 곧 개인정보 암호화의 미흡과 주민등록번호를 개인식별정보로 여전히 사용하는 것을 확인 된다. 이는 곧 법규 위반을 의미하는 것이며, 사회적 기업 책임(CSR)이 외에도 IT컴플라이언스 준수가 미흡한 것으로 해석 된다.

2.4 컴플라이언스를 준수하는 광고 홍보기법 연구

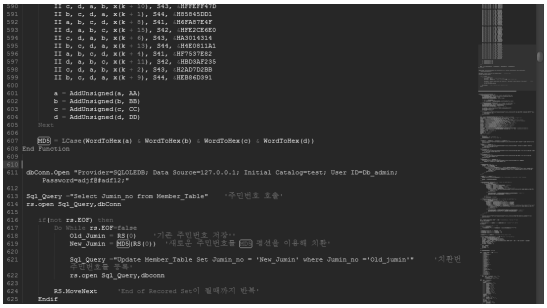
2.3장에서 살펴본 것과 같이 국민의 84%의 개인정보를 취급하는 A社의 분석결과를 보면, 개인정보보호법이 시행되어도 관계기관의 지도와 기술적 대응 방안에 대한 사례연구가 필요하다. 2.4장에서는 개인정보를 사용하지 않고 개인을 식별할 수 있는 기반기술에 대해 언급하도록 한다.

2.4.1 개인정보의 치환 및 관리 방법론

기존 사용되고 있는 개인식별정보인 주민등록 번호는 개개인을 식별하기 위한 용도와 신분 확인의 용도로 사용되는 원장의 경우 신뢰된 암호화 알고리즘에 의해 암호화 되어야 하며, 비밀번호의 경우 일방향 HASH 방식을 이용하여 복호화 될 수 없도록 하여야 한다. 본 논문에서 언급하는 홍보메일 및 타깃 마케팅 방면에서는 개인을 식별하기위해 주민등록번호를 사용할 수가 없다. 이 문제를 해결하기 위해 본 장에서는 일방향 암호를 사용함으로서 개인을 식별할 수 있는 기법을 연구하였다. 현재 각 카드社에서 이용하고 있는 개인식별정



〔그림 19〕 일방향 해쉬함수(HASH)를 이용한 개인식별정보 치환



〔그림 20〕 일방향 해시함수(HASH)를 이용한 개인식별정보 치환 코드

보는 복호화가 가능한 인코딩 기법을 사용했다는 점에서 문제점이 있다. 즉, 복호화가 불가능한 일방향성 해시함수를 이용하여 인식번호를 사용하면 정보가 노출되더라도 안전하게 보호될 수 있다.

HASH 구현 알고리즘은 인터넷을 통해 쉽게 확인이 가능하며, 연구에 사용된 코드는 ASP(Active Server Page)로 구현된 치환 방법을 사용 하였으며, 자세한 코드 내용은 [별첨 3] 문서에 기재하였다.

[그림 20]과 같이 기존 주민등록번호를 HASH화하여 저장할 경우 홍보메일 발송/분석시스템이 외부 해커에 의해 정보가 노출되더라도 개인식별정보를 안전하게 보호할 수 있다. 또한 개인식별정보인 주민등록 번호를 사용하지 아니함으로서 관계법규도 동시에 만족시킬 수 있다.

Ⅲ. 결 론

3.1 연구 결과에 따른 제언

국내 많은 기업에서는 개인정보의 법적 IT컴플라이언스 준수를 위해 개인정보 영향평가(PIA), 기술적·관리적 보호조치, 내부 실태 조사 등의 다양한 형태로 개인정보 파악 및 보호조치를 강구하고 있으나 대부분 기업에서 인증 및 각종 평가에만 치우친 잣대로 개인정보를 평가하기 때문에 실제 개인정보의 유통 및 내부 실태에 대한 파악이 많이 부족한 것으로 파악된다.

또한 2012년 8월 18일 "정보통신망 이용촉진 및 정보보호 등에 관한 법률" 제23조의 2(주민등록번호의 사용 제한) 시행이 고지되었음에도 불구하고 본 연구과정에서 살펴봤듯이 여전히 일부 기업의 법적 준수 현황은 많이 미흡한 편이다.

이러한 연구 결과를 토대를 각 금융권 혹은 그와 관련된 기업에서는 해당 기업의 개인정보 활용에 대한 실태를 다시 한 번 점검하고 연구하여 고객에 대한 신뢰, 법적 준수 등 IT컴플라이언스를 준수할 수 있는 공감대를 형성해야 할 것이다.

참고문헌

[1] 보험개발원(KIDI), “국내 금융사 17%, 개인정보보호 관심 無”, 2012. 04

[2] 위키백과, “기업의 사회적 책임”, 2012. 10

[3] Marketing Terms, “Conversion Rate”, 2004. 11

[4] 여신금융협회, “2011년 3월 신용카드 통계”, 여신금융 제25호. 2011. 03

[5] 통계청 e-나라지표, “보도자료 신용카드시장 동향”, P6, 2012. 03

[6] 디지털 타임즈 보도자료, “신용카드 시장재편 전운 감돈다”, 2009. 08

[7] BC Card 회사소개, “신용카드 발급사”, 2012. 08

〈著者紹介〉

이 병 수 (Byeong-Su, Lee)
2006년 2월: 청주대학교 컴퓨터정보공학과 졸업(공학학사)
2005년 10월~2008년 10월 : (주)나우콤 보안사업부 침해사고분석대응팀
2008년 10월~2012년 11월 : NHN I&S 정보보안팀
2012년 11월~현재 : SK플래닛 플랫폼 기술원 IT팀
<관심분야> 정보보호, 침해사고대응

황 지 상 (Ji-Sang, Hwang)
2005년 8월: 삼육대학교 컴퓨터과학과 졸업(이학사)
2006년 03월~2006년 12월 :(주)엘림넷 망운영팀
2006년 12월~2008년 12월 :(주)윈스테크넷 침해사고 대응팀
2009년 05월~2010년 03월 :(주)인프니스 기술연구소
2010년 04월~2012년 05월 : (주)윈스테크넷 침해사고 분석팀
2012년 05월~현재 : 아주아이티(주) 정보전략기획팀
<관심분야> 정보보호, 네트워크 침입탐지

황 동 욱 (Dong-Uk, Hwang)
2010년~현재 : 숭실사이버대학교 정보보안학과 학사과정
2000년 08월~2005년 08월 :(주)메이콤 중앙연구소
2005년 11월~2007년 11월 : 한국정보보호진흥원 인터넷침해사고대응지원센터
2007년 11월~2008년 03월 : 정부통합전산센터 보안분석담당
2008년 10월~2010년 01월 : (주)나우콤 보안사업부 침해사고분석대응팀
2010년 02월~현재 : 딜로이트안진회계법인 기업리스크자문본부
<관심분야> SCADA, 모의침투, 침해사고분석, 디지털 포렌식

최 봉 철 (Bong-Chul, Choi)
2010년 2월 강원대학교 컴퓨터과학과(공학학사) 졸업
2009년 08월~2012년 12월 : (주)윈스테크넷 침해사고대응팀
<관심분야> 네트워크 침입탐지, 디지털 포렌식, 정보보호

홍 용 진 (Yong-Jin, Hong)
2009년 2월: 백석대학교 정보보호학과 졸업(정보보호학사)
2009년 08월~현재 : (주)윈스테크넷 침해사고대응센터 침해사고분석팀
<관심분야> 정보보호, 소프트웨어 역공학