한국항행학회 논문지 제 15 권 제 6 호 2011년 12월

정보보호관리체계를 통한 기업 및 정부 정보보안 강화 방안에 관한 연구

A Study on Enterprise and Government Information Security Enhancement with Information Security Management System

박청수*, 이동범*, 곽진*

Chung-Soo Park*, Dong-Bum Lee*, and Jin Kwak*

요 약

IT 기술이 발전함에 따라 생활 자체가 지식 혹은 정보 기반 체제로 변화되어 가고 있다. 하지만 IT 기술의 발전 이면에는 사이버 공격 기술을 향상시키고 있으며, 이에 따라 DDoS 대란 등의 사이버 테러가 빈번히 발생하여 주요 자료가 유출되고 있다. 또한 다양한 공격 경로를 통해 정보시스템으로 유입된 악성코드로 인해 기업의 업무 손실 및 정보 자산에 대한 피해가 증가하고 있다. 이러한 환경에서 조직 및 사용자가 보존해야 할 정보 자산을 관리적, 기술적, 물리적 체계를 수립하는 정보보호관리체계를 기반으로 지속적인 점검을 수행하여 조직 내의 위기관리 프로세스가 구축되어야 한다. 또한 제도 및 프로세스의 수립 외에도 악의적인 악성코드가 내부로 유입되는 위협으로부터 내부 자산을 보호하기 위해 정보보호제품을 도입하여야 한다. 따라서 본 논문에서는 정보보호관리체계 및 정보보호제품의 도입 방안을 통해 기업 및 정부 정보보안을 강화하는 방안에 대하여 제안하고자 한다.

Abstract

According to the development of IT technology, life itself is becoming the change to Knowledge-based systems or information-based systems. However, the development of IT technology, the cyber attack techniques are improving. And DDoS a crisis occurs frequently, such as cyber terrorism has become a major data leakage. In addition, the various paths of attack from malicious code entering information in the system to work for your company for loss and damage to information assets is increasing. In this environment, the need to preserve the organization and users of information assets to perform ongoing inspections risk management processes within the organization should be established. Processes and managerial, technical, and physical systems by establishing an information security management system should be based. Also, we should be introduced information security product for protecting internal assets from the threat of malicious code incoming to inside except system and process establishment. Therefore we proposed enterprise and government information security enhancement scheme through the introduction of information security management system and information security product in this paper.

Key words : Enterprise Security, Information Security Management System, Information Product, Risk Management

* 순천향대학교(Department of Information Security Engineering, Soonchunhyang University)
· 제1저자 (First Author) : 박청수 · 교신저자(Corresponding Author) : 곽진
· 투고일자 : 2011년 11월 25일
· 심사(수정)일자 : 2011년 11월 25일 (수정일자 : 2011년 12월 21일)
· 게재일자 : 2011년 12월 30일

Ⅰ. 서 론

작년 7.7 DDoS 대란 및 올해 3.3 DDoS 대란이 발생함에 따라 사용자가 인지하지 못한 상황에서 악성코드가 사용자의 PC에 유입되어 하드 디스크에 저장된 정보를 파괴하고 디스크에 저장된 정보를 유출하여 사회적으로 큰 이슈가 되고 있다. 사용자뿐만 아니라 기업에서도 조직원의 PC에 저장된 중요한 정보자산들이 유출되고 조직원의 개인정보가 거래되며, 기업 내부망으로 악성코드가 유입되어 주요 정보를 파괴하거나 유출하는 사례가 급증하고 있다. 이러한 이유로 기업들은 정보보안을 강화하고 있으며, 정보유출을 통제하고 외부로부터 악성코드가 유입되지 못하도록 각종 보안시스템을 도입하고 보안을 강화하기 위한 프로세스를 구축하고 있다[5].

기업이 도입하고 있는 정보보호관리와 관련된 프로세스 중 가장 핵심이 되는 제도가 정보보호관리체계(ISMS : Information Security Management System)이다. ISMS는 조직이 보존해야 할 정보 자산의 기밀성, 무결성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립, 문서화하여 지속적으로 관리하고 운영하는 체계이기 때문에 기업의 정보보호 관리에 대한 표준적 모델 및 기준을 제시하여 기업의 ISMS 구축 및 운영을 촉진하고 정보보호 활동에 대한 프로세스 개선을 통하여 기업의 주요 정보 자산의 유출 및 피해를 사전에 예방하고 대처할 수 있도록 하고 있다. 따라서 기업에서는 ISMS 인증제도에 따라 컨설팅을 받아 ISMS를 구축하고 조직원들이 준수할 수 있도록 프로세스를 정의하고 있다.

또한 공공기관에 대한 사이버 침해사고가 지속적으로 증가하고 있어 국민들이 사이버 위협에 노출되는 등 전자정부 서비스의 정보보호에 대한 요구가 점차 늘어남에 따라 정부 조직 및 유관 기관의 정보 자산을 체계적으로 보호하기 위한 프로세스를 수립하는 전자정부 정보보호관리체계(G-ISMS : Government-Information Security Management System) 인증에 대한 요구가 점차 증가되고 있다. 제도 및 프로세스를 정의하는 것도 중요하지만 정보 자산을 보호하는 가장 기본적 방안으로 정보보호제품을 도입하여 내부망을 외부 악성코드로부터 보호하고 조직원의 PC에 악성코드가 유입될 경우 이를 탐지하고 삭제할 수 있어야 한다. 특히 최근 이슈가 되고 있는 논리적 망분리 제품은 내부망과 외부망을 완벽히 분리하여 내부망으로 구분된 PC에서는 인터넷을 사용할 수 없도록 하고 있다.

따라서 본 논문에서는 정보보호관리체계에서 정보보호제품과 관련된 통제항목을 도출하고 기업 및 정부에서 정보보안을 실현하기 위한 조치 방안에 대하여 제안하고자 한다.

Ⅱ. 정보보호관리체계 개념

기업은 조직이 가지고 있는 정보 자산을 보호하기 위하여, ISMS 수립·운영을 위한 5단계 관리과정(정보보호정책수립, ISMS 범위설정, 위험관리, 구현, 사후관리), 문서화, 정보보호대책에 대하여 조직의 특성 및 환경에 부합되도록 적절하게 수립·구현하여, 체계적으로 관리·유지하고 이행하는지를 평가하는 제도를 도입하고 있다[2,6,11].

2-1 ISMS 인증

ISMS 인증 제도는 2001년 (구)정보통신부가 '정보통신망이용촉진및정보보호등에관한법률'을 개정하여 공표함으로써 제47조에 근거를 두고 추진하였다. 즉 ISMS는 조직이 보존해야 할 정보자산의 기밀성·무결성·가용성을 실현하기 위한 절차와 과정을 체계적으로 수립, 문서화하여 지속적으로 관리하고 운영하는 체계이다[7]. 이러한 인증 제도를 통하여 단편적이고 일회적이었던 조직의 정보보호활동을 체계적이고 지속적인 관리가 가능하게 함으로써 전사적으로 균형이 잡힌 정보보호활동을 할 수 있게 된다. 특히 기업의 정보보호 관리에 대한 표준적 모델 및 기준을 제시하여 기업의 ISMS의 구축·운영을 촉진하고 정보보호 활동에 대한 프로세스의 개선을 통하여 기업의 주요 정보자산의 유출 및 피해를 사전에 예방하고 대처할 수 있도록 하는데 목적을 두고 있다[4,10]. ISMS를 구축하기 위해서는 ISMS 범위를 결정하고 해당 범위 내의 정보 자산을 식별 및 분류하여 목록

을 작성해야 한다. 목록 작성은 기존의 자산 관리체계를 활용하는 것이 효율적이며, 크게 유형 자산과 무형 자산으로 분류될 수 있다. 자산을 식별했을 경우 자산의 유출, 위·변조, 사용·미사용에 따라 업무에 미치는 영향도를 고려하여 기밀성, 무결성, 가용성을 기반으로 자산 가치를 평가한다. 자산 정보가 유출 또는 외부에 공개되었을 경우 미치는 업무 영향도가 클 경우 기밀성 측면의 가치가 높이 평가된다. 또한 자산 정보가 위·변조 되었을 경우 미치는 업무 영향도가 클 경우 무결성 측면의 가치가 높이 평가되며, 정보 자산의 사용·미사용으로 미치는 업무 영향도가 클 경우 가용성 측면의 가치가 높아진다. 이러한 절차를 통해 평가된 자산 정보의 가치가 높을수록 ISMS 인증을 필요로 하게 된다. 그 절차는 인증 취득을 원하는 기업이 인증심사를 신청하고 평가 받으며, 인증서를 발급 받기까지는 약 3개월의 시간이 소요된다. 사후관리 단계까지 통과했을 경우 인증서가 발급되며 기업의 ISMS 제도가 검증되었음을 보증 받는다.

따라서 기업은 조직이 가지고 있는 정보 자산을 보호하기 위하여 ISMS 수립·운영을 위한 5단계 관리과정(정보보호정책수립, ISMS 범위설정, 위험관리, 구현, 사후관리), 문서화, 정보보호대책에 대하여 조직의 특성 및 환경에 부합되도록 적절하게 수립·구현하여, 체계적으로 관리·유지하고 이행하는지를 평가하는 제도를 도입하고 있다[6]. ISMS의 인증 절차 준비단계, 심사단계, 인증단계, 사후관리 단계로 구성되며, 내용은 표 1과 같다.

표 1. ISMS 인증 절차
Table 2. ISMS Certification Process.

인증 절차	내용
준비 단계	ISMS 구축, 인증신청, 사전심사, 계약, 수수료 납부 등 인증을 준비하는 단계
심사 단계	심사팀을 구성하여 서면심사 및 기술 심사를 수행하고, 그 심사결과로 발견된 결함사항을 신청기관이 보완조치(보완조치기간 : 1개월)하여 확인하는 단계
인증 단계	심사팀의 인증심사결과를 인증위원회가 심의·의결하여 인증서를 교부하는 단계
사후관리 단계	인증 취득기관이 ISMS를 지속적으로 운영·유지하는지를 점검

2-2 G-ISMS 인증

G-ISMS 인증은 기관이 수립하고 구축한 종합적인 ISMS를 제 3자가 객관적으로 심사하여 인증을 부여하는 제도이다[9]. 행정기관 등의 조직 및 서비스의 특성에 적합하게 수립된 종합적인 ISMS를 의미한다. G-ISMS 인증은 역할과 책임에 따라 표 2와 같이 정책기관, 인증위원회, 인증기관, 신청기관으로 구분한다. 정책기관과 인증위원회는 행정안전부가 담당하고, 인증기관의 역할은 한국인터넷진흥원이 수행하고 있다.

G-ISMS 인증을 취득했을 경우 침해사고에 대한 능동적인 예방체계 구축을 통해 전자정부 서비스에 대한 피해를 최소화 할 수 있으며, 종합적인(관리·기술·물리) 정보보호 대책을 수립하여 개인 및 국가 정보 유출을 사전에 예방할 수 있다. 또한 정보보호 관련 법적 요구사항에 대하여 체계적으로 대응하고, 지속적인 정보보호 관리를 통하여 새로운 보안위협에 대하여 효과적으로 대응할 수 있다[3,14,15].

G-ISMS는 전자정부법(제24조 및 제56조), 정보통신망 이용촉진 및 정보보호 등에 관한 법률(제47조), 전자정부 정보보호관리체계 인증 등에 관한 지침에 의거하여 시행되고 있다. 현재까지 22개 기관 및 서비스가 G-ISMS 인증을 획득하였고 15개 기관이 심사 완료 또는 대기 중이며, 행정안전부는 2010년 37개 기관 및 서비스에 이어 2011년에도 약 40개 기관에 대해 인증 컨설팅을 진행하고 있다.

표 2. G-ISMS 구성 조직
Table 2. G-ISMS Configuration Organization.

수행 기관	업무
정책기관 (행정 안전부)	G-ISMS 인증 제도의 수립, 인증기관의 지정 및 감독, 인증위원회 구성 및 관리, 인증심사원 임명, 인증관련 예산의 확보 및 출연, 그 밖의 인증에 필요한 정책의 수립 등 수행
인증 위원회	인증기관에서 제출한 인증심사결과보고서의 심의·승인, 인증기관 자격 심의·인정, 인증심사원 자격 심의·인정, 기타 행정안전부 장관이 위임한 업무를 수행
인증기관 (KISA)	G-ISMS 인증심사, 인증서 발급 및 관리, 인증심사원 교육, 인증상담 및 기술자문, 그 밖의 인증업무에 필요한 연구사업 등을 수행
신청기관	G-ISMS 인증을 신청한 기관

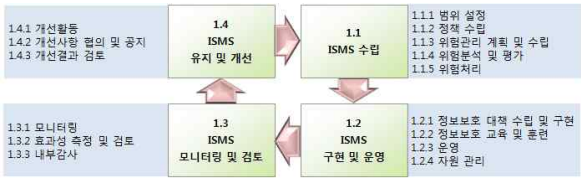

그림 1. G-ISMS 수립 및 관리과정
Fig.1.G-ISMS Establishment and Management Process.

인증기준은 인증심사를 통과하기 위하여 요구되는 조건으로 필수사항인 수립 및 관리과정, 문서화 요구사항과 선택 사항인 12개 분야의 정보보호대책 통제사항으로 구성되어 있다.

수립 및 관리과정은 그림 1과 같이 수립(Plan), 구현 및 운영(Do), 모니터링 및 검토(Check) 유지 및 개선(Act)의 4단계 관리과정으로 운영되고 있다. 조직의 정보보호 환경과 그 위험은 지속적으로 변화하고 있으므로 관리과정은 일회적인 단계가 아니라 지속적으로 유지, 관리되는 순환 주기의 형태를 가지고 있다.

문서화 요구사항은 G-ISMS 수립 및 운영의 근거를 위해 표 3과 같이 이해하기 쉽게 작성되고 확인하기 쉽게 관리되어야 한다. 정보보호대책의 수립 여부를 점검하기 위한 12개 분야의 156개 통제항목은 ISO 27001과 같이 11개 분야에 개인정보보호 수준진단을 포함하여 구성되어 있다.

표 3. G-ISMS 문서화 요구사항
Table 3. G-ISMS Documentation Requirements.

항목	내용
문서화 요구사항	G-ISMS 수립 및 관리에 대한 내용이 문서화되어야 하며, 문서의 내용은 실제 업무를 반영하여 업무와의 일관성을 유지하고 ISMS 정책, 책임자의 결정, 위험관리 결과 등에 따라 ISMS 활동을 추적할 수 있어야 함
문서의 통제	문서의 승인, 검토, 개정 상태의 식별, 관련자 배포, 폐기 및 폐기 문서의 표시 등의 통제 절차를 수립하여 문서 및 문서목록을 관리하여야 함
기록의 통제	기록의 식별, 보관, 보호, 검색, 보유기간, 폐기에 관한 통제 절차를 수립하여 관리하여야 하며 기록은 읽기 쉽고 식별 가능하며 관련 활동을 추적할 수 있어야 함

이러한 G-ISMS 인증 제도는 정보보호 관련 법적 요구사항에 대하여 체계적으로 대응하고, 지속적인 정보보호 관리를 통하여 새로운 보안위협에 대하여 효과적으로 대응할 수 있다. 이에 따라 정부 및 행정기관에서는 G-ISMS 도입에 대한 요구가 점차 증가하고 있다.

Ⅲ. 정보보호제품 도입을 통한 정보보안 강화 방안

조직은 조직의 정보 자산을 보호하고 조직원 및 사용자의 개인정보의 유출을 방지하기 위하여 정보보호관리체계를 도입하여 조직의 정보보안을 강화하고 있다[1]. 이러한 정보보호관리체계가 실제로 구축되기 위해서는 조직원 및 사용자 측면의 보안부터 내부망 전체의 보안을 제공할 수 있는 백신, 방화벽, 망분리 제품군과 같은 정보보호제품을 사용하여 정보보안을 실현해야 한다.

3-1 백신 제품군

조직의 경우 1대의 PC가 악성코드에 감염될 경우 네트워크를 통하여 전사적으로 전파되어 대규모 피해를 일으킬 수 있어 해킹 예방에 대한 요구가 급증하고 있다. 이러한 요구를 만족하는 가장 기본적인 보호 조치가 백신이다. 백신은 조직이나 개인 사용자 모두에게 기본적으로 설치해야 될 제품군으로 외부로부터 유입된 악성코드를 탐지하고 삭제할 뿐만 아니라 실시간으로 감염 여부를 알려주기 때문에 기본적으로 조직원 및 사용자 모두가 설치해야 한다. 특히 DDoS 대란이 발생했을 경우에도 좀비 PC를 생성하는 악성코드들을 탐지하고 분석하는 역할을 하였으며, 분석된 내용을 기반으로 백신을 개발하는 업체에서 전용 백신을 배포하여 좀비 PC를 치료하는데 중요한 역할을 하였다. 또한 최근 개발되는 백신은 악성코드 탐지 및 치료뿐만 아니라 웹 보안, 메일 보안, USB 드라이브 검사 등 다양한 기능을 제공하고 있어 정보 유출 및 악성코드 유입으로부터 보호되고 있다. 웹 보안 기능을 통해서 유해 사이트에 대한 접근을 차단하며, 유해 사이트로부터 파일 다운로드를 차단한다. 메일 보안 기능을 통해서는 메일을 통해

내부로 유입하는 악성코드를 차단하며, USB 드라이브를 검사하는 기능을 활용하여 매체를 통해 악성코드가 전파되는 것을 방지하고 있어 정보보안에 큰 역할을 하고 있으므로 조직의 정보보안에 반드시 필요한 제품이다.

3-2 방화벽 제품군

방화벽은 조직에서 정보보안을 위하여 필수적으로 도입해야 되는 가장 대표적인 정보보호시스템이다. 외부망에서 내부망으로 패킷이 유입될 때 방화벽 정책에 따라 허용·차단 등의 정책을 패킷에 명령하여 내부로 유입 가능한지 여부를 판단하는 시스템으로 가장 기본적으로 필요한 시스템이다. 또한 내부망에서 외부망으로 전송하는 패킷에 대해서도 검사하여 허용된 패킷만 외부로 유출이 가능하도록 하는 시스템이다. 블랙 리스트와 화이트 리스트 기반의 필터링 기능으로 패킷을 허용·차단하고 기본적으로 제공하는 NAT 기능을 통해 유연한 망 호환성을 제공하고 있다. 방화벽은 네트워크 보안 제품 중 하나로 악성코드를 탐지하는 침입방지시스템(IPS : Intrusion Prevention System), 네트워크에 대한 접근 통제 기능을 제공하는 네트워크접근제어시스템, 인터넷망을 전용선과 동일한 안전성을 제공하는 사설망으로 사용하는 가상사설망(VPN : Virtual Private Network) 등의 기능이 접목되어 통합보안시스템(UTM : Unified Threat Management)으로 운영되기도 한다.

3-3 망분리 제품군

망분리 방식은 다음과 같이 물리적 망분리, 논리적 망분리로 구분할 수 있다.

물리적 망분리는 물리적으로 2대의 PC를 가지고 사용하는 방식을 의미한다. 1대의 PC는 업무 서버에만 접근할 수 있으며 인트라넷 및 내부망에서만 할 수 있는 업무를 수행하는데 사용하고, 다른 1대의 PC는 인터넷을 통하여 업무를 수행하는데 사용하는 독립된 2대의 PC로 망분리를 구현한 방식이다. 물리적 망분리 방식을 사용할 경우 분리가 명확하게 이루어지기 때문에 가장 확실한 망분리를 구현할 수 있으나 PC를 도입하는 비용이 2배로 증가하고 자료 이동 및 사용 편의성 측면에서 비효율적이기 때문에 이를 보완할 수 있는 논리적 망분리 방식이 이슈가 되고 있다.

논리적 망분리 방식은 SBC(Server Based Computing) 방식과 데스크탑 가상화 방식으로 구분할 수 있다. SBC 방식은 서버에 사용자가 사용할 응용프로그램들을 모두 구축해 놓고 사용자들이 자신의 터미널을 통해 서버에 접속하여 업무를 수행하는 방식이다. 데스크탑 가상화는 사용자의 PC에서 가상화 기술을 이용한 망분리가 이루어지며, 모든 작업을 사용자의 PC에서 할 수 있는 방식이다.

(1) 2대의 PC를 사용한 물리적 망분리 방식

물리적 망분리 방식 중 PC를 2대 사용하여 망을 분리한 경우 1대는 업무 영역만 접근 가능하며, 다른 1대는 인터넷용으로 사용하게 된다. 그러나 PC가 물리적으로 분리되어 있기 때문에 자료 이동에 대한 불편함이 발생하고 PC 도입 및 별도의 네트워크 구축 비용이 증가한다는 단점이 있다.

(2) 망분리 전환 장치를 이용한 물리적 망분리 방식

망분리 전환 장치를 이용한 물리적 망분리 방식은 1대의 PC에 네트워크 카드와 하드 디스크와 랜카드를 복수개 설치하고 망 설치를 별도로 구성하여 물리적 망분리를 구현한 방식이다. 2대 PC 이용과 같은 수준의 보안성을 제공하며, PC는 물리적으로 1대를 사용하지만 별도의 네트워크 카드와 하드 디스크 비용이 발생하며, 망 전환 시 재부팅을 해야 되기 때문에 재부팅 시간이 소비되고 비효율적이라는 단점이 있다.

(3) SBC 논리적 망분리 방식

SBC 망분리 방식은 사용자들이 사용할 응용프로그램이나 하드웨어 자원은 중앙 서버에서 사용하고, 사용자는 서버에 접속할 터미널, 키보드, 마우스, 모니터와 같이 입·출력 장치만을 가지고 업무를 수행하는 방식이다. 또한, SBC 방식의 목표는 어느 장소에서든, 어떤 디바이스를 이용해서든, 어떤 네트워크를 통해서든, 어떤 환경에서도 응용프로그램을 이용할 수 있도록 하는 것이다. SBC 방식을 사용할 경우 응용프로그램에 대한 유지관리 비용이 감소하고 관리가 용이해지며 사용자의 터미널이 바이러스에 감염

되어도 사용자의 데이터가 서버에 남아 있기 때문에 정보 자산에 대한 안전성을 제공할 수 있는 방식이다. 하지만 서버 구축비용이 발생하고 서버에서 제공하고 있는 응용프로그램만 사용할 수 있기 때문에 업무 확장성이 감소할 수 있는 단점이 있다.

(4) 데스크탑 논리적 망분리 방식

그림 2와 같이 데스크탑 망분리 방식은 사용자의 PC에서 가상화 공간을 구축하여 망을 분리하는 방식이다. 가상화 공간을 업무 영역으로 사용할 것인지, 인터넷 영역으로 사용할 것인지 선택적으로 사용할 수 있는 방식이다. 데스크탑 방식은 가상화 범위에 따라 커널 가상화와 응용프로그램 가상화로 구분할 수 있으며, 별도의 도입 비용 없이 구축이 가능하고 간편하게 사용할 수 있다. 하지만 사용자의 PC가 바이러스에 감염되어 저장된 데이터가 손실 될 경우 정보 자산에 대한 안전성을 제공할 수 없다는 단점이 있다.

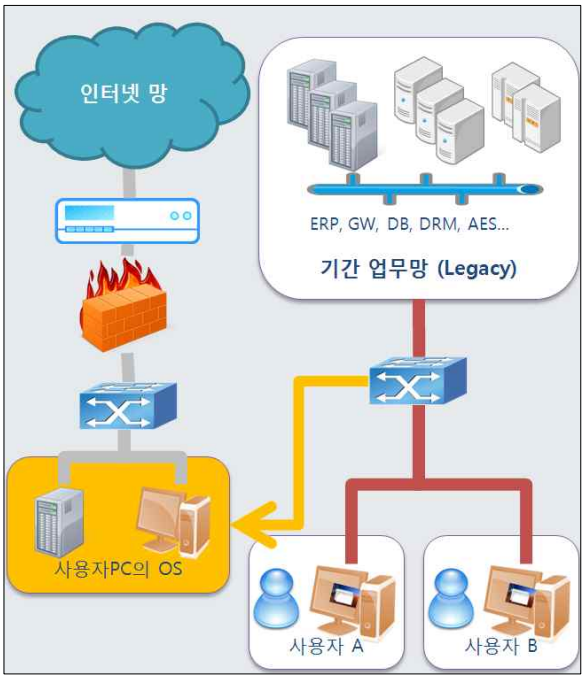

그림 2. 데스크탑 논리적 망분리 방식
Fig.2. Desktop Logical Network Separation Method.

Ⅳ. 정보보호관리체계를 이용한 기업 및 정부 정보보안 강화 방안

기업 및 정부의 정보 자산의 가치가 점차 높아짐에 따라 정보를 보호하고 정보통신 인프라를 강화하는 방안이 강구되고 있다. 기업 및 정부의 정보보안을 강화하기 위해서는 다음과 같이 ISMS, G-ISMS에 따라 프로세스를 수립하여 관리하고 유지하는 것이 중요하다.

정보보호관리체계 인증심사 기준은 필수사항인 '관리과정 통제항목', '문서화 요구사항 통제항목', 선택사항인 '정보보호관리 통제항목 항목'으로 구성되어 있다. 인증 신청 조직은 관리과정과 문서화 요구사항인 항목은 반드시 이행하여야 하며, 선택사항인 정보보호대책을 위한 정보보호관리 통제항목은 해당되는 항목을 선택하면 된다. 이렇게 선택된 심사기준의 요구사항을 충족하고 기업에 정보보호제품을 도입한다면 기업의 정보보안을 강화할 수 있다. 또한 정보보호 정책 수립 및 관리가 필요하며, ① 정보보호정책 수립, ② 인증 범위 설정, ③ 위험관리, ④ 구현, ⑤ 사후관리 등 5단계의 과정을 거쳐 수립·운영된다.

새로운 위협요소 및 취약성 발견 등 지속적으로 변화하는 IT 및 인터넷 환경에서 내부의 주요 정보자산을 효과적으로 보호하고 관리하기 위해서는 주기적인 위험분석을 통한 지속적인 사후관리가 필요하다. 이 과정은 일회성 단계가 아니라, 지속적으로 유지 관리되어야 하는 순환 주기의 형태를 가진다. 특히 사후관리를 통해 실질적으로 운영되고 있는 정보보호관리체계의 적합성을 판단하고 부족한 부분에 대한 갱신이 이루어져야 한다. 정보보호 관리과정에 대한 심사기준은 각 단계에서 통제항목을 만족하도록 정보보호 정책을 수립하고 관리되어야 한다. 또한 ISMS 수립 및 운영의 근거는 정책, 지침, 절차 등을 수립하고, 문서화하여 관리되어야 한다. 마지막으로 앞서 설명한 것과 같이 정보보호제품 중 가장 대표적인 정보보호제품에 해당하는 통제항목을 ISO27001, ISMS, G-ISMS에서 도출하고, 도출된 통제항목을 실현할 수 있는 조치 방안을 표 4와 같이 분석 및 제안

표 4. 정보보호 대책 통제사항 및 조치방안
Table 4. Information Security Measure Control Item and Action Method해야 한다.

구분	정보보호 대책 통제사항			조치방안
	ISO 27001	G-ISMS	ISMS	
백신	A.10.4.1 악성코드에 대한 통제	6.4.1 악성코드 통제	11.5 악성 소프트웨어 통제	• 악성코드 방지에 대한 사용자 교육, 복구 및 보고에 대한 절차 등 유해 소프트웨어를 예방하는 정책을 수립함 • 악성코드 방지 프로그램의 설치와 주기적인 업데이트를 수행함
	A.11.7.1 이동 컴퓨팅 및 통신	7.7.1 이동 컴퓨팅 및 통신	11.6.1 이동컴퓨팅	• 물리적 보안, 접근통제, 악성코드 방지 등의 내용이 포함된 이동 컴퓨팅 도구 사용에 대한 보호 정책을 수립함 • 악성코드 방지 프로그램 설치 및 주기적인 업데이트를 수행함
방화벽	A.10.6.1 네트워크 통제	6.6.1 네트워크 통제	10.3.1 네트워크 접근	• 네트워크로 전송되는 정보의 기밀성, 무결성 등을 보장하는 네트워크 통제 정책을 수립함 • 침입차단시스템, 침입탐지시스템, 방화벽 등 정보보호시스템 도입을 통하여 네트워크에 연결된 정보시스템에 대한 보안 강화
	A.10.8.1 정보 교환 정책과 절차	6.8.4 전자적 교환 보안	11.3.2 인터넷 접속관리	• 전자 메일, 메신저, P2P 통신 등을 통한 전자적인 정보 교환에 대한 보호 방안을 수립함 • 정보보호시스템 도입을 통하여 외부 메신저, 상용 메일, P2P 서비스 등 차단
망분리	A.11.4.1 네트워크 서비스 사용 정책	7.4.1 네트워크 서비스의 사용정책	10.1.1 접근통제 정책의 문서화	• 접근이 허용된 네트워크와 네트워크 서비스, 네트워크 연결 및 서비스를 보호하기 위한 절차와 보호 방안을 수립함 • 업무특성 또는 보안요구 사항에 따라 내부망과 외부망의 분리를 수행함
	A.11.4.5 네트워크에서의 분리	7.4.5 네트워크 분리	11.3.1 네트워크 운영대책	• 내부 네트워크 도메인과 외부 네트워크 도메인 분리 • 보안 게이트웨이, IP 스위칭, 무선 네트워크 분리 등

Ⅴ. 결 론

조직의 정보 자산의 가치가 점차 높아짐에 따라 조직이 가지고 있는 정보를 보호하고 정보통신 인프라를 강화하는 방안이 강구되고 있다. 정보보안을 강화하기 위해서는 정보보호관리체계에 따라 프로세스를 수립하여 관리하고 유지해야 하며, 조직원 및 사용자 측면의 보안부터 내부망 전체의 보안을 제공할 수 있는 정보보호제품 등을 도입하여 정보 자산을 보호하는 것이 중요하다.

전자정부의 정보보안 강화를 위해서는 새로운 위협요소 및 취약성 발견 등 지속적으로 변화하는 IT 및 인터넷 환경에서 내부의 주요 정보자산을 효과적으로 보호하고 관리하기 위해서는 주기적인 위험분석을 통한 지속적인 사후관리가 필요하다. 이 과정은 일회성 단계가 아니라, 지속적으로 유지·관리되어야 하는 순환주기의 형태를 가진다. 특히 사후관리를 통해 실질적으로 운영되고 있는 정보보호관리체계의 적합성을 판단하고 부족한 부분에 대한 갱신이 이루어져야 한다.

또한 각 단계에서 통제항목을 만족하도록 정보보호 정책을 수립하고 관리되어야 하며, 정보보호와 관련된 위험을 통제하기 위한 대책을 수립하고 관리하여 위협에 대응할 수 있는 대책을 마련해야 한다.

정보보호제품 중 조직의 정보 자산 유출을 방지하기 위하여 망분리 제품에 대한 요구가 증가하고 있으며, 망분리 제품에 대한 관심이 증가하고 있다. 망분리 방식 중 물리적 망분리 방식은 비용이 높기 때문에 논리적 망분리 제품이 개발되고 점차 시장이 확대되고 있다. 논리적 망분리 제품은 자료유출방지 제품군의 기능을 포함하고 있으며, 정보 자산의 유출을 방지하는데 효과적이기 때문에 많은 수요가 예상되고 있다. 논리적 망분리 방식을 구현함에 있어서도 다양한 가상화 기술이 기반이 되어 기술적인 측면에서도 많은 관심을 받고 있다. 하지만 아직 논리적 망분리 방식이 물리적 망분리 방식과 동일한 보안을 제공하는지에 대한 검증이 정확히 이루어지고 있지 않기 때문에 인증 제도를 통한 보안 검증이 반드시 필요할 것으로 사료된다.

참 고 문 헌

[1] D. Lenton, “The small screen [TV to Mobile Devices],” *IEE Rev.,* vol. 49, no. 10, pp. 38-41, Oct. 2003.

[2] Albert, Christopher & Dorofee, Audrey. "Managing Information Security Risks: The OCTAVE Approach.", *Addison Wesley,* July 2002

[3] Carey, Mark. “Enterprise Risk Management: How To Jumpstart Your Implementation Efforts.” *International Risk Management Institute*, 2005

[4] Control Objectives for Information and related Technology COBIT 4.1. "Information Systems Audit and Control Association." www.isaca.org

[5] Corporate Governance Task Force. “Information Security Governance: A Call to Action.” *National Cyber Security Partnership,* 2004.04

[6] David A Chapin and Steven Akridge. "How Can Security Be Measured? Information Systems Audit and Control Association." www.isaca.org 2005

[7] ISO(International Standard organization), ISO 27001, 2005.10

[8] John Sherwood, Andrew Clark and David Lynas. "Enterprise Security Architecture: A Business-Driven Approach", *CPM Books* 2005

[9] Schneier, Bruce. “Hacking the Business Climate for Network Security.” Computer, *IEEE,* April 2004

[10] ISO(International Standard organization), ISO 27001, 2005.10

[11] *한국인터넷진흥원,* ISMS(정보보호관리체계), 2008.05

[12] *한국인터넷진흥원,* PIMS(개인정보보호관리체계), 2010.11

[13] *한국인터넷진흥원,* 개인정보보호관리체계 인증준비 안내서(사업자용), 2010.12

[14] *행정안전부,* G-ISMS(전자정부정보보호관리체계), 2009.12

[15] *한국정보보호학회,* 전자정부 정보보호관리체계(G-ISMS) 적용 정책, 2009.10

박 청 수 (朴淸秀)

2008년 02월 순천향대학교 정보보호학과(공학사)

2008년 08월 ~ 2010년 07월 한국인터넷진흥원 인터넷서비스보호팀 주임연구원

20010년 09월 ~ 현재 SK 인포섹 전임 컨설턴트

관심분야 : ISMS, 기반시설 등

이 동 범 (李東範)

2008년 02월 순천향대학교 정보보호학과(공학사)

2010년 02월 순천향대학교 정보보호학과(공학 석사)

2010년 03월 ~ 현재 순천향대학교 정보보호학과 박사과정

관심분야 : 정보보호, 보안성 평가, 복합기 보안, 스마트워크 등

곽 진 (郭鎭)

1994년 ~ 2006년 성균관대학교 (공학사, 공학석사, 공학박사)

2006년 ~ 2006년 일본 큐슈대학교 방문연구원

2006년 ~ 2006년 일본 큐슈시스템 정보기술연구소 특별연구원

2006년 ~ 2007년 정보통신부 개인정보보호기획단 개인정보보호팀 통신사무관

2007년 ~ 2009년 정보통신연구진흥원 집필위원

2007년 현재 순천향대학교 정보보호학과 교수

2009년 순천향대학교 공과대학 교학부장

2009년 ~ 2010년 순천향대학교 정보보호학과 학과장

2010년 ~ 2010년 교육과학기술부 국가기술수준평가 전문위원

현재 : 정보통신산업진흥원 기술평가위원, 사)국제정보능력 평가원 쇼핑몰 플래너 자격 검정 출제 및 채점위원, 한국과학기술정보연구원 충남 과학기술 정보협의회 전문위원, 지식경제부 지식경제기술혁신평가단 평가위원, 순천향BIT 창업보육센터 센터장, 순천향대학교 중소기업 산학협력센터 센터장

관심분야 : 암호프로토콜, 응용시스템보안, 개인정보보호, 정보보호제품평가, 클라우드 컴퓨팅보안 등