개인정보시스템 위험도 분석 기준 지원 도구 개발 연구

한경수* · 정현미* · 이강수*

*한남대학교 컴퓨터공학과

Personal Information System risk analysis standard supporting tool development

Kyung-su Han*, Hyun-mi Jung *, Gang-Soo Lee *

*Dept of Computer Engineering, Hannam University

E-mail : psksmail@hnu.kr, mihj@se.hannam.ac.kr, gslee@eve.hannam.ac.kr

요 약

2011년 9월 30일부터 개인정보보호법 제29조 및 개인정보의 안전성 확보조치 기준 제7조 5항에 따라 공공 및 민간 기업의 개인 정보처리 자가 내부 망에 고유 식별 정보를 저장하는 경우, 위험도 분석 기준결과에 따른 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다. 2012년 12월 31일까지 암호화 기술의 적용 또는 이에 상응하는 조치를 완료해야한다. 행정안전부 및 한국인터넷진흥원에서 제공한 개인정보 위험도 분석 기준을 토대로 해당 시스템에서 개인정보 처리 시 위험도분석 기준을 제시 하는 지원 도구를 개발 및 연구 하였다.

ABSTRACT

Since September 30 2011, depending on Personal Information Protection Act article 29 and Act standard securing personal information safety the fifth clause of article 7, in case personal information manager of public and private enterprise saves unique indentifying information to internal network, the manager can enforce that decide checking of cryptographic application and a range of application following risk analysis criteria result. Until December 31 2012, enterprises complete the application of cryptographic technology or the equivalent.

The paper is research and development on supporting tool that suggest risk analysis criteria based on personal information risk analysis criteria that be provided by MOPAS(Ministry Of Public Administration and Security) and KISA(Korea Internet Security Agency) for personal information processing.

키워드

개인정보 보호법, 개인정보 처리 자, 위험 분석 기준, C#, WPF

Ⅰ. 서 론

개인정보 보호법 제33조(개인정보 영향평가) 공공기관의 장은 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선사항 도출을 위한 평가를 하고, 그 결과를 행정안정부장관에게 제출해야 한다. 이 경우 공공기관의 장은 영향평가를 행정부장관이 지정하는 기관 중에서 의뢰해야 한다 **[1]**.

이러한 개인정보 영향평가는 개인정보처리시스템 즉, 개인정보를 처리할 수 있도록 체계적으로 구성한 데이터베이스시스템을 운영하고 해당시스템에 대한 개인정보보호를 위해 관리 및 위험도 평가를 포함 하고 있다.

위험도 분석은 개인정보 처리 시스템에 있는 개인정보보호를 유출시 정보 주체의 권리를 침해하는 위험의 정도를 위험도 분석 기준을 이용하여 분석하는 것을 말한다. 이 기준은 고유 개인정보를 암호화 하지 않고 저장하는 경우 개인정보처리 자가 이행해야 할 최소한의 보호조치 기준으로 어느 하나의 항목이라도“아니오”에 해당하는 경우 암호화 대상이다.

본 논문은 행정안전부와 한국인터넷 진흥원에

서 제공한 '개인정보 위험도 분석'의 내용을 바탕으로 사용자 기반, 정책기반, 네트워크기반, DB 및 APPLICATION기반, 웹기반, 위험도 분석 점검항목을 데이터베이스 자료로 사용한다. 개인정보 처리 자가 위험도 분석 점검항목을 체크하고, "아니오"로 대답하는 항목을 최종 REPORT로 작성하여 항목에 대한 취지와 해설을 보여주는 도구를 개발 및 연구 하였다.

Ⅱ. 관련 연구

1.위험도 분석 기준 및 절차.

위험도 분석 기준은 현황 조사, 위험도 분석 점검 항목, 위험도 분석 결과 보고서로 구성되어 있다.

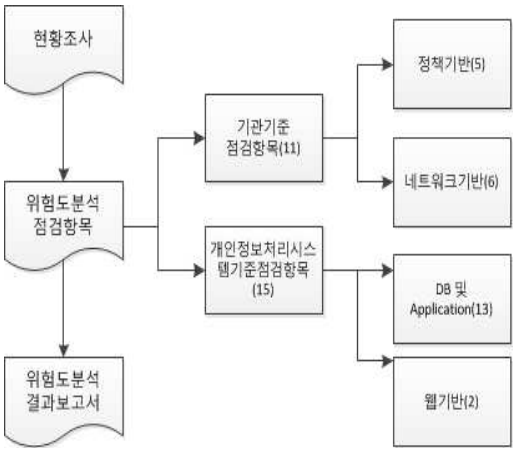

그림 1 위험도 분석 기준 절차**[2].**

위험도 분석을 위해 개인정보 파일 보유 여부의 현황을 조사하고, 위험도 분석 항목별 점검을 수행한다. 위험도 분석 결과보고서를 작성하여 내부결재 후 보관하며, 점검 결과에 따라 고유 식별 정보 암호화 등을 수행해야한다.

2.사용자 기반의 위험도 분석

주민등록 번호 저장에 대하여 의무화한 정보 통신망 법 제15조(개인정보의 보호조치) 법 제28조 제1항 제4호에 따라 정보통신서비스 제공자등은 개인정보가 안전하게 저장·전송될 수 있도록 보안조치를 해야 한다**[2]**.

개인 고유 식별 정보를 저장할 경우, 암호화 여부를 결정하는 기준이므로 해당 개인정보파일에서 고유 식별 정보를 처리하고 있는지 점검하여 체크한다.

암호화 체크 항목으로 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호 등을 설정할 수 있으며, 암호화 되지 않은 개인정보에 대하여 상용 솔루션 'privacy-i'로 암호화 할 수 있다.

3.위험도 분석 점검 항목

3.1기관 기준 점검

개인정보 파일이 포함되어 있는 개인정보 처리 시스템 환경에 관한 내용으로 기관 전체를 대상으로 한다. 정책기반 항목(5)과, 네트워크 기반항목(6)으로 나누워 개인정보 처리자가 점검 항목을 체크 할 수 있다.

3.1.1 정책 관리자 기반 점검 항목

개인정보 관리 책임자의 자격요건으로 정보 통신망 법 제 27조(개인정보 관리 책임자의 지정)과 정보 통신망 법 시행령 제13조(개인정보관리책임자의 자격요건 등)에서 안내하고 있다**[1]**. 실제 개인정보관리를 담당하는 담당자를 별도로 지정하여 개인정보의 안전한 관리를 위해 필요로 하고 있다. 개인정보보호법 제31조 1항 및 시행령 제32조에 따라 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자(CPO: Chief Privacy Officer)를 지정해야 한다.

아래 표 1. 정책기반 점검 항목은 행정안전부 및 한국인터넷 진흥원에서 제공한"개인정보 위험도 분석 및 해설서"의 내용 중 체크리스트 항목이다.

표 1.정책기반 점검 항목**[2].**

구분	점검항목	Y	N	해당 없음
정책	개인정보 보호를 위한 책임자를 지정하여 운영하고 있습니까?			
	개인정보 보호를 위한 정책 또는 관리계획(침해사고 대응계획 포함)을 수립·운영하고 있습니까?			
	외주인력 보안 관리를 위해 보안서약서 집행, 비밀번호 노출 예방 등 조치를 하고 있습니까?			
	DB 서버에 접속하는 장비(PC, 노트북 등)에서 불법 또는 비인가된 S/W 사용을 방지하고 정품 S/W만 사용하도록 하는 정책을 수립·운영하고 있습니까?			
	DB서버에 접근 가능한 자(내부직원, 위탁인력, 개발자 등) 대상으로 개인정보보호 관련 교육을 연2회 이상 실시하고 있습니까?			

3.1.2 N/W기반 점검항목

개인정보보호법과 정보통신망에서의 접근 통제 지침을 통해 '개인정보 위험도분석' 네트워크 기반 점검 항목을 보장할 수 있다. 침입차단시스템과 침입탐지시스템이 동시에 구현된 침입방지시스템(IPS)과 웹 방화벽 또는 보안 운영체제(Secure OS) 등을 도입함으로써 설비·구축해야 한다. 네트워크 장비에서 제공하는 ACL(Access Control List:접근제어목록)등의 기능을 이용하여 IP주소 제한, 침입차단 기능 구현을 한다**[1].**

표 2. 네트워크 기반 점검 항목**[2].**

구분	점검항목	Y	N	해당 없음
네 트 워크	상시적으로 비인가 IP 주소의 접근을 통제하고 있습니까?			
	상시적으로 불필요한 서비스포트사용을 통제하고 있습니까?			
	상시적으로 불법적인 해킹시도를 방지하고, 이에 대해 모니터링을 실시하고 있습니까?			
	상시적으로 바이러스, 웜 등의 네트워크 유입을 차단하고 있습니까?			
	주기적으로 네트워크 접속에 대한 로그를 관리하고, 분석하고 있습니까?			
	네트워크 장비 및 정보보호시스템의 보안패치 발생시 지체없이 업데이트를 수행하고 있습니까?			

3.2개인정보 처리시스템 기준 점검

3.2.1 DB 및 APPLICATION기반

개인정보보호법에 의해 암호화라는 요건이 명시 되며 DB에 대한 암호화가 필요하다.

웹서버에 개인정보가 노출되지 않도록 기본적인 어플리케이션 설정을 최소화해야 하며, 개인정보보호 노출 점검/차단 시스템 도입이 필요하다.

네트워크 단의 침입방지 시스템이 잘 운용되고 있는 상황이라도 DB에 대한 비인가자의 접근통제는 별도로 실시한다.

표3은 현재 사용되는 DB암호화 기술을 나타낸다.

표3. DB 암호화 기술

종 류	설 명
TDE(Transparent Database Encryption)	SQL Sever2008 자체에서 데이터 파일 및 로그 파일의 암호화를 수행해줌.
TDE + HSM (Hardware Security Module)	암호화키 자체를 암호화 하여 DB서버의 파일에 두고 다른 키는 DB서버 외부의 HSM에 보관.
소프트웨어 기반 DB암호화	암호화 키는 DB서버에 존재하지 않고 별도의 키 저장서버에 있다가 암·복호화 작업이 일어난 동안에만 DB서버의 메모리에 로딩.
하드웨어 기반 DB암호화	암호화키는 암호화 전용 하드웨어에 저장돼 있고, 암.복호화 작업이 필요하면 키가 DB서버로 가는 대신 데이터가 암호화 전용 하드웨어에 가게 됨.

3.2.2 웹기반 점검항목.

웹페이지에 대한 주기적인 개인정보 점검은 실시간으로 필요하다. 웹서버의 게시판, 웹 하드, 블로그 등에 등록되는 개인정보를 차단할 수 있어야 하며, 웹서버에 이미 올라가있는 개인정보를 진단하는 솔루션 설치가 필요하기 때문에 관련 위험도 분석 점검 항목으로 필요하다. '개인정보 위험도 분석'에서 제시하는 항목 또한 이와 같은 내용을 보여주고 있다.

표4. 웹기반 점검 항목**[2].**

구분	점검항목	Y	N	해당 없음
웹	신규 웹 취약점 및 알려진 주요 웹(Web) 취약점 진단/보완을 년1회 이상 실시하거나, 상시적으로 비인가자에 의한 웹서버 접근, 홈페이지 위·변조 등을 자동으로 차단할 수 있는 보호 조치를 하고 있습니까?			
	웹서버 프로그램과 운영체제 보안패치를 제조사 공지 후 지체 없이 수행하고 있습니까?			

Ⅲ. 위험도 분석 점검 도구 개발 연구

개인정보 처리자는 개인정보 위험도 분석 시, 행정안전부 와 한국인터넷 진흥원에서 제공한

‘개인정보 위험도 분석’자료를 바탕으로 기관을 기준으로 한 항목과 개인정보 처리시스템 기준 점검 항목별로 나눌 수 있다. 개인정보 처리자를 위해 개발한 위험도 분석도구는 Microsoft visual studio 2010 개발 툴과 WPF응용프로그램 개발 프레임워크를 이용하여 디자인하였다. C#으로 프로그래밍 작업과 XML기반의 XAML언어를 통해 디자인을 동시에 할 수 있는 장점이 있다.

위험분석 점검 항목의 메인화면은 그림2와 같다. 왼쪽에는 기관, 개인정보 처리시스템 기준으로 해당 목록을 선택 시 “개인위험도 분석”의 체크 항목이 나타난다.

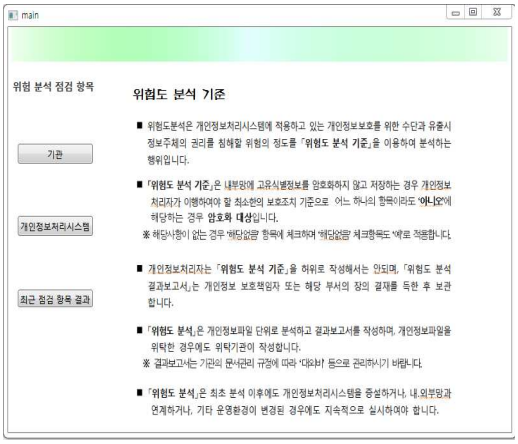

그림 2 실행 시 메인화면

그림 3과 같이 기관항목을 선택하면, 기관기준은 정책기반과, 네트워크 기반으로 설문 항목을 “YES”나 “NO”로 체크를 할 수 있다. 모든 항목에 대해 설문이 끝나면 “NO”로 답한 항목은 최종 결과화면에 나타나게 된다.

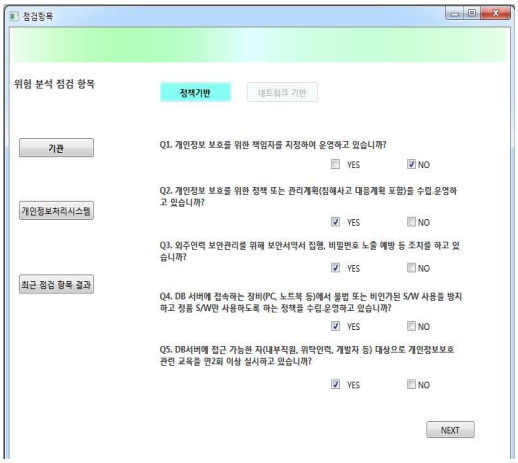

그림 3 체크 항목 리스트

그림 4와 같이 기관기준->정책기반항목 체크->네트워크 기반 항목 체크 한 결과 중 “NO“로 답한 항목에 대한 최종 리포트다. 항목에 대한 이해를 위해 개인정보 보호법에 의한 취지와 해설을 보여줌으로써 개인정보 처리 자는 결과보고서 작성 시 항목에 대한 개인정보를 처리할 수 있는 방법을 파악 및 해결 할 수 있다.

그림 4 점검항목 최종 결과

Ⅳ. 결론

위험 분석 점검을 통해 개인정보 처리시스템에 존재할 수 있는 위험의 정도를 분석하는 기준을 바탕으로 개인정보 암호화 여부 등의 위험도 분석 결과를 작성할 수 있다. 항목 중 어느 한부분이라도 “아니오”에 해당한다면 암호화의 적용여부 및 적용범위를 정할 수 있다. 개인 정보 법 제33조, 시행령 38조, 개인정보 영향 평가에 관한 고시를 참조하면, 2012년 12월 31일까지 암호화 기술의적용 또는 이에 상응하는 조치를 해야 한다. 개인정보 처리 자는 본 논문에서 제시된 위험분석 점검항목 도구를 이용하여 ‘개인정보 위험분석 기준 및 해설서’의 내용인 위험분석 기준에 대한 이해와 암호화 대상을 시간적으로 좀 더 빠르게 파악할 수 있으며, 기관의 위험도 결과보고서를 작성할 수 있다.

향후 암호화가 필요한 개인정보파일에 대하여 개인정보 보호조치 솔루션을 적용할 수 있는 해결방안을 제시하고, 추가로 개인정보보호법 의무 조치사항에 대한 항목을 제시할 수 있는 연구가 필요하다.

참고문헌

[1] 개인정보보호법,“제정 2011.3.29. 법률 제 10465호”.

[2]행정안전부&KISA(한국인터넷진흥원),“개인정보 위험도 분석 기준 및 해설서”, 2010.3.