중소기업을 위한 JSP기반의 기업정보보호포탈

권영범, 박성욱, 이임영
순천향대학교 컴퓨터소프트웨어공학과
e-mail:[clauzevith, swpark, imylee]@sch.ac.kr

Company information security portal based on jsp for small or medium sized business enterprise

Young-Beom Kwon, Sung-Wook Park, Im-Yeong Lee
Dept. of Computer Software Engineering, Soonchunhyang University

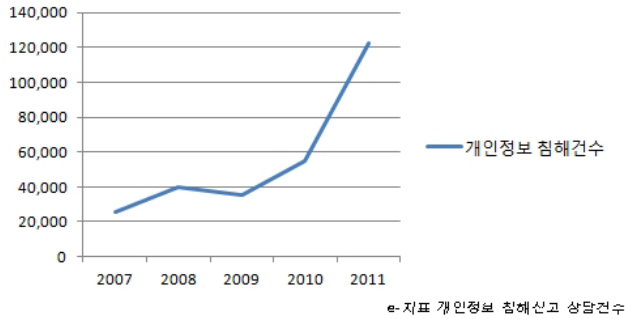
요 약

최근 정보화의 급속한 발전과 함께 다양하고 첨단화된 서비스를 제공하기 위해 개인정보에 대한 의존도 및 활용도가 높아지고 있다. 특히 오늘날 개인정보는 사회의 모든 분야에서 없어선 안 되는 필수재 역할을 하고 있고, 이러한 이유로 개인정보보호는 단순히 개인의 권익에 관한 문제로 국한되지 않고, 기업의 사활을 좌지우지하는 비즈니스 이슈로 대두되고 있다. 따라서 본 논문에서는 보안 컨설팅을 중소기업을 대상으로 제공하여 개인정보를 보다 안전하게 보호하고 중소기업 또한 기업 활동에 지장이 없게 도와줄 수 있도록 설계하고 구현한다.

1. 서론

최근 정보화의 급속한 발전과 함께 다양하고 첨단화된 서비스를 제공하기 위해 개인정보에 대한 의존도 및 활용도가 높아지고 있다. 특히 오늘날 개인정보는 사회의 모든 분야에서 없어선 안 되는 필수적 역할을 하고 있고, 이러한 이유로 개인정보보호는 단순히 개인의 권익에 관한 문제로 국한되지 않고, 기업의 사활을 좌지우지하는 비즈니스 이슈로 대두되고 있다. 이에 따라 최근 들어 개인정보 침해사례가 급증하고 그 심각성이 극대화 되고 있는 등 개인정보보호의 중요성 또한 점차 증대되고 있다. 그러나 그에 반해 개인정보 침해 건수는 2010년 약 50,000건에서 2011년 100,000건을 넘어서고 있다(그림 1).

이렇듯 개인정보의 위협은 나날이 증가하고 있어 기업들의 개인정보에 대한 보안의식이 필요하게 되었다. 하지만 이러한 보안위협을 내재하고 있는 기업 중 중소기업은 대기업 및 공공기관에 비해 자금력 등이 부족하여 정보보호법 관련 인프라를 보유하지 못하고 있으며 구체적인 개인정보보호법의 내용과 기술적 조치내용을 이해하지 못함으로써 기업 활동에 지장을 받을 수 있다. 또한 중소기업은 소규모경제로 인한 효율향상의 어려움과 이에 따른 시장경쟁력의 미흡 등 그 본질적인 면에서 대기업에 비해 상대적으로 열위에 놓이게 되는 경우가 많아 불리하다고 보인다. 본 논문의 구성은 2장 에서는 관련연구에 대한 기술을 하고 3장은 본 논문에 대한 요구사항을 기술한다. 4장은 중소기업을 위한 jsp기반의 기업정보보호포탈을 제안하고 5장에서는 제안한 기업정보보호포탈에 대한 구현을 기술한다. 마지막으로 6장에서 결론을 맺는다.



(그림 1) 개인정보 침해건수

2. 관련 연구

본 연구는 개인정보보호법, 보안 컨설팅을 주제로 한 jsp기반의 연구이므로 개인정보보호법과 보안 컨설팅의 종류에 대해 분석을 하였다.

· 개인정보보호법

개인정보 보호법은 당사자의 동의 없는 개인정보 수집 및 활용하거나 제3자에게 제공하는 것을 금지하는 등 개인정보보호를 강화한 내용을 담아 제정한 법률이다. 이 법은 각종 컴퓨터 범죄와 개인의 사생활 침해 등 정보화 사회의

역기능을 방지하기 위해 1995년 1월 8일부터 시행됐던 법률인 '공공기관의 개인정보보호에 관한 법'을 폐지하고 새로 제정한 법률이다. 2011년 3월 29일 제정되어 같은 해 9월 30일부터 시행되었다. 상대방의 동의 없이 개인정보를 제3자에게 제공하면 5년 이하의 징역이나 5,000만 원 이하의 벌금에 처할 수 있다.

이 법은 개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현하기 위하여 개인정보 처리에 관한 사항을 규정함을 목적으로 한다. 여기서 개인정보란 살아 있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보(해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함함)를 말한다[1].

· 주요 정보통신 기반 시설 취약점 분석·평가

이 유형은 정보통신 기반 보호법에 의거 주요정보통신기반시설로 지정된 정보시스템을 대상으로 하며 전자적 침해행위에 대비해 주요 정보통신 기반 시설을 안정적으로 운용하도록 해 국가의 안전과 국민생활의 안정을 보장함을 목적으로 하여 기반 보호법에서 요구하는 취약점 분석·평가기준에 따라 수행되며, 지난해 수립된 보호대책의 이행평가와 급년도 취약점 분석·평가 시 발견된 취약점에 대해 보호대책을 수립하는 것이다.

· 정보보호 국내외 인증

한국인터넷진흥원에서 인증하는 정보보호 관리체계 인증과 국제표준 인증기관에서 인증하는 정보보호 관리체계를 구축하기 위한 인증인 ISO27001이 있으며 개별적인 정보통신 서비스 또는 전사적 정보보호 관리체계를 대상으로 하여 국내외 정보보호 관리체계의 기준에 따라 기업의 정보보호 활동을 객관적으로 평가하고 인증하여 정보보호 관리체계 수립을 지원하며, 향후 지속적으로 정보보호 관리체계를 유지·발전시킬 수 있도록 지원한다[9].

· 정보보호안전진단

정보통신서비스 제공자가 운영하는 정보통신시설 및 설비를 대상으로 하여 정보통신서비스 제공자가 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위함으로 11개 통제분야에 48개 통제항목을 정의하고 있으며, 4개의 사업자 분류에 따라 의무적으로 적용해야 하는 보호조치 항목을 각각 다르게 정의하고 있으며 이것은 안전진단 대상기업의 범위, 세부 보호조치항목, 수행절차 등 정보통신망법 및 안전진단 관련 세부지침에 정의돼 있다. 정보보호 안전진단 사전 컨설팅은 사업자가 의무적으로 수행해야 하는 보호조치 항목에 대해 정보보호 현황을 검토하고 개선함으로써 안전진단 기준을 준수할 수 있도록 지원한다. 또한, 안전진단 대상기업이 안전진단 보호조치를 이행하고 있는지 여부를 점검한다[10].

· 개인정보 영향평가

개인정보는 현대사회에서 핵심정보역할을 담당하고 있어서 유출시 에 사회 및 경제활동에 치명적인 문제를 야기하므로 개인정보를 취급하는 정보통신서비스 제공자 또는 개인정보이용자의 정보시스템대상으로 하여 개인정보의 취급에 대한 정보보호 활동을 평가하고 보호대책을 마련함으로써 보안을 강화한다[7].

· 웹 애플리케이션 보안취약점 분석

웹 기반으로 개발, 운영되는 기업의 모든 웹 프로그램을 대상으로 하여 웹 애플리케이션 개발상의 오류로 인해 발생할 수 있는 보안 사고를 미연에 방지를 목적으로 웹 애플리케이션에 대한 보안 취약점을 점검하고 사전에 이를 제거함으로써 내·외부의 악의적인 공격으로부터 시스템을 보호해 안전하고 편리한 웹 서비스를 제공할 수 있도록 한다. 웹 애플리케이션의 보안을 강화하기 위해서는 설계단계부터 구현, 테스트, 운영단계 까지 보안을 고려한 검토가 필요하나 최소한 테스트단계에서 보안 취약점 분석 작업을 실시해야 한다[8].

· 모의해킹

인터넷에 연결된 모든 정보 시스템을 대상으로 하여 비인가된 사용자가 정보 시스템의 임의 접근 및 정보의 유출, 파괴의 가능성을 점검하기 위함으로 인터넷기반 서비스의 급속한 확산과 함께 악의적인 목적의 사용자에 의해 중요 정보자산에 대한 침해사고가 급속히 증가하고 있어 이러한 보안 사고를 방지하기위한 보호대책이 수립·이행돼야 하는데, 보호대책의 안전성을 테스트하기 위한 목적으로 모의해킹을 수행하게 되며 모의해킹 대상은 시스템 취약점 분석 대상에 포함되지 않는 부분까지 확대해 실증 보안점검을 수행해야 한다. 특히, 침입위협의 발생가능성을 검증하기 위해 가장 위험성이 높은 최근 침입유형을 우선적으로 실시하게 된다[7].

· 시스템 취약점 분석

시스템 취약점 분석은 기관 및 기업에 설치·운영되는 서버, 네트워크 및 보안 시스템을 대상으로 하여 비 인가된 사용자가 정보 시스템의 취약성을 이용해 시스템에 임의의 접근을 차단하기 위함으로, 서버, 네트워크장비, 보안시스템, PC, 응용프로그램 등 모든 정보 시스템에 대해 주기적으로 이루어지며, 새로운 취약점이 발견된 경우 즉각적인 조치를 하게 된다.시스템 취약점 분석 방법에는 자동화된 스캐닝 도구를 사용해 원격으로 점검하는 방법(네트워크 기반 취약점 분석)과 체크리스트 기반으로 로컬에서 점검하는 방법(시스템 취약점 분석)으로 구분할 수 있다[8].

(그림 2) 보안 컨설팅 프로세스

3. 요구사항

기업 내에 다양한 보안요구사항에 만족하기 위한 보안 컨설팅 프로세스로는 환경 분석, 현황분석, 정책수립 및 솔루션 도입, 보안아키텍처 설계, 지속적 관리가 있다.

• 환경 분석

기업의 비즈니스 관점에서 실질적인 개인정보 유형 및 내용을 식별, 식별된 개인정보의 가치 및 민감도를 평가한다.

• 현황분석

기업의 기밀의 다양한 위협에 대해서 현재 시스템의 취약성을 인식 및 예상되는 손실을 분석한다.

• 정책 수립 및 솔루션 도입

조직의 전체 수준에서 운영수준까지 계층구조별로 달성해야 하는 보안 목적을 달성하기 위한 정책 규정한다.

• 보안아키텍처 설계

해당 기업에 맞는 보안 정책, 지침/규정, 조직/ 프로세스 등 보안 전 영역으로 맞춤형 보안 아키텍처 설계하고, 대내외 동향을 분석하여 아키텍처에 반영한다.

• 지속적 관리

구축된 시스템이 효과적으로 운용되고 있는지 점검하는 활동, 운영 상태를 파악하여 문제점을 조사해서 시스템을 보완한다.

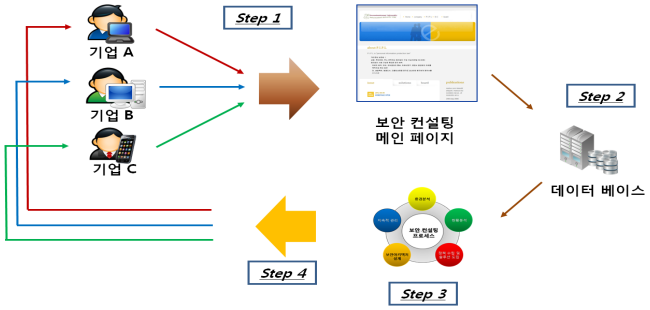
4. 제안방식

본 연구에서는 보안 컨설팅 요청 기업에게 기업의 보안 실태를 제공받아 이에 해당하는 보안 컨설팅은 실시할 수 수 있도록 설계하였다(그림 3).

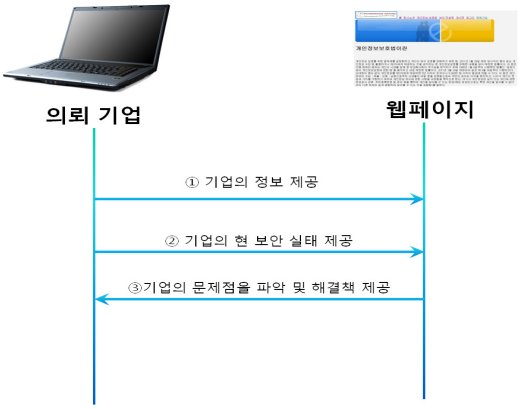
4.1 시나리오

Step 1 : 업체가 웹사이트를 이용하여 자사의 정보를 입력하여 컨설팅을 의뢰한다.

Step 2 : 웹페이지에서 기입되는 자료를 데이터베이스에 연동하여 사례를 수집한다.



(그림 3) 아이템 시나리오



(그림 4) 웹을 이용한 컨설팅 시나리오

Step 3 :요청업체의 현황을 조사 및 분석을 하여 그에 맞는 보안 컨설팅 프로세스를 통하여 맞춤형 컨설팅을 수립한다.

Step 4 : 프로세스를 통한 컨설팅을 업체에게 제공하여 업체가 만족할 수 있는 서비스를 제공한다.

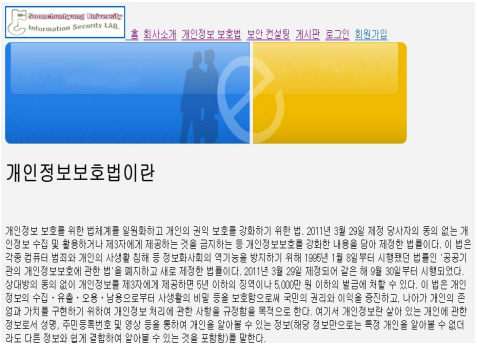
4.2 보안 컨설팅 방식

본 연구는 회원가입을 통하여 사용자의 정보를 입력받고 그에 해당하는 컨설팅 정보를 제공한다.
컨설팅 정보를 제안하기 위하여 회사의 상시 근로자수, 종업원 의 수, 매출액, 및 개인정보의 보유량과 수집항목 등의 정보를 요구하게 되며 이정보에 따라 현재 기업에 필요한 보안 컨설팅을 제공하며 지속적으로 사례를 저장하여 컨설팅 정보를 업그레이드 하게 된다(그림 4).

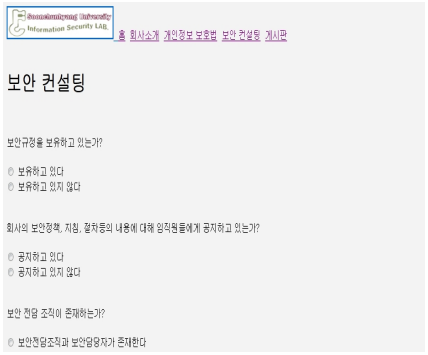
Step 1 : 의뢰기업이 현 기업의 인원 및 기업의 현재 등록되어 있는 종류 등 기타 정보를 제공

Step 2 : 웹페이지에서 현 기업의 보안 실태를 제공함

Step 3 : 현 기업의 보안실태를 파악하여 의뢰한 기업에게 맞는 보안 컨설팅을 하게 되고 지속적으로 데이터베이스에 저장함으로 사례를 저장하게 됨



(그림 5) 웹페이지 현황



(그림 6) 보안 컨설팅 현황

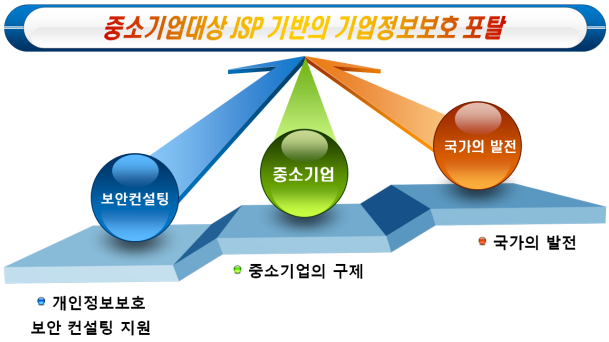
5. 제안방식 구현

본 연구는 웹페이지를 이용하여 보안 컨설팅이 필요한 기업에게 컨설팅을 제공하여 줌으로써 해당 기업이 개인정보보호법에서 보다 안전하고 합법적으로 기업 활동을 지속할 수 있게 도와줄 수 있는 연구로써 해당 웹페이지에서 회원가입을 통하여 기업의 근로자수, 매출액, 개인정보의 보유량, 수집항목의 종류, 업종 등의 정보를 넘겨주게 되고 이를 기반으로 웹페이지의 보안 컨설팅 과정을 통하여 현 기업의 보안 관련 업무실태를 넘겨줄 수 있게 된다(그림 5).

웹페이지에서는 이러한 보안관련 업무 실태 및 현 기업의 상황을 제공받아 이를 토대로 기업에게 지금 기업이 시행하여야 하는 보안 컨설팅을 해줄 수 있게 되고 이를 데이터베이스에 지속적으로 저장하여 사례를 수집하여 현재 제공되고 있는 보안컨설팅을 보다 더 효과적으로 수행할 수 있도록 업데이트하게 된다(그림 6).

6. 결론 및 향후 연구 방향

본 연구는 2012년 4월에 시행된 개인정보보호법을 기반으로 한 연구이다. 따라서 아직 기업들에게 생소하며 대처 또한 미흡하다는 보도가 2012년 7월에 발표된 바 있다. 그리고 기업들의 인식이 20%수준에 그치고 있다는 보도도 2012년 9월 20일자 뉴스로 발표되었다. 그러므로 본 연구를 통한 기대효과에는 개인정보보호법을 장차 중소



(그림 7) 기대효과

기업들이 인식하기 쉬우며 대처를 보다 정확하게 할 수 있게 도와줄 수 있을 것이며 중소기업의 정보보호 관리체계 확립 및 정보보호 대외기준 인증 획득 및 유지를 위한 기반 마련 또한 본 연구의 결과로 이끌어 낼 수 있을 것이다. 그리고 이를 통해 국가의 개인정보보호에 앞장 설 수 있으며 안전한 정보사회를 만들 수 있을 것이다.

본 연구는 현재 연구하고 있는 분야가 개인정보보호이기 때문에 현재 기업에서 개발한 솔루션들의 특징 및 장점에 대한 정보와 개인정보가 주로 사용되고 있는 기업이나 분야에 대한 기술적 정보에 대한 도움이 있으며 현재 본 연구의 검증과 테스트 보조 및 향후 업그레이드를 위한 여러 가지 개선방안 조언 과 본 아이템의 광고 등의 역할이 될 수 있겠다.

참고문헌

[1] 방송통신위원회, "정보통신망 이용촉진 및 정보보호 등에 관한 법률", 시행령, 시행규칙, 2011.

[2] 박은엽, 최진원, 조태희 "개인정보보호관리체계 인증제도 구축 사례 연구", 2011. 8.

[3] "국내외 개인정보보호법 동향과 기업의 대응전략", 2011

[4] 김동진, 조성제, "국가DB기반의 국내외 보안 취약점 관리체계 분석", 2011. 11. 19.

[5] 한국정보화진흥원. "정보화 법 제도 정비". 2009.4.

[6] 중소기업기술정보진흥원. "보안컨설턴트 실무 가이드북". 2007

[7] "보안컨설팅의 종류와 적용방안" 2007.02

[8] "정보보안 컨설팅" 2011.05

[9] "SW사업 대가산정 가이드" 2012.02.24

[10] "KISA 정보보호 안전진단"