

개인정보보호법을 대비한 개인정보보호 시스템에 관한 연구

김동례*, 심기창**, 전문석***

요 약

개인정보보호법이 2011년 3월 국회 법사위에서 통과되어 2011년 9월 30일 시행예정에 있다. 시행예정에 있는 개인정보보호법은 기존 공공기관의 개인정보보호에 관한 법률을 포함하게 된다. 기존의 개인정보보호 관련 법규 및 시행령은 크게 관리적 보호조치와 기술적 보호조치로 구분된다. 기술적 보호조치의 주요 기반기술은 개인정보보호시스템, 접근통제, 암호화, 출력매체, 접근 및 이용, 웹사이트 노출방지대책 등으로 분류할 수 있다. 본 연구에서는 개인정보보호 기술적 조치 사항의 주요기반기술에 대해 기술 및 솔루션, 시스템을 살펴보고 최근 웹 사이트 및 내부 업무시스템에서의 개인정보보호 시스템 특징을 연구하고 단계적 적용을 제안하였다. 본 연구를 통하여 2011년 9월30일 시행되는 개인정보보호법에 대비하여 기술적 보호조치 단계를 제시함으로써 개인정보 담당자 및 정보보호 담당자에게 한정된 예산과 일정기간에 단계별로 개인정보보호 수준을 높이는 참조 모델로 활용될 수 있을 것으로 기대된다.

I. 서 론

정보사회의 고도화와 개인정보의 경제적 가치 증대로 사회 모든 영역에 걸쳐 개인정보의 수집과 이용이 보편화되고 있다. 그러나 2011년4월에도 한 해커가 현대캐피탈의 보조사버에서 고객들의 이름, 주민등록번호, 이메일, 휴대전화 번호 등 42만명의 개인정보를 빼내갔다. 게다가 문제는 13,000명의 신용등급 정보와 비밀번호까지 유출된 것으로 현대캐피탈 자체조사에서 밝혀졌다. 현재까지 공공기관은 공공기관의 개인정보보호에 관한 법률 및 시행령, 시행규칙에 의해 정기적인 개인정보 실태점검 및 공공기관 개인정보 수준진단을 시행하였다. 이에 따라 공공기관은 관리적 보호조치와 기술적 보호조치를 해 왔다. 반면 민간 기업은 자체적으로 준비를 해 왔으나, 한국인터넷진흥원(KISA)의 민간기관 개인정보 유·노출점검에 의해 의존하여 점검이 이루어져 왔다. 그럼에도 불구하고 최근 개인정보의 유출·오용·남용 등 개인정보 침해 사례가 지속적으로 발생함에 따라 국민의 프라이버시 침해는 물론 명의도용,

전화사기 등 정신적·금전적 피해를 초래하고 있다. 공공부문과 민간부문을 망라하여 국제 수준에 부합하는 개인정보 처리원칙 등을 규정하고, 개인정보 침해로 인한 국민의 피해 구제를 강화하여 국민의 사생활의 비밀을 보호하며, 개인정보에 대한 권리와 이익을 보장하려 개인정보보호법이 시행예정에 있다.

본 연구의 구성은 2장 관련연구에서 2011년 9월 30일에 시행하는 개인정보보호법의 특징을 살펴보고, 개인정보보호법의 기술적보호조치의 주요사항을 정리한다. 3장 개인정보보호 시스템에서는 최근의 특징적인 개인정보보호 주요 기술과 적용방법 및 그 특징을 살펴본다. 4장 개인정보보호 솔루션 단계별 적용 방안에서는 개인정보보호 시스템 단계별 적용을 제안하고 5장에서 결론과 향후발전방향을 제시한다.

II. 개인정보보호법의 기술적 보호조치의 특징

개인정보보호법은 기존의 공공기관의 개인정보보호에 관한 법률 내용을 포함하게 되며, 개인정보를 취급하

* (주)이지서터 기업부설연구소 연구소장 (drkim@easycerti.com)

** (주)이지서터 대표이사 (gcschim@easycerti.com)

*** 숭실대학교 정교수 (mjun@ssu.ac.kr)

[표 1] 개인정보관련 주요 법률 및 고시의 특징

법률 및 고시	개인정보관련 주요조항	주요 내용
개인정보보호법	개인정보 보호 원칙(제3조제4항, 제6항), 국가 등의 책무 (제5조제1항)	개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해 받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.
	28조 개인정보취급자에 대한 감독	개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘, 감독을 받아 개인정보를 처리하는 자에 대하여 적절한 관리, 감독을 행하여야 한다.
	29조 안전조치의무	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.
정보통신망 이용촉진 및 정보보호 등에 관한 법률	개인정보의 보호조치[제28조 1항]	개인정보를 취급할 때에는 개인정보의 분실, 도난, 누출, 변조 또는 훼손을 방지하기 위하여 기술적, 관리적 조치를 하여야 한다.
	개인정보의 보호조치[시행규칙 제9조]	개인정보의 안전성 확보에 필요한 관리적 조치를 해야 한다. -개인정보보호를 위한 정기적인 자체 감사 실시 -개인정보의 안전성 확보에 필요한 기술적 보호조치
방송통신위원회 고시	개인정보의 암호화[제2009-21]	개인정보를 PC에 저장할 때에는 이를 암호화 해야 한다.

는 모든 공공·민간, 비영리단체 등의 대상범위 확대와 온·오프라인의 보호범위 확대되며, 관리적 보호조치는 물론 기술적 보호조치의 적용범위 확대에 그 특징이 있다. 개인정보관련 주요 법률 및 고시의 특징을 살펴보면 [표 1]과 같다.

개인정보보호법은 17대 국회에서 발의 되어, 행정안전부에서 11차례의 논의와 공청회를 거쳐 2008년 11월 28일 국회에 제출되었다. 국회의 상정을 통해 2011년 3월 29일 공포되고 2011년 9월 30일 시행이 된다. 개인정보보호법 제정으로 달라지는 점은 [표 2]와 같다.

개인정보보호의 기술적 보호조치의 내역을 살펴보면 (1)개인정보보호시스템, (2)개인정보보호 시스템 접근 통제, (3)개인정보 파일대상, (4)개인정보 저장 및 출력 매체, (5)개인정보처리시스템의 접근 및 이용, (6)웹사이트 개인정보 노출방지 대책으로 나누어 볼 수 있다.

[표 2] 개인정보보호법 제정으로 달라지는 점

구분	현행	개인정보보호법 (11.9월 시행)
규율대상	공공기관, 정보통신사업자 등 개별법이 규정하고 있는 경우 (51만개 사업자)	공공·민간의 모든 개인정보 처리자 (350만개 사업자)
보호범위	컴퓨터 등에 의해 처리되는 개인정보파일	종이문서에 기록된 개인정보도 포함
주민등록번호등고유식별정보처리제한	고유식별정보의 민간사용에 대한 사전적 제한 규정 없음	원칙적 처리금지 (정보주체의 별도 동의, 법령의 근거가 있는 경우 예외 허용)
유출통지	관련 제도 없음	개인정보 유출통지 의무화
집단분쟁조정	관련 제도 없음	집단분쟁제도 도입 (재판상 화해 효력 부여)
단체소송	관련 제도 없음	단체소송(권리침해 중지) 도입
위원회	국무총리 소속 개인정보보호 심의위원회	대통령 소속 개인정보보호위원회

행정안전부의 공공기관 개인정보 수준진단 지표에서 기술적 보호조치 항목을 분석하면 다음의 [표 3]와 같은 기술 및 솔루션으로 정리할 수 있다.

본 연구는 [표 3]의 기술적 보호조치에서 웹 시스템과 관련이 있는, 즉 어플리케이션 레벨을 중심으로 개인정보보호를 살펴보고자 한다. 개인정보보호시스템에서 웹 어플리케이션 방화벽, 즉 웹 방화벽을 살펴 볼 것이며, 개인정보처리시스템의 접근 및 이용 측면에서는 개인정보처리시스템 로그파일의 생성·관리, 로그파일의 정기적 분석 및 결과 보고에 대하여 제시할 것이다. 또한 웹사이트 개인정보 노출방지 대책으로 개인정보 노출 사전차단 필터링 시스템과 개인정보노출 자체모니터링 시스템에 대하여 그 특징을 볼 것이다.

III. 개인정보보호 시스템의 특징 및 적용방안

개인정보보호법의 기술적 보호조치 기반기술에 대한 기술 및 솔루션을 살펴보면 서버와 클라이언트에서 의 개인정보보호 솔루션으로 구분된다. 클라이언트 기반의 솔루션은 단독으로 운영이 가능한 반면 서버 개인정보 보호 솔루션은 네트워크의 트래픽 및 운영환경에 영향을 받는다. 본 논문에서는 상호 연관관계가 큰 네트워크

[표 3] 개인정보보호 주요 기반기술

기반기술	기술 및 솔루션 적용
개인정보보호 시스템	키보드해킹방지솔루션, 백신프로그램 설치
	침입차단시스템과 침입탐지시스템 설치
	웹 방화벽 설치와 서버보안 실시
개인정보보호 시스템 접근통제	차등 접근권한 지정 및 비밀번호 의무갱신
	개인정보처리시스템에 관리자 접근시 PKI방식 물리적 보안장치 설치 및 출입대장 기록·관리
개인정보 저장·전송시 암호화	개인정보 DB에 대한 중요필드의 암호화
	사용자PC부터 웹서버구간 간 암호화
개인정보 파일대장	개인정보파일대장 작성·관리와 내용에 정보기록
개인정보 저장 및 출력매체	개인정보 출력물에 대한 워터마킹
	P2P, 웹하드 등 비인가 프로그램의 접속 차단
개인정보처리시스템의 접근·이용	개인정보처리시스템 로그파일의 생성·관리 백업
	로그파일의 정기적 분석 및 결과 보고
웹사이트 개인정보 노출방지 대책	첨부파일 게재 시 상급자 등의 확인
	개인정보 노출 사전차단 필터링
	개인정보노출 자체모니터링 실시
	공공·PIN 등 웹사이트 주민등록번호 대체수단 도입

및 서버에 영향을 주어 전체 네트워크에 부하를 주는 기술 및 솔루션에 대해 살펴보고자 한다.

3.1 기존 개인정보보호 관련 기술 및 솔루션

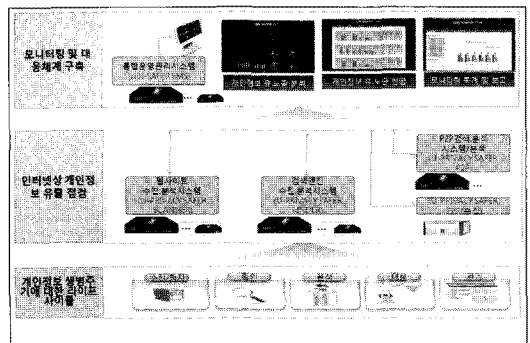
네트워크 및 서버의 개인정보보호와 관련된 대표적 기술 및 솔루션과 그 특징은 [표 4]와 같다. 여기서는 기존의 보안 기술과 솔루션은 어플리케이션 레이어와 웹 페이지에 대한 필터링과 방화에 능동적이지 않음을 알 수가 있다. 그 원인은 기존의 보안 기술과 솔루션은 패킷 단위의 필터링 즉 TCP/IP기반에서 그 역할을 수행하였다. 현재 웹서비스의 증가와 하드웨어의 성능향상으로 콘텐츠 필터링의 기술이 급속도로 발전함에 따라 네트워크 보안에서 웹 콘텐츠의 필터링 및 보안이 가능해 졌다. 우리는 웹의 특성에 따라 인터넷상 개인정보 노출점검, 웹 어플리케이션 방화벽, 개인정보 필터링 시스템, 개인정보 종합관리 시스템을 살펴 보고 그 특징 및 적용방안을 제안한다.

[표 4] 인정보를 위한 주요 기술적 보호조치 솔루션

구분	방화벽	IDS	IPS	Secu-OS
대상	내부 NW	내부 NW	NW, Server	서버
계층(OSI)	L3	L3	L4	OS 커널
HTTP 보안	×	×	△	×
SSL 보안	×	×	△	×
방어 유형		- DoS/ DDoS - Exploit공격 - 일부웹공격기법		
Unknown 방어	×	×	△	×
Web Caching	×	×	×	×
설치방식	Inline	Bypass	Inline	웹서버
필터링단위	패킷	패킷	패킷/세션	
필터링방식	포지티브	패킷/스트림 (네거티브)	패킷/스트림 (네거티브)	포지티브
신용카드번호 보호	×	×	×	×
주민등록번호 보호	×	×	×	×

3.2 인터넷상 개인정보 노출점검

인터넷의 발달과 함께 홈페이지 등 웹 서버가 외부에서 접속가능하게 되었다. 따라서 웹페이지에 대한 주기적인 개인정보 점검이 필요하다. 주기적인 점검을 하더라도 웹서버의 게시판 등에서 개인정보가 1차적으로 구글, 바이두 등의 포탈에서 검색해 갔을 때는 캐시서버에 의해 웹서버의 원본 개인정보를 삭제하더라도 계속적으로 유통이 되어진다. 따라서 2차 피해의 예방을 위해 구글, 바이두 등의 포탈도 점검을 해야한다. 만일 구글 등의 검색서버로부터 파일을 다운로드 받은 사람의 PC가



[그림 1] 인터넷상 개인정보 노출점검에 대한 흐름도

공유되어 있거나 웹하드등에 올려 유통이 될 경우에는 3차적으로 피해를 입게된다. 따라서 인터넷상 개인정보 유출 점검은 (1)웹사이트에대한 점검, (2)구글, 바이두 등 포털에 대한 점검, (3)P2P 개인정보 점검이 포함되어져야 한다. [그림 1]은 개인정보 생명주기에 대한 인터넷 개인정보 유출 점검의 흐름도를 표현 한 것이다.

3.3 웹 어플리케이션 방화벽

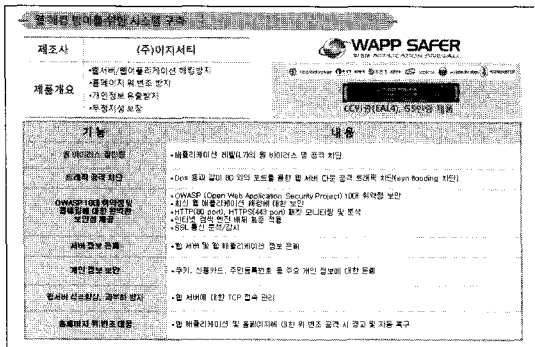
웹 어플리케이션 방화벽(웹방화벽)은 웹 어플리케이션을 통해 해킹을 함으로써 개인정보를 취득할 수 있다. 물론 웹 방화벽은 해킹 방지 및 홈페이지 위변조 방지에 그 목적이 있다. 기본적으로 OWASP (Open Web Application Security Project) 10대 취약점 보안 및 국정원의 8대 웹 취약점을 방어해야 한다. [그림 2]는 웹 방화벽의 기능 및 내용 및 기능에 대한 예를 표시하였다.

웹 방화벽은 기존의 네트워크 장비와 달리 패킷 필터링이 아닌 콘텐츠 필터링을 수행하여야 그 기능을 만족할 수 있고 오작동을 최소화 할 수 있다. 또한 네트워크

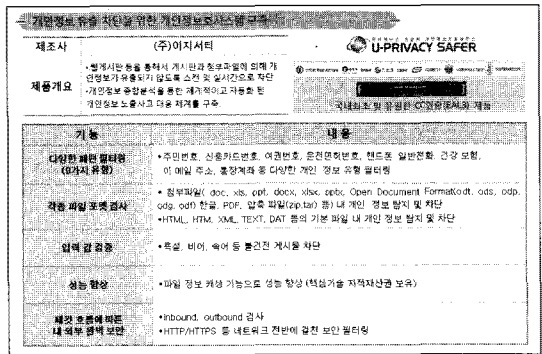
의 어플라이언스 타입의 보안장비는 소프트웨어 타입에 비해 웹 소스가 변경 되거나, 이기종 환경의 웹서버에서도 중단 없는 서비스의 연속성을 보장하여야 한다. [그림 3]은 이런 콘텐츠 필터링 및 구성도를 소개하였다.

3.4 개인정보보호 솔루션(개인정보 필터링 시스템)

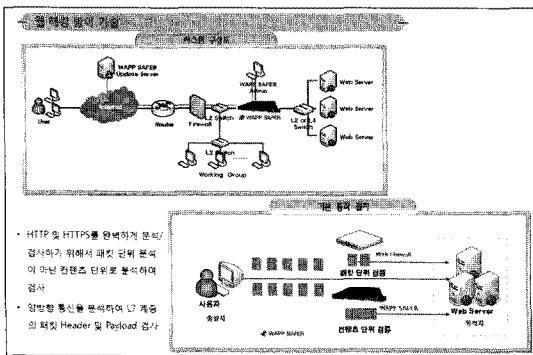
게시판 등의 웹페이지에 대한 개인정보보호는 웹 방화벽에서도 수행할 수 있지만, doc, xls, ppt, docx, xlsx, pptx, Open Document Format(odt, ods, odp, odg, odf) 한글, PDF, 압축 파일(zip,tar) 등의 다양한 확장자를 가지는 첨부 파일 내의 개인정보유출은 대용량이라는 점에서 그 위험이 더욱 크다. 특히 위와 같은 첨부 파일은 클라이언트 프로그램으로 하드웨어의 자원을 분배하여 사용하기 보다는 독점적으로 사용함에 그 문제가 있다. 특히 다수의 사용자가 동시에 접근하여 수행하였을 경우에는 시스템의 부하에 영향을 줌으로서 서비스의 안정성을 크게 떨어 뜨린다. 따라서 개인정보



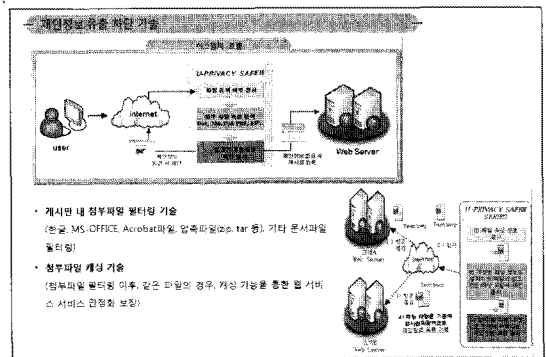
[그림 2] 웹 방화벽 기능 및 내용에 대한 사례



[그림 4] 개인정보보호 기술 및 솔루션의 기능과 내용의 사례



[그림 3] 웹 방화벽의 콘텐츠 필터링 및 구성도

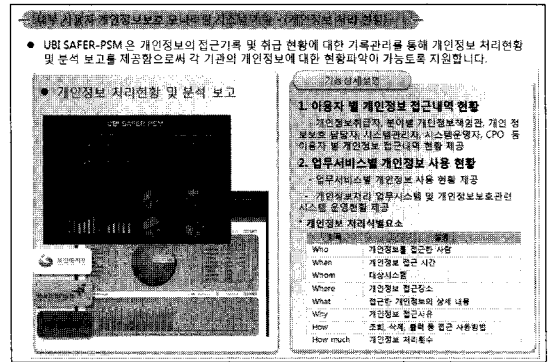


[그림 5] 네트워크 계층별 검사를 통한 웹 보안 시스템 및 그 방법

보호 솔루션, 즉 개인정보 필터링 시스템은 개인정보 필터링의 정확성은 물론 서비스의 안전성을 보장할 수 있는 기술이 중요하다. 필터링 방법에 대한 기술과 MSF(네트워크 계층별 검사를 통한 웹 보안 시스템 및 그 방법)의 활용이 중요한 요소이다. [그림 4]는 개인정보보호 기술 및 솔루션의 기능과 내용의 사례를 보여 주고 [그림 5]는 네트워크 계층별 검사를 통한 웹 보안 시스템 및 그 방법의 구성도를 보여 준다.

3.5 개인정보 종합관리 시스템(개인정보 상시 모니터링 시스템)

웹 사이트에 대한 개인정보 노출점검, 웹 해킹 방지 솔루션, 개인정보 필터링 시스템에 의하여 인터넷 상의 개인정보 노출 점검 및 개인정보 차단의 보안을 적용한 후 외적으로 개인정보보호 단계가 한 단계 업그레이드 되었다. 그러나 업무시스템에 대한 권한 있는 사용자에 의한 개인정보 오남용은 더 큰 사회적 문제가 되고 있다. 특히 특정인에 대하여 권한을 오남용 하는 것은 프라이버시 침해에 위협적인 요인이다. 또한 개인정보보호의 중요성 측면에서 개인정보의 생명주기(수집, 보유, 이용 및 제공, 파기)에 따른 개인정보의 체계적 관리 및 오남용 및 대량노출을 방지하는 개인정보 종합관리라 필요하게 되었고, 국민 대부분의 개인정보를 보유하고 있는 보건복지부, 교육과학기술부는 개인정보 상시모니터링 시스템, 개인정보 종합관리 시스템을 구축 운영하고 있다. 금번 행정안전부도 기존의 개인정보에 대한 이력관리에서 오남용 모니터링을 구축하는 것도 국민에 대한 기본권을 보호하기 위함이다. [그림 6]은 개인정보



(그림 7) 개인정보보호 모니터링 구현 기술(개인정보 처리 현황)

종합관리 시스템, 개인정보 모니터링 시스템의 기능과 내용을 정리한 예제이다.

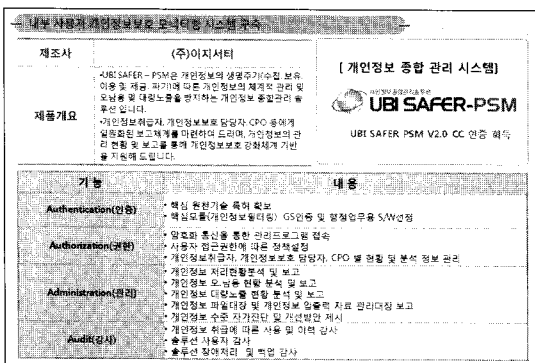
개인정보 생명주기에 따른 개인정보 처리 현황을 모니터링 하는 것은 개인정보 처리 식별 요소에 의해 결정되고 처리현황 및 분석보고가 이루어져야 한다. 개인정보보호 모니터링 구현 기술은 [그림 7]과 같다.

IV. 개인정보보호 시스템션 단계별 적용 방안

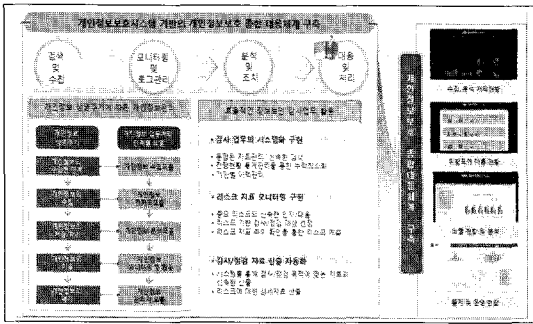
기존의 기술과는 달리 개인정보보호법의 기술적 보호조치에 해당하는 제시된 개인정보보호 기술 및 솔루션은 콘텐츠 필터링에 그 기반을 둔다. 또한 개인정보 처리자 및 개인정보보호 담당자는 법률의 제정에도 불구하고 한정된 예산과 정해진 스케줄에 의해 조직의 개인정보보호 조치를 취하여야 한다. 이에 본 논문에서 제안된 기술과 솔루션에 대하여 적용 단계의 모델과 안정성 측면에서 보안솔루션 최소 인증의 범위에 대하여 정리하고자 한다.

4.1 개인정보보호를 위한 단계별 적용 방안

제안된 개인정보보호 기술과 솔루션은 일반 업무 프로세스와 달리 개인정보 생명주기에 따라 관리되어진다. 개인정보 생명주기는 (1)개인정보의 수집 전 단계, (2)개인정보의 수집, (3)개인정보의 저장 및 관리, (4)개인정보의 이용, (5)개인정보의 폐기의 단계를 거친다. 본 논문은 [그림 8]과 같이 개인정보 업무처리 단계별 모듈로 (1)개인정보 수집모듈, (2)개인정보 전처리 모듈, (3)개인정보 분석모듈, (4)개인정보 모니터링 및 활용, (5)개인정보 관리자 모듈로 구성함을 제안한다. [그



(그림 6) 개인정보 종합관리 시스템, 개인정보 모니터링 시스템의 주요 기능과 내용의 사례기록



(그림 8) 개인정보 생명주기에 따른 개인정보보호 종합대응 체계

림 8]은 개인정보 생명주기에 따른 개인정보보호 종합대응 체계를 표현하였다.

본 제안은 개인정보보호 기술과 솔루션이 효율적인 정보보안 감사업무에 활용될 수 있음을 제시한다. 세가지로 구분하면, 첫째 감사업무의 시스템화 구현, 둘째 리스크 지표 모니터링 구현, 셋째로 감사 및 점검 자료 산출 자동화의 활용이 될 수 있다.

[표 5]는 위 개인정보 생명주기별 프로세스를 반영하여 3장에서 제안된 컨텐츠 필터링 기반의 기술 및 솔루션의 적용단계를 제시하였다. 특히 1단계는 조직의 특성 및 현황을 반영하고자 사전분석단계로서 개인정보보호를 위한 자가진단 단계를 제안하였다. 이는 개인정보영향평가, 개인정보 수준진단 실태점검의 필요성을 의미하며, 외부의 조직에 의하여 진단 혹은 컨설팅이 필요

(표 5) 개인정보보호 단계별 종합 대응체계

단계	기술적 대응절차	수행내역
1단계	개인정보보호를 위한 자가진단	- 개인정보보호를위한조직및시스템에 대한개인정보보호수준진단수행 - 정보보호시스템구축및개선때마른개인정보영향평가수행
2단계	개인정보보호시스템구축	- 홈페이지서비스의웹해킹공격방어를 위한웹보안솔루션구축운영 - 개인정보유출방지를위한개인정보보호솔루션구축운영
3단계	정기적 개인정보노출 점검 수행	개인정보유출대상(홈 페이지, 인터넷(검색포털,P2P),개인PC등)에대한정기적인개인정보노출점검을위한시스템구축및수행
4단계	내부업무시스템모니터링	내부사용자의업무통한개인정보유출 및오남용예방을위한모니터링시스템구축및운영

제품명	인증번호	인증기관	인증등급	인증사항	인증일
Evernote V2.0	1015-0538-2011	민통본	E-AL2	개인정보보호	20110609
PrivacyFilter V2.0	0515-0217-2011	인통본	E-AL0	개인정보보호	20110610
UBI SAFER P&M V2.0	1015-0108-2011	이시제티	E-AL2	개인정보보호	20110411
U-PRIVACY SAFER V	0515-0277-2011	이시제티	E-AL3	개인정보보호	20110102
Privacy-VX.0	1015-0242-2010	소원사	E-AL2	개인정보보호	20100512

(그림 9) 국가정보원 개인정보 제품유형 CC인증제품 목록 (2011.09 기준)

할 수 있음을 암시한다. 2단계는 예산이나 스케줄의 부담이 작은 범위에서부터 개인정보보호 시스템의 구축 단계를 제안하였고, 3단계는 주기적인 개인정보 노출 점검을 제안함으로써 개인정보 관제 체계를 제안한다. 마지막 단계에서는 내부 개인정보 처리자의 관리적 보호조치에도 불구하고 오남용 사고를 대비하며, 조직원의 개인정보 인식제고의 효과가 큰 개인정보 상시모니터링 체계 혹은 개인정보 종합관리 체계를 구축하여야 한다.

4.2 개인정보보호 기술 및 솔루션에 필요한 인증

본 논문은 개인정보보호법 발효에 따른 개인정보보호 기술 및 솔루션의 기능 및 구성을 제안하였다. 또한 예산과 스케줄을 고려한 적용방안을 제시하였다. 한편 이러한 기술과 솔루션은 다양한 특징을 가지고 있으며, 개인정보를 위한 필터링 기술은 일반 MIS 등 경영관리 시스템과 달리 프로세스와 Input/Output의 검증이 쉽지 않다는 특징이 있다. 또 시스템 내부의 메카니즘 검증이 쉽지 않다. 따라서 품질관리 측면과 안정성 측면에서 도입되는 개인정보보호 기술과 솔루션은 보안솔루션의 일부분으로 국가정보원의 CC인증 및 한국정보통신기술협회(TTA)의 GS 품질인증 제품을 선정할 것을 권고한다. [그림 9]는 국가정보원 개인정보 제품유형 CC인증 제품 목록(2011.09 기준)을 표현 하였다.

V. 결 론

본 논문에서 개인정보보호법 제정에 따라 달라지는 사항들을 살펴보고 기술적 보호조치의 특징과 기술 및 솔루션에 대하여 살펴보았다. 기술적 보호조치의 기술

및 솔루션의 종류를 진단했고, 어플리케이션 레이어에서 개인정보보호를 위한 오답률의 최소화를 위한 콘텐츠 필터링을 살펴보았다. 기존 개인정보보호 관련 기술 및 솔루션의 특징을 살펴보고, 개인정보보호를 위한 기술 및 솔루션에서 클라이언트 기반의 솔루션은 단독으로 운영이 가능한 반면 서버 개인정보보호 솔루션은 네트워크의 트래픽 및 운영환경에 영향을 받음에 따라 본 논문에서는 상호 연관관계가 큰 네트워크 및 서버에 영향을 주어 전체 네트워크에 부하를 주는 기술 및 솔루션에 대해 특징 및 적용방안을 제시하였다.

특히 웹의 특성에 따라 (1)인터넷상 개인정보 노출점검, (2)웹 어플리케이션 방화벽, (3)개인정보 필터링 시스템, (4)개인정보 종합관리 시스템의 특징 및 적용방안을 제안하였다.

마지막으로 개인정보보호를 위한 솔루션들에 대한 적용방안으로 단계적 적용방안을 제안하고 4단계의 방안을 제시했다. 이러한 제안은 예산과 일정에 대한 개인정보 처리자 및 담당자에게 체계적인 개인정보보호에 대한 적용에 도움이 되고 보다 프라이버시에 대한 안전한 사회로의 접근에 기여할 것이라 믿는다. 향후 연구과제로는 해킹에 의한 개인정보 유출에 대비하여 악성코드에 대한 정적분석 및 동적분석에 대한 분석기법에 대하여 연구를 제안한다. 또한 스마트 폰의 보급에 따라 모바일 악성코드 및 개인정보보호의 필요성이 높아짐에 따라 이 분야의 연구도 수행 되어야 할 것이다.

참고문헌

- [1] 대한민국국회, “개인정보보호법,” 법률 제10465호, March 2011.
- [2] 대한민국국회, “공공기관의 개인정보보호에 관한 법률,” 법률 제4743호, January 1994.
- [3] 대한민국국회, “공공기관의 개인정보보호에 관한 법률 시행령,” 대통령령 제21025호, September 2008.
- [4] 대한민국국회, “공공기관의 개인정보보호에 관한 법률 시행규칙,” 행정자치부령 제1호, March 2008.
- [5] 차건상, “개인정보보호법 주요 내용 및 향후 추진과제,” 행정안전부, pp.2-7, June 2011.
- [6] (주)이지서티, “2011년 개인정보보호 수준진단 진단지표 및 프로그램 상세 매뉴얼,” June 2011.
- [7] (주)이지서티, “2009년 개인정보보호 수준진단 진단지표 및 프로그램 상세 매뉴얼,” June 2009.
- [8] (주)이지서티, “2008년 개인정보보호 수준진단 프로그램 매뉴얼,” June 2008.
- [9] (주)이지서티 기업부설연구소, “내부정보 유출 자동모니터링 대응량 로그분석 기술개발 중소기업기술혁신개발사업 최종보고서,” 중소기업청, May 2010.
- [10] (주)이지서티 기업부설연구소, “고성능 네트워크 프로세스 기반의 보안관리 웹 어플리케이션 방화벽 개발 정보통신 산업경쟁력강화사업 최종보고서,” 정보통신부, May 2007.
- [11] 여성구, 심미나, 이상진, “웹 로그 데이터에 대한 개인정보 위협분석 및 보안 가이드,” 정보보호학회 논문지, 19(6), pp.135-143, 2009년 12월.
- [12] 이준택/배민호/박미영 공저, “네트워크 보안과 방화벽 구축,” 가남사, 2002.
- [13] 김효중, “웹 환경에서 HTTP 프로토콜의 특성을 활용한 웹 방화벽 성능향상 모듈설계,” 석사학위논문, 숭실대학교 대학원 컴퓨터학과, 2011년2월
- [14] 전정훈, “인바운드 네트워크의 성능 및 보안성 향상을 위한 전형적인 방화벽의 기능분산,” 박사학위논문, 숭실대학교 대학원 컴퓨터학과, 2009년 2월

〈著者紹介〉



김 동 래 (Dong Rye Kim)
 2000년 2월 : 한국외국어대학교 경
 영정보대학원 응용전산학과 석사
 2010년 9월~현재 : 숭실대학교
 컴퓨터학과 박사과정
 2002년 8월~현재 : (주)이지서터
 기업부설연구소 연구소장
 1995년~1999년 : 상명대학교 AIT
 연구소
 1999년~2002년 : (주)마크애니 기
 술기획/마케팅 팀장
 <관심분야> 개인정보보호, 악성코
 드, 웹 어플리케이션 방화벽, 포렌
 직, 컴퓨터 통신, 정보보호



심 기 창 (Gi Chang Shim)
 1993년 2월 : 숭실대학교 졸업
 1995년 8월 : 한국외국어대학교 경
 영정보대학원 응용전산학과 석사
 2002년 8월~현재 : (주)이지서터
 대표이사
 1995년~2001년 : 대림정보통신(현,
 대림 I&S) 솔루션사업부 개발팀장
 2001년~2002년 : (주)마크애니 공
 공사업부 이사
 2007년 7월~현재 : 한국전자문서
 산업협회 이사
 <관심분야> 개인정보보호, 악성코
 드, 웹 어플리케이션 방화벽, 포렌
 직, 컴퓨터 통신, 정보보호



전 문 석 (Moon-seog Jun)
 1981년 2월 : 숭실대학교 졸업
 1986년 2월 : University of Mary-
 land Computer Science 석사
 1989년 2월 : University of Mary-
 land Computer Science 박사
 1991년 3월~현재 : 숭실대학교 정
 교수
 <관심분야> 정보보호, 네트워크
 보안, 전자여권, 암호학