The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 14, No. 5, pp.1-10, Oct. 31, 2014. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2014.14.5.1
JIIBC 2014-5-1

대민서비스 온라인 보안위협 분석 및 대응방안 연구

A Study On Security Threat Analysis and Government Solution for Civil Service Online

최도현*, 전문석*, 박중오**

Do-Hyun Choi*, Mun-Seog Jun*, Jung-Oh Park**

요 약 전자정부 대민서비스는 과거부터 현재까지 공공기관 홈페이지가 다양해지고 서비스 수가 증가함에 따라, 전자민원 문서의 위·변조에 대한 가능성이 제기되는 등 전자민원 서비스 전반에 대한 보안에 대한 요구사항이 증가하고 있다. 기존 연구[1][2][3][4]는 전자정부 중 민원서비스(G4C)와 같은 하나의 서비스와 서비스 제공자 관점에서 보안위협과 대응방안을 제시하였다. 본 연구는 분석 범위를 확대하여 최근 대민서비스 제공 중인 289개 홈페이지를 대상으로 서비스 유형 별 적용되어 있는 보안기술을 분석하고 보안위협에 따른 대응방안을 제시하였다. 본 논문을 통해 대민서비스에 대한 실질적인 대응방안과 동시에 현재 해결해야 할 전자정부 대민서비스의 핵심적인 문제에 대하여 논의하고자 한다.

Abstract As the number of public institution web sites and civil services based on electronic government has increased from the past until now, there is an increasing demand for security of the overall electronic civil services such as possibility for forgery and falsification of electronic documents. Existing studies[1][2][3][4] proposed security threats and response methods on an electronic government service (G4C) from the perspective of service provider. In this study, the scope of analysis was expanded to analyze security technology used for each service type on 289 web sites providing civil services and to present response methods on security threats. The aim of this paper is to discuss practical responses to civil services and core problems of civil services in electronic government that need to be resolved.

Key Words : Government Civil Service, G4C, e-government

Ⅰ. 서 론

전자정부 대민서비스(이하 '대민서비스'라 한다)는 국민이 행정기관을 방문하지 않고 인터넷을 통해 각종 행정정보를 제공받을 수 있고 민원사무도 처리할 수 있도록 행정기관이 제공하는 온라인 서비스를 의미한다[5].

이러한 전자정부 대민서비스는 '전자정부서비스 이용실태조사[6]' 결과 현재까지 해마다 행정서비스 이용률이 점차 증가하는 것으로 나타났다[7]. 대민서비스는 포털 사이트를 통해 각종 서식을 다운로드 받고 필요한 정보(법률/행정정보, 공무원시험정보, 취업정보, 날씨 정보, 부동산 실거래가 정보 등)를 검색하거나, 주민등록등초본, 등

*정회원, 숭실대학교 컴퓨터학과
**정회원, 동양미래대학교 정보통신과 (교신저자)
접수일자 : 2014년 9월 11일, 수정완료 : 2014년 10월 1일
게재확정일자 : 2014년 10월 10일

Received: 11 September, 2014 / Revised: 1 October, 2014
Accepted: 10 October, 2014
*Corresponding Author: jopark13@dongyang.ac.kr
Dept of Information & Communications, DONGYANG MIRAE University, Korea

기부등본, 토지이용계획 확인원 등 다양한 민원서류를 신청, 열람, 발급받을 수 있다. 특히, 전자정부 대국민 창구의 역할을 수행하고 있기 때문에 서비스의 효율성과 안전성이 필요하므로 대민서비스 사용자 환경을 중심으로 보안을 강화시키는 실제적인 대응방안이 요구된다. 표 1은 국민 대부분이 전자정부 대민서비스의 인지도와 이용률, 만족도에 대한 변화 추이를 나타낸다. 전체 이용률(2012년 기준)이 88.6%를 기록하여 OECD 27개국 전체 평균(2011년 기준) 81%와 비교하면 27개국 중 최상위 수준이며 검색포털·모바일서비스 등 간접적으로 서비스를 이용한 경험도 22.7%로 전자정부 웹 사이트(홈페이지)를 직접 방문하여 이용한 경험이 68.3%를 기록했다[6]. 이는 세계 최고수준의 전자정부 서비스 이용률에 해당된다.

표 1. 전자정부 활용수준 조사 결과
Table 1. Survey of e-Goverment Service

구분	09년도	10년도	11년도	12년도
인지도(%)	92.5	92.6	92.4	81.9
이용률(%)	60.2	60.0	86.3	88.6
만족도(%)	67.9	74.0	82.6	91.2

본 논문 2장 관련연구에서는 기존 온라인 사용자 보안기술 적용 현황과 대민서비스 온라인 사용자 보안기술 적용 현황에 대해 분석하고 3장에서는 대민서비스 유형 및 사용정보 분석 4장에서는 대민서비스 유형 별 위협분석 5장 대응방안 6장 결론으로 마친다.

(본 연구는 한국인터넷진흥원이 주관하고 KCC Security가 12년 5월부터 12년 12월말까지 '전자정부 대민서비스 정보보호 수준진단 컨설팅' 사업의 컨설팅 대상 289개 사이트 목록을 사용하였음.)

II. 관련연구

1. 온라인 사용자 보안기술 적용 현황

현재 온라인상에서 적용되는 보안기술들은 서비스 별로 보호해야 하는 중요정보의 대상이 다르고 특성에 따라 제공하는 보안기술에 차이가 있다. 일반적으로는 금융거래 서비스, 전자상거래 서비스, 일반포털 서비스 등으로 일반적으로 온라인 사용자 보안 기술 적용 현황은 표 2과 같다. (본 현황의 조사 대상은 국내 인터넷 뱅킹 19개, 쇼핑몰 25개, 일반 포털 서비스 7개를 대상으로 분석 : 2013년 2월 기준)

표 2. 온라인 사용자 보안기술 현황
Table 2. Security Technology of Online User

보안 기술	서비스 종류		
	금융 거래 서비스	전자상거래 서비스	일반 포털 서비스
암호통신(SSL)	O	O	O
키보드 보안	O	O	O
웹 보안	O	X	X
IP 보안	X	X	O
가상키보드	O	X	X
피싱 방지	O	O	X
웜/바이러스 백신	O	X	O
Mobile OTP	O	O	O
하드웨어 OTP	O	X	X
NPKI, GPKI	O	X	X
문서위변조(DRM)	X	X	X

금융 거래 시에 사용자 보안기술은 암호통신 및 전자서명, 키보드 보안, 웹 보안, 가상키보드, 피싱 방지, Mobile OTP, 하드웨어 OTP 등이 있으며 사용자의 예금조회, 계좌이체, 자동이체 등 금융거래내역 등에 대한 정보를 보호한다.

전자상거래시 사용자 보안기술은 암호통신, 키보드 보안, 피싱 방지, Mobile OTP 등이 있으며 온라인을 통한 상품의 구매나 판매에 대한 사용자의 거래정보 등을 보호한다.

일반 포털 사용 시 사용자 보안기술은 암호통신, IP 보안, 키보드 보안, 웜/바이러스 백신, Mobile OTP 등이 있으며 주로 포털 커뮤니티나 블로그, 카페 등을 이용하는 개인정보 등을 보호한다. 분석 결과, 각 서비스 특성에 따라 제공하는 보안기술 적용에 차이가 있는 것으로 분석되었다.

금융거래 서비스의 경우 암호통신(SSL), 키보드보안, 웜/바이러스 백신을 설치해야 서비스를 이용할 수 있으며, 기타 금융거래 서비스 보안 기술은 사용자의 선택에 따라서 사용여부를 결정했다.

전자상거래 서비스의 경우 암호통신(SSL)을 설치해야 서비스를 이용할 수 있으며, 기타 전자상거래 보안 기술은 사용자의 선택에 따라서 사용여부를 결정했다. 일

반포털 서비스의 경우 보안기술 모두 사용자의 선택에 따라서 사용여부를 결정했다.

2. 대민서비스 온라인 보안기술 적용 현황

대민서비스 대상기관 289개 대민서비스에 적용된 보안 기술을 분석한 결과 14.8%(43/289)만 보안기술이 적용된 것을 확인하였다.(모바일 환경 제외) 정부민원포털 민원24, 국세청 등 결제 및 사용자의 개인정보와 같은 중요정보 서비스는 보안기술이 잘 적용되어 있는 것으로 나타났지만 이외 85.2% (246/289) 사이트들은 보안기술이 잘 적용되어 있지 않은 것으로 분석되었다. 사이트 내 각 보안기술 별 통계는 표 3과 같다.

표 3. 대민서비스 온라인 사용자 보안기술 현황
Table 3. Security Technology of e-Goverment Online User

보안 기술	서비스 수	설명	제공방식
키보드 보안 프로그램	34	사용자의 키보드 입력정보(ID, Password 또는 개인정보) 핵킹 방지를 위한 보안 솔루션	Active X
NPKI, GPKI	7	PKI를 이용한 상호인증과 공인인증서 유출 및 부인방지 기능을 제공	Active X
문서위변조 (DRM)	2	대민서비스에서 제공하는 증명서(주민등록등본, 세금납부명세서 등)의 위·변조 방지 기능을 제공	독립 프로그램 또는 Active X
PC 방화벽, 웹 방화벽	25	사용자 외부나 내부에서 유입되는 악성 패킷에 대한 차단 기능을 제공	독립 프로그램 또는 Active X
총 서비스 수	43	14.8% (43/289)	

조사 결과인 14.8%에서 위 모든 보안기술이 아닌 일부는 적용되고, 일부는 적용되지 않은 것으로 나타났으며 비교적 중요한 정보를 다루는 사이트가 비교적 많은 보안기술이 적용된 것을 확인하였다. 보안 기술을 제공하지 않는 사이트에서 대부분 민원24, 국세청, 국민신문고 등 사용자가 많이 이용하는 민원서비스들로 서비스가 링크되어 연동되어있는 것으로 나타났다. 보안되어 있지 않은 사이트에서 링크를 따라 이동하면서 로그인시에 유지된 세션(ID, Password 등 입력정보)은 해킹의 대상이 될 수 있다. 이것은 사용자들이 여러 사이트에 일반적으로 같은 아이디와 패스워드를 이용하기 때문에 이러한 정보가 유출될 경우 다른 사이트들로 피해가 전파될 수 있다. 아이디 패스워드 노출은 로그인 후 사용자의 기본 정보인 이메일이나 연락처와 같은 정보를 쉽게 알아낼 수 있기 때문에 이는 스팸메일, 보이스 피싱, 스팸 문자 등 다른 보안위협들과 연결될 수 있다.

Ⅲ. 대민서비스 유형 및 사용정보 분석

본 논문에서는 대민서비스 온라인 보안기술 현황을 기반으로 다양한 대민서비스 이용 시 발생할 수 있는 보안 위협을 도출하기 위해 대민서비스 유형 분석을 선행한 후 서비스 유형 별 위협을 분석한다.

1. 대민서비스 유형 분석

전자정부 대민서비스를 제공하는 중앙부처 및 광역지자체 72개 기관의 289개 서비스를 조사한 결과 세부 서비스 유형은 표 4과 같이 총 9가지로 분류되었다.

표 4. 대민서비스 유형 별 서비스 통계
Table 4. Statistics Based on e-Goverment Service Type

대민서비스 유형	서비스 수	비율
단순정보제공	75개	26.6%
공공정보제공	25개	8.8%
증명서 열람 및 발급	16개	5.6%
납부/결제 조회 및 확인	9개	3.2%
민원신청 및 신고	103개	36.6%
국민참여 및 개선	44개	15.6%
예약	9개	3.2%
위치정보/증강현실	4개	0.3%
재난안전알림	2개	0.1%
계	총 289개	100%

민원신청 및 신고 서비스가 가장 많은 것으로 나타났으며 다음으로는 단순 정보제공, 국민참여 및 개선, 공공정보제공, 증명서 열람 및 발급, 납부/결제 조회 및 확인, 예약 서비스 순으로 나타났다.

단순정보제공 서비스는 필요한 정보를 쉽고 편리하게 조회하고 접근할 수 있도록 제공하는 서비스로 이용 안내,

공지사항, 정책 안내, 홍보, 근황 소개, 자료검색 등이 있으며, 서비스 사례로 통계청의 민원안내, 통계지리정보의 지방 변화, 국가보훈처의 전자도서관 자료검색 등이 있다.

공공정보제공 서비스는 각 기관에서 직무상 전자적 방식으로 처리, 작성 취득하여 관리하고 있는 데이터로써 영리・비영리 목적으로 재활용할 수 있도록 제공하는 서비스로 사례는 통계청, 금융위원회, 법무부, 특허청 등이 있다.

증명서 열람 및 발급 서비스는 민원서류 및 증명서류 발급 등을 온라인으로 할 수 있도록 제공하는 서비스로 대표적으로 민원24라는 통합 플랫폼이 만들어져 있으며 각 시, 구청이나 여러 기관들이 제공하는 민원서비스들의 각종 증명서 발급신청 등을 이용할 수 있다. 각종 증명/확인서는 발급 신청자의 개인정보를 포함하기 때문에 반드시 사용자인증을 위해 공인인증서를 통한 인증을 거쳐야 서비스를 제공받을 수 있으며 서비스 사례는 방통위, 국세청 등이 있다.

납부/결제 조회 및 확인 서비스는 온라인상에서 금융결제를 제공하는 서비스로 각 기관을 방문해 납부·결제하던 불편함을 없애고 온라인이나 모바일 기기 등으로 간편하게 실시간으로 납부·결제할 수 있도록 편의를 제공하는 서비스로 해당 납부/결제 서비스 이용 시 ID/Password 및 공인인증서를 이용하여 사용자 인증을 받고, 사용자의 신용카드 등 결제 방식에 따라 서비스를 이용할 수 있으며 사례는 행정안전부와 각 지방별 경기도(경기사이버 장터), 경상남도(중소기업안정자금), 전라남도(남도장터)등이 있다.

민원신청 및 신고 서비스는 생활에서 일어나는 불편이나 각종 부조리, 비리, 불공정거래 등을 신고할 수 있도록 만든 서비스로 정확한 신고자 식별과 허위신고에 대한 문제점이 있기 때문에 최소한의 개인정보를 요구하고 있으며 사례는 민원포털(민원 신청, 신청 내역 조회, 고충민원 신청/확인), 통계청(온라인 민원신청, 예산낭비신고) 등이 있다.

국민참여 및 개선 서비스는 국가에서 진행하고 있는 정부시책이나 행정제도, 운영의 개선을 목적으로 하여 행정기관에 의견을 전달하고 새로운 제안을 신청 할 수 있는 서비스로 의견제안자에 대한 신분 확인 및 의견에 대한 답변을 제공하기 위해 사용자 인증정보를 요구하며 사례는 국가보훈처(제대군인지원센터), 기획재정부(공공기관 채용정보 시스템), 경찰청(사이버 경찰청), 법제처(국민참여입법센터) 등이 있다.

예약 서비스는 전화, 팩스, 직접방문 등 기존 예약서비스의 사용자 대기시간을 최소화 할 수 있는 편리함을 제공하며 예약 서비스로 사례는 법무부(하이코리아), 경찰청(경찰박물관), 국가보훈처(전자도서관) 등이 있다.

위치정보/증강현실 서비스는 모바일 전자정부 서비스에서 GPS 정보를 이용하거나 증강현실 기술을 이용하여 사용자에게 편의를 제공하는 서비스로 행정안전부(생활공감지도), 서울시(스마트불편신고), 환경부(공간정보 서비스) 등이 있다.

재난안전알림은 재난속보 서비스를 통하여 재난이 발생했을 시 빠르게 재난을 인지하고, 국민행동요령을 제공함으로 국민들이 재빨리 재난상황에 대하여 적절히 대처할 수 있도록 재난알리미 앱 등을 통하여 국민들에게 무료로 제공되는 서비스로 사례는 국립산림과학원(산림재해위치정보시스템, 산림항공사진검색 시스템) 등이 있다.

2. 대민서비스 사용정보 분석

대민서비스 사용자에게 발생하는 보안 위협을 체계적으로 분류, 분석하기 위해서는 대민서비스 사이트에서 발생하는 정보의 중요도를 파악하는 것이 선행되어야 한다. 이를 위해 실제 통신상의 요청/응답 정보를 입력정보와 제공정보로 정의하고 분석하였다. 입력정보란 사용자가 서비스를 사용하기 위해 필수적으로 입력해야 하는 정보를 의미한다. 이러한 입력 값은 신원확인을 위한 이름과 주민등록번호, 아이핀과 사용자인증을 위한 ID/Password, 공인인증서 등 모두 포함 된다.

가장 일반적으로 사용되는 ID/Password의 경우 공공정보제공은 80%(20/25), 민원신청 및 신고 47.5%(49/103), 국민참여 및 개선 72.7%(32/44), 예약 77.7%(7/9)로 총 67.6% 나타나 대민서비스에서 ID/Password 입력을 이용한 사용자 인증이 가장 많은 것으로 나타났다. 이외 단순정보제공, 위치정보/증강현실, 재난안전알림은 특별한 입력정보 없이 제공받을 수 있는 것으로 나타났다.

공인인증서의 경우 민원신청 및 신고 내역이 21.3%(22/103)로 가장 많이 나타났다. 이것은 서비스의 특성상 증명서와 같은 정보의 중요도가 비교적 높은 서비스에서 공인인증서를 이용하도록 되어있기 때문인 것으로 분석되었다. ID/Password 와 공인인증서와 같이 입력 빈도가 높은 사용자의 입력정보 통계는 표 5과 같다.

표 5. ID/Password와 공인인증서 입력정보 통계
Table 5. Statistics of the input information (ID/Password, Cerificate)

대민서비스 유형	ID/Password	ID/Password, 공인인증서
단순정보제공	해당사항 없음	해당사항 없음
공공정보제공	공공정보 : 80%(20/25)	공공 : 16%(4/25)
증명서 열람 및 발급	50%(8/16)	50%(8/16)
납부/결제 조회 및 확인	77.7%(7/9)	11%(1/9)
민원신청 및 신고	47.5%(49/103)	21.3%(22/103)
국민참여 및 개선	72.7%(32/44)	해당사항 없음
예약	77.7%(7/9)	11.1%(1/9)
위치정보/증강현실	해당사항 없음	해당사항 없음
재난안전알림		
전체 평균	67.6%	18.2%

ID/Password 조합만을 사용하는 사이트가 67.6%로 전체에서 과반수가 특별한 추가 인증을 수행 없이 사용할 수 있는 것을 확인 하였다. 서비스 유형 별 사용자 입력정보(세부 서비스 포함)는 표 6과 같다.

표 6. 서비스 유형 별 사용자 입력정보
Table 6. Input information(Type of Services)

서비스 유형	세부 서비스	사용자 입력정보
단순정보제공	민원안내, 자료검색, 연구정보, 교육뉴스, 재난대비	무인증
공공정보제공	버스정보, 길찾기 등 안내	무인증
	도로명 주소 확인	이름/주민등록번호/이메일/전화번호
	자료신청	ID/Password
	국가입법 정보 조회 및 안내	ID/Password, 주민등록번호/아이핀
증명서 열람 및 발급	장애인 보조기구 신청	이름/전화번호/이메일/주소
	소득공제 자료 조회, 출력 및 제공동의	주민등록번호/공인인증서
	증명발급, 세금신고, 세금 신청 및 확인	ID/Password, 공인인증서
	온라인 민원(접수 및 면허)	ID/Password, 주민등록번호/공인인증서
	기록물 온라인 신청	아이핀
	문서 원본 확인	원본확인 문서 번호
납부/결제 조회 및 확인	요금정보(조회)	이름, 계좌번호
	원서접수 및 확인, 결제	이름/주민등록번호/Password, 이메일, 아이핀
	상품구매 및 주문/배송조회	ID/Password, 이름/전화번호
	원서접수 및 확인, 결제	ID/Password, 공인인증서
민원신청 및 신고	신체검사결과확인, 이산가족 신청 및 취소	이름/주민등록번호
	민원신청 및 신고, 신고내역 조회	이름/전화번호/주민등록번호/이메일/주소
	민원신청	주민등록번호, 공인인증서
	민원신청	ID/Password
	민원 신청 및 신고, 신청내역 조회	ID/Password, 공인인증서, 이름/주민등록번호, 아이핀
	문서 위·변조 신고	전화번호/이름/전자문서 확인번호
국민참여 및 개선	창업상담	이름/주민등록번호
	알림마당	이름/주민등록번호, 아이핀
	맞춤, 관심 채용 정보	ID/Password
	국민 의견 및 국민토론	ID/Password, 주민등록번호/아이핀
예약	민원상당사전예약	이름/주민등록번호, 아이핀
	도서대출	ID/Password
	방문예약신청	ID/Password, 아이핀
위치정보/증강현실	사용자 위치 서비스	무인증
재난안전 알림	산불관련 정보	무인증

ID/Password, 공인인증서이외에 요구되는 기타 입력정보는 이름/주민번호, 아이핀 등으로 분석되었으며 단순정보제공, 위치정보/증강현실 및 재난안전 알림의 경우 특별한 인증 없이 사용자에게 정보를 제공하였다. 사용자 입력정보 중 전자문서, 차량내역 등 일부 서비스의 경우 전자문서번호, 차량등록 번호 등이 정보조회로 사용되었으며, 전화번호, 이메일 주소 등 개인정보는 민원신청을 위한 입력 정보로 많이 사용되었다. 대민서비스 온라인 사용자가 정보입력 이후 서비스를 사용하면서 제공받는 정보는 표 7과 같다.

표 7. 서비스 유형 별 사용자가 제공받는 정보
Table 7. Provide information(Type of Services)

제공받는 정보	서비스 유형
민원 안내, 교육뉴스, 녹색산업, 건설현황, 녹색에너지, 기상 속보, 문화유산 안내 등	단순정보제공
국가통계, 통계정책, 위탁처리현황, 원격접근현황, 제도권금융회사 조회 등	공공정보제공
민원신청서 발급 정보, 주민등록 및 증명서 발급 정보, 세금 신청 증명서 발급 정보, 현금 영수증 발급 정보, 온라인 기록물 정보, 문서 원본 확인 정보 등	증명서 열람 및 발급
원서접수 및 결제, 각 지역별 장터 상품 결제, 시설자금 결제, 단속정보 조회(결제 필요) 등	납부/결제 조회 및 확인
고충민원, 예산낭비 신고, 부동산신고, 신체검사 확인, 공적조사서 등록, 포장신청 확인, 부조리 신고, 일자리 신청, 범죄 신고, 비리 신고, 수사 조회 등	민원신청 및 신고
창업상담, 알림마당, 홍보마당, 국민의견 및 국민토론, 알림마당, 도민참여, 고객센터, 열린 의회 등	국민참여 및 개선
민원상담 사전예약, 도서 대출, 방문상담예약, 참여마당, 해외여행등록제, 교육, 시설, 문화/관광 예약, 공공시설 예약 등	예약
지역별 전파지도, Wifi정보, 방송수신정보, 지리정보, 해양 위치정보, 전국 주유소 위치정보, 공원 위치정보 등	위치정보/증강현실,
호우, 태풍, 대설 등 돌발기상 정보, 대형화재 등 재난 정보 등	재난안전알림

Ⅳ. 대민서비스 유형 별 위협 분석

입력정보 유형 별 나타나는 위협은 세부 위협을 포함하여 총 6가지 유형으로 통신경로상의 정보 노출 및 변조, 유해프로그램 설치로 인한 정보유출, 키보드 입력 노출, 화면노출 및 화면캡처, 문서정보 위변조, 명의 도용으로 도출되었으며 상세 내용은 표 8과 같다.

ID/Password, 이름, 전화번호, 이메일 등을 이용한 인증과정에서 사용자의 PC와 대민서비스 제공자간 네트워크 구간 사이에 평문으로 노출될 수 있기 때문에 통신경로상의 정보 노출 및 변조 위협으로 도출되었다. 공인인증서를 사용하는 서비스는 세션 암호화 및 부인방지 기능을 제공하기 때문에 통신경로상의 정보 노출 및 변조 위협에서 제외되었다.

표 8. 입력정보 유형 별 보안위협
Table 8. Security Threats(Type of Input Information)

입력정보 유형	위협
이름, 주민번호	통신경로상의 정보 노출 및 변조
	유해프로그램 설치로 인한 정보유출
	키보드 입력 노출
	명의 도용
아이핀	유해프로그램 설치로 인한 정보유출
	키보드 입력 노출
	명의 도용
ID, Password	통신경로상의 정보 노출 및 변조
	유해프로그램 설치로 인한 정보유출
	키보드 입력 노출
	명의 도용
공인인증서	유해프로그램 설치로 인한 정보유출
	키보드 입력 노출
	명의 도용
사업자 등록번호, 원본 확인 문서번호, 차량등록번호 등	통신경로상의 정보 노출 및 변조
	유해프로그램 설치로 인한 정보유출
	키보드 입력 노출
	명의 도용
	화면노출, 화면 캡처
	문서 정보 위변조
전화번호, 이메일, 주소 등	통신경로상의 정보 노출 및 변조
	유해프로그램 설치로 인한 정보유출
	키보드 입력 노출
	명의 도용
	화면노출, 화면 캡처

사이트의 서비스를 사용하면서 저장되는 웹브라우저 정보(쿠키, 통신 세션 등), 기타 저장매체(USB, 외장 하드디스크)는 사용자의 운영체제에 감염된 악성코드나 스파이웨어, 백도어로 인해 정보가 유출 될 수 있기 때문에 유해프로그램 설치로 인한 정보유출(인증 및 식별 정보) 위협으로 도출되었다.

사용자의 입력 정보는 일반적으로 PC에 연결된 키보드에서 발생한 아스키코드(ASCII code)값으로 조합으로 입력된다. 아스키코드 값은 실제로 운영체제를 통해 메모리 전송되는 과정에서 키 후킹 기법이나 메모리 핵킹에 의해 평문으로 노출될 수 있기 때문에 키보드 입력 노출 위협으로 도출되었다.

이름/주민번호, 아이핀과 같은 입력정보는 평문으로 노출 시 악의적인 제 3자가 정당한 사용자 명의를 도용할 수 있기 때문에 명의 도용 위협으로 도출되었고, 세금내역 확인서, 주민등록등본 등 사용자가 조회 및 확인하는 문서정보는 악의적인 제 3자가 사용자의 문서를 위·변조할 수 있기 때문에 문서정보 위·변조 위협으로 도출되었고, 문서정보나 개인정보 등 중요정보가 모니터 화면에 노출되는 화면을 핵킹 프로그램으로 캡처하여 정보를 유출할 수 있기 때문에 화면노출, 화면캡처 위협으로 도출되었다.

입력받는 정보이외에 나타나는 보안위협 분석을 위해 제공받는 정보 유형에 대한 위협을 분석하였다. 표 9과 같이 입력 정보에 대한 위협을 제외하고, 총 4가지 유형으로 통신경로상의 정보노출 및 변조, 유해프로그램 설치로 인한 정보유출, 화면노출 및 화면캡처, 문서정보 위·변조로 분류되었다.

표 9. 제공받는 정보 유형 별 위협
Table 9. Security Threats(type of Provide information)

서비스 유형	제공받는 정보	위협
단순정보제공	민원 안내, 교육뉴스, 녹색산업, 건설현황, 녹색에너지, 기상 속보, 문화유산 안내 등	해당사항없음
공공정보제공	국가통계, 통계정책, 위탁처리현황, 원격접근현황, 제도권금융회사 조회 등	통신경로상의 정보노출
증명서 열람 및 발급	민원신청서 발급 정보, 주민등록 및 증명서 발급 정보, 현금 영수증 발급 정보, 온라인 기록물 정보, 문서 원본 확인 정보 등	통신경로상의 정보노출
		유해프로그램 설치로 인한 정보유출
		화면 노출, 화면캡처
		문서정보 위·변조
납부/결제 조회 및 확인	원서접수 및 결제, 각 지역별 장터 상품 결제, 시설자금 결제, 단속정보 조회(결제 필요) 등 원서와 같은 증명서나 상품 결제 정보 등	통신경로상의 정보노출
		유해프로그램 설치로 인한 정보유출
		화면 노출, 화면캡처
민원신청 및 신고	고충민원, 예산낭비 신고, 부동산신고, 신체검사 확인, 공적조사서 등록, 일자리 신청, 범죄 신고, 비리 신고, 수사 조회 등	통신경로상의 정보노출
		유해프로그램 설치로 인한 정보유출
국민참여 및 개선	창업상담, 알림마당, 홍보마당, 국민의견 및 국민토론, 알림마당, 도민참여, 고객센터, 열린 의회 등	통신경로상의 정보노출
예약	민원상담 사전예약, 도서 대출, 방문상담예약, 교육, 시설, 문화/관광 예약, 공공시설 예약 등	통신경로상의 정보노출
위치정보/증강현실	지역별 전파지도, Wifi정보, 방송수신정보, 전국 주유소 위치정보, 공원 위치정보 등	해당사항 없음
재난안전알림	호우, 태풍, 대설 등 돌발기상 정보, 대형화재 등 재난 정보 등	해당사항 없음

단순정보제공, 위치정보/증강현실, 재난안전알림 서비스 유형에서 제공받는 정보인 민원 안내, 교육뉴스, 방송수신정보, 재난 정보 등은 대민서비스 사용자가 홈페이지에 접속하여 인증 없이 제공받을 수 있는 공개된 정보이기 때문에 위협이 도출되지 않았다. 단순정보를 제외한 6가지 서비스 유형은 입력정보 위협과 동일하게 네트워크상에 평문으로 노출될 수 있기 때문에 통신경로상의 정보노출 위협이 도출되었다. 특징은 입력정보와 같이 일정한 입력 정보가 아닌 제공받는 다양한 정보의 특성을 지녔기 때문에 변조의 위협은 도출되지 않았다. 증명서 열람 및 발급, 납부/결제 조회 및 확인 서비스 유형에서 제공받는 정보인 증명서 발급정보, 현금 영수증 발급정보, 원서접수 및 결제 정보 등은 화면에 노출되거나 악의적인 제 3자가 위·변조 할 수 있기 때문에 화면노출 및 화면캡처, 문서정보 위·변조 위협이 도출되었다. 사용자 입력정보와 제공받는 정보를 바탕으로 대민서비스 유형별 위협은 총 6가지로 통신경로상의 정보노출 및 변조, 유해프로그램 설치로 인한 정보유출, 키보드 입력 노출, 화면노출 및 화면캡처, 문서정보 위·변조, 명의도용으로 표 10과 같다. 분석 결과 입력정보 유형의 별 위협은 제공받는 정보 위협을 모두 포함하였고, 사용자의 입력 정보를 요구하지 않는 서비스는 입력정보 위협과 제공받는 정보 위협 동일하게 위협이 도출되지 않았다.

표 10. 서비스 유형 별 보안위협
Table 10. Security Threats(type of Services)

서비스 유형	입력정보 형태	보안 위협
단순정보 제공	무인증	해당사항 없음
공공정보 제공	아이핀 ID, Password	통신경로상의 정보노출 및 변조
		유해프로그램 설치로 인한 정보유출
		키보드 입력 노출
		명의 도용
증명서 열람 및 발급	이름/주민번호 아이핀 ID, Password 공인인증서 사업자 등록번호, 원본 확인 문서번호 등	통신경로상의 정보노출 및 변조
		유해프로그램 설치로 인한 정보유출
		키보드 입력 노출
		명의 도용
		화면노출, 화면캡처
		문서정보 위·변조
납부/결제 조회 및 확인	이름/주민번호 아이핀 ID, Password 공인인증서	통신경로상의 정보노출 및 변조
		유해프로그램 설치로 인한 정보유출
		키보드 입력 노출
		명의 도용
		화면노출, 화면캡처
민원신청 및 신고	이름/주민번호 아이핀 ID, Password 공인인증서	통신경로상의 정보노출 및 변조
		유해프로그램 설치로 인한 정보유출
		키보드 입력 노출
		명의 도용
		화면노출, 화면캡처
국민참여 및 개선	이름/주민번호 아이핀 ID, Password	통신경로상의 정보노출 및 변조
		유해프로그램 설치로 인한 정보유출
		키보드 입력 노출
		명의 도용
예약	이름/주민번호 아이핀 ID, Password	통신경로상의 정보노출 및 변조
		유해프로그램 설치로 인한 정보유출
		키보드 입력 노출
		명의 도용
위치정보/ 증강현실	무인증	해당사항 없음
재난안전 알림	무인증	해당사항 없음

통신경로상의 정보 노출 및 변조는 세부 위협으로 스니핑, 스푸핑, MITM, 재사용 공격 등이 존재했고, 유해프로그램 설치로 인한 정보유출은 세부 위협으로 악성코드, 피싱 및 파밍 등이 해당되었다. 키보드 입력 노출의 경우 사용자가 키보드로 입력되는 모든 데이터에 대한 노출이 해당되었고, 명의도용의 경우 본인을 인증하기 위한 주민번호 또는 이메일 등으로 식별 정보에 해당되었다. 문서정보 위·변조는 증명서나 세금납부 등 출력 전후 정보를 악의적으로 변조 및 위조 가능성 문제가 해당되었고, 화면 노출 및 화면 캡처의 경우 악의적인 사용자가 화면을 직접 보거나, 사진을 찍는 문제, PC 내 SW상으로 스크린샷 하는 행위도 포함된다.

V. 대민서비스 유형 별 대응방안

도출된 대민서비스의 보안위협에 따른 보안 요구사항을 기준으로 대민서비스 사용자 보안강화를 위한 대응방안을 도출한다. 보안적용 방안은 각 보안 요구사항에 따른 해결책으로써 활용된다. 대민서비스 보안 요구사항 별 대응방안은 표 11과 같다.

표 11. 대민서비스 보안 요구사항 별 대응방안
Table 11. Countermeasures of e-Goverment Service security requirements

서비스 유형	보안 위협	대응방안(보안기술)
단순정보제공	해당사항 없음	
공공정보제공	통신경로상의 정보노출 및 변조	암호화 통신(SSL, SSH), 가상사설망(VPN), 파일암호화, 전자서명
	유해프로그램 설치로 인한 정보유출	웜/바이러스 백신, 웹 방화벽, 파일 암호화, 개인PC방화벽, 스파이웨어 제거프로그램, 웹 쉘탐지 및 방어
	키보드 입력 노출	키보드 해킹 방지프로그램
	명의 도용	실명인증, 전자서명
증명서 열람 및 발급	통신경로상의 정보노출 및 변조	암호화 통신(SSL, SSH), 가상사설망(VPN), 파일암호화, 전자서명
	유해프로그램 설치로 인한 정보유출	웜/바이러스 백신, 웹 방화벽, 파일 암호화, 개인PC방화벽, 스파이웨어 제거프로그램, 웹 쉘 탐지 및 방어

서비스 유형	보안 위협	대응방안(보안기술)
	키보드 입력 노출	키보드 해킹 방지프로그램
	명의 도용	실명인증, 전자서명
	화면노출, 화면캡처	화면캡처방지 프로그램
	문서정보 위변조	DRM, DNA 코드 파일암호화, 전자서명
납부/결제 조회 및 확인	통신경로상의 정보노출 및 변조	암호화 통신(SSL, SSH), 가상사설망(VPN), 파일암호화, 전자서명
	유해프로그램 설치로 인한 정보유출	웜/바이러스 백신, 웹 방화벽, 파일 암호화, 개인PC방화벽, 스파이웨어 제거프로그램, 웹 쉘 탐지 및 방어
	키보드 입력 노출	키보드 해킹 방지프로그램
	명의 도용	실명인증, 전자서명
	화면노출, 화면캡처	화면캡처방지 프로그램
민원신청 및 신고	통신경로상의 정보노출 및 변조	암호화 통신(SSL, SSH), 가상사설망(VPN), 파일암호화, 전자서명
	유해프로그램 설치로 인한 정보유출	웜/바이러스 백신, 웹 방화벽, 파일 암호화, 개인PC방화벽, 스파이웨어 제거프로그램, 웹 쉘 탐지 및 방어
	키보드 입력 노출	키보드 해킹 방지프로그램
	명의 도용	실명인증, 전자서명
	화면노출, 화면캡처	화면캡처방지 프로그램
국민참여 및 개선	통신경로상의 정보노출 및 변조	암호화 통신(SSL, SSH), 가상사설망(VPN), 파일암호화, 전자서명
	유해프로그램 설치로 인한 정보유출	웜/바이러스 백신, 웹 방화벽, 파일 암호화, 개인PC방화벽, 스파이웨어 제거프로그램, 웹 쉘 탐지 및 방어
	키보드 입력 노출	키보드 해킹 방지프로그램
	명의 도용	실명인증, 전자서명
예약	통신경로상의 정보노출 및 변조	암호화 통신(SSL, SSH), 가상사설망(VPN), 파일암호화, 전자서명
	유해프로그램 설치로 인한 정보유출	웜/바이러스 백신, 웹 방화벽, 파일 암호화, 개인PC방화벽, 스파이웨어 제거프로그램, 웹 쉘 탐지 및 방어
	키보드 입력 노출	키보드 해킹 방지프로그램
	명의 도용	실명인증, 전자서명
위치정보 증강현실	해당사항 없음	
재난안전알림	해당사항 없음	

분석결과 대민서비스의 보안 위협에 따른 대응방안은 총 14개의 종류로 암호화 통신(SSL/TLS, SSH)과 같은 보안프로토콜, 가상사설망(VPN), 파일 암호화, 전자서명, 웜/바이러스 백신, 스파이웨어 제거 프로그램, 웹 쉘 탐지 및 제거, 개인 PC 방화벽, 키보드 해킹 방지 프로그램, 실명인증, 화면캡처 방지 프로그램, DRM와 DNA 코드 등으로 정의 되었다.

Ⅵ. 결론

본 논문은 현재 서비스 중인 289개 대민서비스 사이트를 대상으로 실제 입력, 제공 정보를 분석하여 정보의 중요성을 중심으로 위협을 분석하고 서비스 별 대응방안을 제시하였다. 대응방안 적용 이전 선행되어야 할 과제는 각 서비스 별 보안평가에 대한 문제이다. 모든 서비스에 대해 요구되는 보안 기술을 적용할 수 없기 때문이다. 국제 인증등급 표준 ISO/IEC 29115 에서는 '유출 가능 정보 기반 인증기술 보안등급 수립을 위한 기준'을 정의하고 있으며 적절한 보안 등급의 인증기술을 수립하기 위한 기준으로 총 여섯 가지 분야에 대한 위협을 최소에서 높음 까지 총 네 가지로 분류하고 있다.

국내의 경우 대민서비스의 정보의 중요도에 따라 보안레벨 수립과 보안 위협분야에 대하여 정의할 수 있는 국내 인증등급 표준이 정의되어야 할 것이다. 이후 각 분류된 서비스 별 보안기술이 단계적으로 적용해 나가야 한다. 현재 제공하는 개발 보안 가이드라인은 각 분야별 다양한 가이드라인이 존재한다. 대부분 보안위협에 따른 대안을 제시하고 있기 때문에 운영 중인 사이트에 적용하기 어려운 문제가 있다. 어떠한 서비스와 중요정보를 취약성으로 보고 해결해야 하는지 범위가 명확하지 않기 때문이다. 이는 사이트 내 정보의 중요도나 서비스 별 보안등급을 판단할 수 있는 가이드라인 수준의 기준이 필요하다는 것을 의미한다.

대민서비스 입력정보 분석 결과 대민서비스는 주로 ID/PW, 공인인증서(NPKI, GPKI)를 사용하여 사용자에 대한 인증을 수행했다. 민간에서 사용되는 인증기술보다 보안성이 낮은 단일 채널의 인증기술을 사용하기 때문에 다중채널, 다중 Factor등 보안성이 높은 인증 기술을 도입 또한 필요할 것이다.

References

[1] Mun-Seog An, "Study on e-government information security system, deployment orientation", Korean Institute of Information Security, Vol.13 No.3, 1-14 (14 pages), 2003

[2] Eun-Seon Lee, "A Study on Security of E-Government Service Based on Web Service", Korea Information Processing Society, Vol.12 No.3, 347-360 (14 pages), 2005

[3] Myung-Won Song, "e-government Civil Service (G4C) Security Management Plan", National Informaion-Society Agency, Weekly Technical Trends No.1304, 2007

[4] Eui-Young Jung, "E-government Civil Service Status and Security Countermeasures", National Informaion-Society Agency, e-goverment Focus 2007-05, 2007

[5] Nak-Hyun Kim, "Importance of e-government Civil Service Privacy Standards", Korea Internet & Security Agency, 2014

[6] Ministry of Public Administration and Security, "User Take-up Survey of e-Government Service", Approval number No. 11029, 2012.

[7] Ministry of Public Administration and Security, "Civil Government portal - 24 Civil Service Usage", 2013

저자 소개

최 도 현(정회원)

- 2008년 2월 : 동서울대학 컴퓨터소프트웨어 공학사
- 2010년 8월 : 숭실대학교 컴퓨터학과 석사
- 2010년 9월 ~ 현재 : 숭실대학교 컴퓨터학과 박사과정
- 관심분야 : Mobile Security, Virtualization, 802.16x, PKI, Secure Coding
- E-mail : cdhgod0@ssu.ac.kr

전 문 석(정회원)

- 1981년 2월 : 숭실대학교 전자계산학과 졸업
- 1986년 2월 : University of Maryland Computer Science 석사
- 1989년 2월 : University of Maryland Computer Science 박사
- 1991년 3월 ~ 현재 : 숭실대학교 정교수
- 관심분야 : 정보보호, 네트워크 보안, 전자여권, 암호학
- E-mail : mjun@ssu.ac.kr

박 중 오(정회원)

- 2000년 7월 : 성결대학교 컴퓨터공학과 졸업
- 2003년 3월 : 명지대학교 전자계산교육 석사
- 2011년 8월 : 숭실대학교 컴퓨터공학 박사
- 2013년 3월 ~ 현재 : 동양미래대학교 조교수
- 관심분야 : PKI, Network security, 암호학
- E-mail : jopark13@dongyang.ac.kr