공공기관의 정보보안 관리 모델 연구

김재경[*], 정윤수[**], 오충식[***], 김재성[****]

Study of Information Security Management Model in Public Institution

JaeKyeong Kim[*], Yoon-Su Jeong[**], ChungShick Oh[***], JaeSung Kim[****]

요 약 최근 지능화· 고도화 되고 있는 사이버위협으로부터 기업의 정보자산을 안전하게 보호하기 위해서는 기술적인 분야뿐만 아니라 관리적, 환경적 분야 등 전방위적 대응체제를 구축하여야 한다. 본 연구에서는 보안적으로 안전한 망 설계를 위해 물리적 망분리와 논리적 망분리등 보안 망 이론에 대한 사례를 분석하여 기업 환경에 적합하고 상시적 대응 및 관리가 가능한 정보보호 관리 모델을 제안한다. 특히, 제안 모델은 기존 망에서의 개선사항을 도출하고, 개선사항이 적용된 망을 설계하기 위해서 중앙 관리성을 향상시킨 실시간 보안 대응 능력, 보안 위협 발생 시 선제 탐지 및 능동적 대처, 중요 장비 이중활르 통한 고가용성, 고성능, 고신뢰성 확보, 개별 네트워크의 보안 정책 통합 관리, 개별 네트워크의 망 분리로 보안성 향성 등의 기능을 적용하였다.

주제어 : 정보보호, 정보보호 관리체계, 실시간 보안관리, 보안관리 프로세스, 보안망

Abstract Recently, Cyber threats that is doing intelligence and sophistication from the organization's information assets to secure order technical disciplines, as well as managerial and environmental sectors, such as mind-response system is must established. In this paper, possible to analyze the case for the theory in network security, such as the logical network and physical network separation suitable for the corporate environment and constantly respond and manage the Information Security Management Model A secure network design is proposed. In particular, the proposed model improvements derived from the existing network, network improvements have been made in order to design improved ability to respond to real-time security and central manageability, security threats, pre-emptive detection and proactive coping, critical equipment in the event of a dual hwalreu through applied features such as high-availability, high-performance, high-reliability, ensuring separation of individual network security policy integrated management of individual network, network security directional.

Key Words : Information Security, ISMS, Realtime Security Management, Security Management Process, Secure Network

1. 서론

현재 발생하고 있는 보안 위협들은 하루가 다르게 변하고 있으며, 정보시스템이 다양해지고 복잡해짐에 따라 보안 위협들도 점점 다양해지고 있다. 하지만 현재 이러한 보안 위협을 실질적으로 평가 및 관리 할 수 있는 관리체계는 없는 상황이다[1].

국내외 주요 정보보호 관리체계는 정보보호관리체계, 전자정부 정보보호관리체계, 개인정보보호관리체계, 국제 정보보안 경영시스템으로 나뉘어져 있고 각각 방송통

[*]한국과학기술정보연구원 정보화전략실, 선임연구원
[**]목원대학교 정보통신공학과 조교수 : 교신저자
[***]한국과학기술정보연구원 정보화전략실, 책임연구원
[****]한국과학기술정보연구원 정보화전략실, 실장
논문접수: 2013년 1월 15일, 1차 수정을 거쳐, 심사완료: 2013년 2월 14일, 확정일: 2013년 2월 20일

신위원회, 행정안전부, 방송통신위원회, 한국인정원에서 사용되고 있다[2,3].

국내에는 수많은 기관이 존재하지만 기관의 특성이 반영되지 않은 채 동일한 규격의 관리체계 모델이 적용되고 있어 대상 기관의 적절한 정보보호 특성을 반영하기 힘들다. 현 정보보호 관리체계 모델은 일시적인 관리에 그치기 때문에 지속적인 대응 및 관리가 불가능하여 보안 체계에 허점이 생기기 쉽다. 또한 현 정보보호 관리체계 인증 심사 시 수개월의 시간 및 인력이 소요되는 체계로 되어 있어서 정보보호 관리체계 구축에 따른 비용 대비 효과가 저조한 문제점이 존재한다. 실제로 행안부, 교과부, 국정원 등 다양한 정부차원의 정보보호 평가체계들을 수용하지 못하며, 평가 준비를 위한 다수의 인력 및 시일이 소요되고 있다[4,5].

〈표 1〉 기존 ISMS와 실시간 ISMS의 차이

	기존 ISMS	실시간 ISMS
측정 결과	절대적 (통과 / 거부)	상대적 (현재 상태)
측정 항목	조직 보안 통제 항목	자체 측정 항목 개발
특징	제3자 평가	자체 평가

<표 1>에서는 기존 ISMS와 실시간 ISMS의 차이를 비교 분석하고 있다. <표 1>처럼 기존의 ISMS의 한계를 극복하기 위해서 기업에서는 기업에 맞는 상시적인 대응 및 관리가 가능한 정보보호 관리체계 모델이 필요하다.

본 논문에서는 보안적으로 안전한 망 설계를 위해 물리적 망 분리와 논리적 망 분리 등 보안 망 이론에 대한 사례를 분석하여 기업 환경에 적합하고 상시적 대응 및 관리가 가능한 정보보호 관리 모델을 제안한다. 특히, 제안 모델은 기존 관리체계 모델의 문제점을 분석하여 각 관리체계별로 상이한 평가지표들을 통합하고 분류하여 상시적으로 대응 및 관리가 가능하도록 하였다. 또한, IT 인프라 환경의 변화 및 신규 보안 위협들로부터 안전하고 신뢰성 있는 망 구축을 위해 실시간 ISMS에 의해 조절 가능한 원내망 구축, 유무선 원내망을 모두 지원하는 방화벽 및 침입 방지 시스템 구축, 내부 정보 유출 방지, 네트워크 접근제어, PC 보안관리 등의 시스템 구축, 특정 장비에서 장애가 발생하더라도 서비스 가용성 보장 등을 지원하고 있다.

이 논문의 구성은 다음과 같다. 2장에서는 국내외 정보보호 관리체계에 대해서 알아본다. 3장에서는 기업의 정보보호 관리 체계 모델을 제시하고, 4장에서는 기업의 정보보호 수준을 평가하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

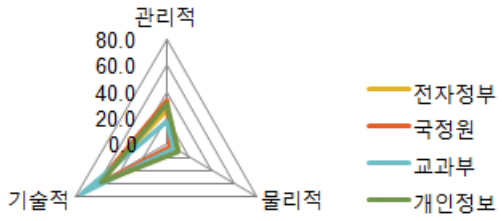
2.1 전자정보 정보보호 관리체계

전자정부 정보보호 관리체계(G-ISMS, Government Information Security Management System) 인증은 기관이 수립하고 구축한 종합적인 정보보호 관리체계(ISMS)를 제 3자가 객관적으로 심사하여 인증을 부여하는 제도이다[2,6]. 정보보호 관리체계(ISMS)는 조직의 정보 자산을 체계적으로 보호하고 사이버침해 위협으로부터 조직이 유기적으로 대응하기 위한 종합적인 관리체계를 의미한다. G-ISMS는 정부 행정기관 등의 조직 및 서비스의 특성에 적합하게 수립된 종합적인 정보보호 관리체계를 의미한다[7].

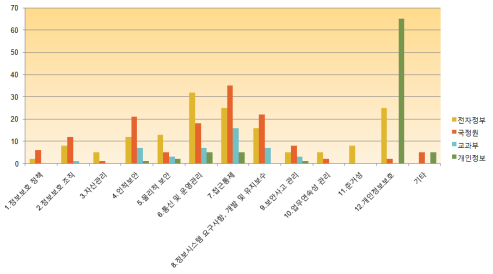
[그림 1] G-ISMS 목표 및 기능

2.2 기존 관리체계 분석

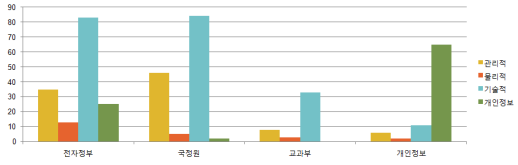
기존 관리체계를 분석한 결과 보안의 3요소 중, 전자정부 정보보안 관리모델은 무결성을, 국정원의 평가기준은 기밀성을 더 중요한 목표로 설정하고 있다[8,9]. 또한 전자정부, 국정원 모두 관리체계에 있어 전체적으로 많은 부분을 담고 있으며, 항목 수의 차이는 있으나, 기술적, 관리적 분야에 많은 비중을 두고 있음을 알 수 있다.



[그림 2] 기존 관리체계 분포도



[그림 3] 기존 관리체계 분류 1



[그림 4] 기존 관리체계 분류 2

2.3 국외 관리체계 분석

2.3.1 영국 및 유럽권의 정보보호 관리체계

유럽 전체의 정보보호관련 가장 대표적인 기관은 European Network and Information Security Agency (ENISA)로써 European Union (EU)의 정보보호 관련 이슈들을 담당하는 기관이기도 하다[10]. ENISA가 운영하는 웹사이트의 주 목적은 정보보호에 관한 정보 교환 및 실제 필드에서의 best practice와 지식들을 공유하는 허브 역할이다. EU의 주된 설립 목표는 EU 회원국들과 산업계들의 정보보호 관련 문제들을 방지하고, 또한 사고 발생시 대응가능한 체계를 만들기 위함이다.

2.3.2 SP 800-53국외사례

SP 800-53(연방 정보 시스템을 위한 권고된 보안 통제, Recommended Security Controls for Federal Information Systems and Organizations)은 FIPS 199에서 명시하고 있는 보안 분류 및 정보 시스템의 최소한의 보안 통제 요구사항에 대한 이용 가이드라인을 제공하기 위하여 제정되었다[11,12]. 다시 말하면, SP 800-53은 정보 시스템에 대한 추가적인 위협과 위험 고려사항에 관하여 요구되는 보안 통제에 대한 상위 분류 기준을 제공한다.

SP 800-53은 FIPS 200의 요구사항에 부합되도록 정보 시스템에 대한 보안 통제를 올바르게 선택하기 위한 지침으로써, 보안 통제 목록을 정의하고 정보 시스템의 보안 통제를 선택하는 과정을 설명하고 있다. SP 800-53에 따라 선택된 보안 통제는 연방기관의 정보를 처리, 저장, 전송, 수신하는 정보 시스템의 모든 구성요소에 적용되고, 안전한 정보 시스템을 구축하고 효율적인 위험 관리가 가능하도록 수행된다.

3. 기업의 정보보안 관리 체계 모델 설계

이 절에서는 현재 기업에서 제공하는 정보보호 관리체계가 외부 위협으로부터 상시적으로 대응 및 관리할 수 있는 보안 관리 모델을 제안한다.

3.1 기업의 보안관리 모델

제안 모델의 보안관리 모델은 G-ISMS이기 때문에 이를 바탕으로 관리적 보안, 기술적 보안, 물리적 보안, 개인정보보호 등 4가지 분야로 분류하면 [그림 4]와 같다.

분야	도메인	분야	도메인
관리적 보호	정보보호 정책 및 조직	기술적 보호	침해사고 관리
	정보자산 관리		전자정보 관리
	업무 연속성 관리		어플리케이션 보안
	정보화 사업 관리		무선 및 네트워크 보안
	인적 보안		시스템 보안
	준거성 관리	개인정보보호	관리적 개인정보보호
물리적 보호	보호구역 관리		개인정보 처리
	일반구역 관리		기술적 개인정보보호

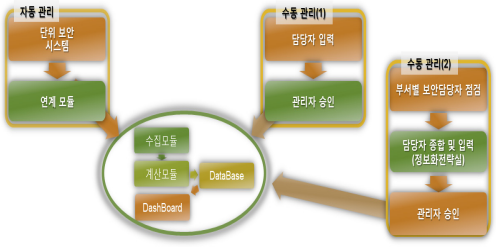
[그림 4] 기업의 정보보호 관리체계 모델 (도메인)

[그림 4]처럼 제안 모델은 필요한 세부 통제 항목을 산출식으로 점수를 매긴다. 산출식은 부서별 산출식과 기업산출식으로 나뉘는데, 부서별로 점수를 매길 필요가 있는 경우에는 부서별 산출식을 사용하여 그 점수의 평균을 기업 산출식 점수로 사용하고 그 외의 경우에는 각

세부 통제 항목에 맞게 산출식을 정하였다. 그리고 이렇게 매겨진 점수와 목표 수준 점수를 비교하여 그 통제 항목을 지켰는지 확인할 수 있고, 각 관리체계에 대한 인증을 용이하게 받을 수 있다.

3.2 상시적 대응 관리 프로세스

제안 모델이 국정원, 교과부, 행안부, 개인정보보호 등 다양한 관리체계에 대한 인증을 용이하게 받기 위해서 제안 모델은 공통적인 통제 항목을 통합하고 매월 사이버보안진단의 날에 각 부서별 보안담당자가 기본적인 사항을 점검하고 결과를 정보화 전략실에서 종합, 이력관리를 통해 실제 평가에 사용한 [그림 5] 같은 관리 프로세스를 사용한다. [그림 5]의 각 세부 통제 항목들은 그 특성에 따라서 관리방법이 자동과 수동으로 나뉜다. 자동 관리 항목은 단위 보안 시스템 및 관련 시스템과 연계하여 자동으로 데이터를 산출하는 방법이고 수동 관리 항목은 정보화전략실에서 관련 근거 자료를 매월 사이버 보안진단의 날에 확인한 뒤, 직접 입력하는 방법과 부서별 보안 담당자가 사이버 보안 진단의 날 점검결과를 정보화전략실로 송부하고 그 정보를 토대로 정보를 확인 및 입력하는 크게 두 가지가 있다.



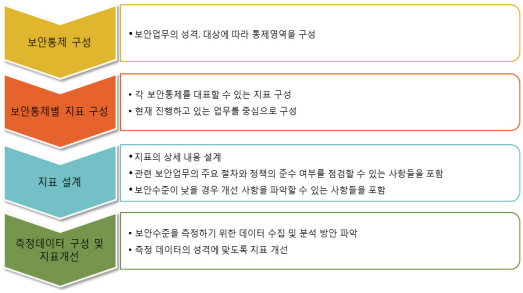
[그림 5] 관리 프로세스

[그림 5]의 관리 프로세스에서 수동관리1과 수동관리2는 둘 다 정보화전략실의 관리자의 승인을 받아서 정보가 올라간다는 점은 같지만 수동관리2의 경우는 각 부서별 내용이 필요한 세부 통제 항목의 경우이고 수동관리1은 그 외의 경우를 뜻한다.

자동 관리와 수동 관리 방법을 통하여 데이터 수집이 되면 각 산출식에 따라서 점수가 매겨지게 되고 그것을 데이터베이스에 저장한 뒤, 대쉬보드를 통하여 기관의 전체적 보안 수준을 확인할 수 있다. 데이터베이스에 저장된 데이터는 각 관리체계의 인증 시 필요한 것만 뽑아서 사용되고 그것을 이용하여 심사를 용이하게 받을 수 있다.

3.3 보안 요구사항에 따른 지표 설계

기밀성, 무결성, 가용성에 따라 요구 수준 차별화가 필요하기 때문에, 기업 특성에 적합한 보안 목표, 통제, 지표를 설계한다. 지표 설계 절차는 [그림 6] 지표 설계 절차와 같다.



[그림 6] 지표 설계 절차

보안 지표 설계에 대한 예제는 [그림 7]과 같이, 보안업무의 성격, 대상에 따라 섹션을 구분하여 각 섹션 별로 통제 목표를 정하였다.

Section	Control objective	설명
보호정책	정보보호 정책서	**정보보호정책서**는 경영층의 승인을 득한 후 전 직원 및 관련 외부 인력에게 **배포 및 인지**시켜야 한다.
인적자원 보호	정보보호 인식, 교육 및 훈련	모든 조직의 임직원 및 관련 계약자와 제3의 사용자에 대한 적절한 인식훈련 및 직무와 관련된 조직정책 및 관련 절차에 대한 **주기적인 갱신 교육**을 수행하여야 한다.
접근통제	**네트워크** 서비스 사용 정책	사용자는 사용에 있어 특별히 **인가된 서비스의 접근만 허용**할 수 있도록 하여야 한다.
	사용자 접근권한 검토	관리자는 **사용자의 접근 권한을 검토**하는 공식적인 절차를 주기적으로 수행하여야 한다.
정보시스템 획득, 개발, 유지보수	기술적 취약점 통제	적절한 기술적 취약점 인식 및 인식된 **취약점**에 대한 조직의 노출에 대한 **평가**가 이행되어야 한다.

[그림 7] 섹션별 설계 예제

3.4 평가지표 정량화 및 분류

제안 모델에서 설계한 지표를 토대로 항목별 정량화 방법 연구와 정량화 수치에 대한 검증 절차는 [그림 8]과 같은 평가지표를 상세화하여 정량화 한다한다. 제안 모델에서 통제 목표가 설정되면, [그림 8]과 같이 통제목표를 측정하기 위한 지표의 근거자료와 계산식을 구성한다.

Measure ID	원격 접근 제어 측정 1 (혹은 자체 정의한 유일한 값)
Goal and Objective	1. 전략 목표 : 손쉬운 보안과 추적 가능한 개인, 시설, 장비의 환경보장 2. 보안 목표 : 정보, 시스템 등이 사람, 기계 등에 대한 접근을 확인, 파악, 인정, 인증하여 제한함
Measure	비 인가된 원격지 접근 포인트의 비율(%)
Measure Type	Effectiveness/Efficiency
Formula	(비인가 원격 접속 수/전체 원격 접속 수) X 100
Target	조직에서 결정한 하위 비율(예, Low)
Implementation Evidence	1. 조직이 모든 원격접속을 확인하기 위해 자동화 툴을 사용하고 네트워크 구성을 최신으로 유지 업데이트 하는가(CM-2)? 2. 얼마나 많은 원격 접속 포인트가 존재하는가? 3. 원격 접속 트래픽 감시를 위하여IDS를 유지 관리하는가(SI-4)? 4. 원격 접속 로그를 남기고 분석하는가(AU-6)? 5. 침해사고 분류 표준을 만들고 데이터베이스를 운영하고 있는가(IR-5)? 6. 침해사고 데이터베이스, IDS 로그, 원격 접속 로그 분석에 기반하여 얼마나 많은 접속 포인트가 비인가 접속을 하였나?
Frequency	1. 수집 주기(조직정의) : 월별 2. 보고 주기(조직정의) : 분기별
Responsible Parties	1. 정보담당 : CSIRT 2. 정보보안담당 : ISSO 3. 정보고객 : CIO, SAISO, CISO, Auditor

[그림 8] 평가지표 상세내역

3.5 관리체계 보안 모델 설계

이 절에서는 기업의 보안 목표를 달성하기 위해 분야 / 도메인 / 통제항목 / 세부 통제 항목 등 4단계로 구분하였다. 세부 통제 항목은 기존의 4가지 관리체계의 세부 통제 항목을 재분류 및 통합을 하였기 때문에 그 관리 체계들을 모두 수용하였으며 각 세부 통제 항목에 대해 평가 항목, 증빙 자료, 관리 방법, 통제 목표, 목표 수준, 산출식을 포함함으로서 외부 관리체계에 대해 기업 내부적으로도 관리할 수 있는 프로세스를 구현하고 있다.

3.5.1 통제 항목 분류

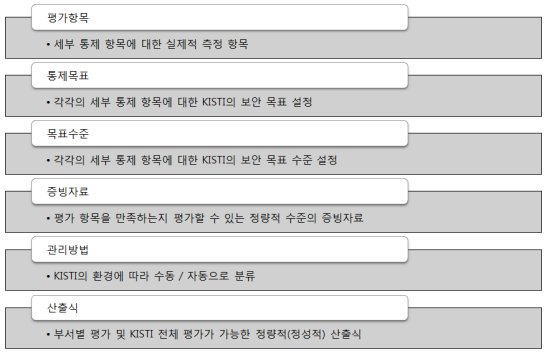
관리체계 보안 모델에서 통제 항목은 기존 G-ISMS와 개인정보보호법을 기반으로 관리적 보안 / 기술적 보안 / 물리적 보안 / 개인정보보호 4가지로 분류하고 각 분류당 기존 관리체계의 통제 항목들을 통합할 수 있도록 도메인과 통제항목을 [그림 9]처럼 설정한다.

분야	도메인	통제항목	분야	도메인	통제항목
관리적 보안	정보보호 정책 및 조직	정보보호 정책	기술적 보안	무선 및 네트워크 보안	네트워크 보안
		정보보호 조직		시스템 보안	사용자 인증
		정보보호 활동			정보시스템 관리
		기관장 관심도			PC 보안
	정보자산 관리	정보자산 보안관리			서버 보안
		국가용 보안시스템 관리	물리적 보안	보호구역 관리	보호구역 관리
		휴대용 저장매체 관리		일반구역 관리	일반구역 관리
	업무연속성 관리	재해 복구	개인정보보호	관리적 개인정보보호	개인정보보호 정책
	정보화 사업 관리	용역사업 관리			개인정보보호 조직
	인적 보안	내부인원 보안			개인정보보호 교육
		외부인원 보안			개인정보 처리방침
		정보보안 교육			개인정보 영향평가
	준거성 관리	준거성 관리		개인정보 처리	영상정보 관리
기술적 보안	침해사고 관리	침해사고 대응체계			수집 동의
		로그 관리			수집 정보 관리
	전자정보 관리	비밀 전자적 관리			이용 및 제공
		전자우편 유출방지			업출력 관리
	어플리케이션 보안	전자우편 보안		기술적 개인정보보호	개인정보보호 시스템 관리
		홈페이지 관리			침해사고 대응절차
	무선 및 네트워크 보안	무선랜 보안			

[그림 9] 기업의 정보보호 관리체계 통제 항목

3.5.2 통제 항목 세부사항

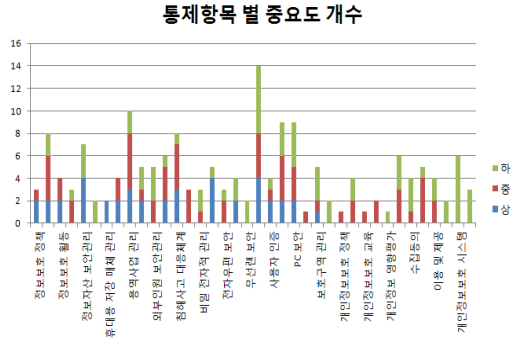
통제 항목을 크게 분류한 뒤, 각 세부 통제 항목마다 평가항목, 통제목표, 목표수준, 증빙자료, 관리방법, 산출식 등을 제시하였다. 각 세부사항에 대한 정의와 구조는 [그림 10]과 같다.



[그림 10] 통제 항목 세부사항 정의

3.5.3 통제 항목 별 중요도

제안 모델에서 통합 된 통제 항목 별 중요도는 [그림 11]과 같으며, [그림 11]에서 통제항목별 중요도를 비교 평가하고 있다.



[그림 11] 통제 항목별 중요도 개수

4. 평가

이 절에서는 제안 모델을 기업에 적용한 정보보호 관리체계의 측정결과를 분석한다.

4.1 지표 선정 및 산출식

제안 모델에 사용되는 지표는 <표 2>와 같이 총 24개의 통제항목으로 선정하고 <표 3>의 지표 산출식 (□: 수기 입력, ■: 자동입력)은 해당 통제항목의 산출식을 나타낸다. 측정지표는 4개 분야에서 적어도 1개 이상의

지표를 포함하고, 중요도가 '상'인 지표를 대상으로 선정한다. 자동관리항목 뿐만 아니라 수동관리항목 또한 포함한다.

〈표 2〉 구현을 위한 지표 선정 예

분야	도메인	통제항목	세부통제항목
1. 관리적 보안	1.1 정보보호 정책 및 조직	1.1.1 정보보호 정책	1.1.1.1 정보보호 정책수립 및 개정
		1.1.2 정보보호 조직	1.1.2.2 정보보안 조직구성
			1.1.2.8 정보보안 위원회
		1.1.3 정보보호 활동	1.1.3.2 사이버보안진단의 날 활동
	1.2 정보자산 관리	1.23 휴대용 저장매체 관리	1.2.3.1 휴대용 저장매체 보안관리
	1.4 정보화사업 관리	1.4.1 용역사업 관리	1.4.1.7 정보보안 정책수립 및 개정
			1.4.1.8 용역업체 업무망 보안관리
			1.4.1.9 용역업체 인터넷 보안관리
	1.5 인적 보안	1.5.2 외부인원 보안	1.5.2.4 용역사업자 휴대용 저장매체 보안관리
2. 기술적 보안	2.1 침해사고 관리	2.1.1 침해사고 대응체계	2.1.1.5 DDoS 대응시스템 구축
	2.2 전자정보 관리	2.2.2 전자정보 유출방지	2.2.2.1 정보유출 방지 보안대책
			2.2.2.4 비인가 사이트 차단
	2.4 무선 및 네트워크 보안	2.4.1 무선랜 보안	2.4.1.2 무선랜 운영 보안관리
	2.5 시스템 보안	2.5.2 정보시스템 관리	2.5.2.8 변경 관리
		2.5.3 PC 보안	2.5.3.1 PC 운영체제 패치 관리
			2.5.3.2 PC 백신 관리
			2.5.3.3 부재중 PC 보안관리
			2.5.3.4 PC 공유폴더 관리
			2.5.3.5 PC 응용프로그램 패치관리
			2.5.3.6 USB 자동실행 차단
			2.5.3.8 개인정보 필터링 시스템 구축 및 운영
3. 물리적 보안	3.1 보호구역 관리	3.1.1 보호구역 관리	3.1.1.1 보호구역 지정 및 관리
4. 개인정보보호	4.2 개인정보처리	4.2.2 수집동의	4.2.2.1 개인정보의 수집 동의
		4.2.3 수집 정보 관리	4.2.3.1 개인정보 파일관리

4.2 프로토타입

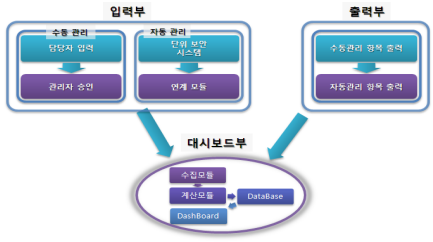
제안 모델에서 프로토타입의 전체적인 구성은 [그림 12]와 같으며, 크게 대시보드부, 입력부, 출력부 등으로 3개의 구성요소를 포함한다. 대시보드부는 정보보호 관리체계의 측정결과가 그래프 형태로 출력되는 부분이다. 측정결과는 100점 기준의 수치로 나타나며, 분야별, 도메인별, 통제항목별, 세부통제항목별로 각각 별도의 그래프가 출력된다. 또한 누적된 측정결과를 통해 조직의 보안수준 추이를 한눈에 파악하기 위한 추이별 그래프 또한 제공한다.

입력부는 산출식에 사용되는 데이터를 수집하기 위한 기능을 수행한다. 입력부를 통해 수기관리항목에 대한 데이터를 직접 입력할 수 있으며, 자동관리항목에 해당되는 데이터는 시스템별 로그파일을 직접 등록시킴으로써 데이터를 입력한다. 출력부는 입력부를 통해 입력된

〈표 3〉 지표 산출식 (□: 수기 입력, ■: 자동입력)

세부 통제항목	수기 및 자동 입력
1.1.1.1 정보보호 정책수립 및 개정	□ 정보보안 정책수립 여부 (50%) □ 전 직원 공지여부 (20%) □ 유관기관 및 상급기관과 연 1회 이상 검토 여부 (30%)
1.1.2.2 정보보안 조직구성	□ 정보보호 전담 조직여부 (100%)
2.1.1.5 DDoS 대응시스템 구축	□ DDoS 대응시스템 도입 여부 (30%) ■ 탐지 로그 여부 (30%) ■ 차단 로그 여부 (40%)
2.2.2.1 정보유출 방지 보안대책	□ 관련규정 (30%) ■ (Agent 설치 수/전체 PC 수)*70 (70%)
2.5.3.1 PC 운영체제 패치 관리	□ 관련규정 (30%) ■ 지키미 항목에 대한 점수(평균)*0.7 (70%)
2.5.3.2 PC 백신 관리	□ 관련규정 (30%) ■ 지키미 항목에 대한 점수(평균)*0.7 (70%)
2.5.3.3 부재중 PC 보안관리	□ 관련규정 (30%) ■ 지키미 항목에 대한 점수(평균)*0.7 (70%)
3.1.1.1 보호구역 지정 및 관리	□ 관련규정 (20%) □ 보호구역 지정여부 (30%) □ CCTV 설치여부 (15%) □ 이중잠금장치 설치여부 (15%) □ 개인정보 포함 서류 이중케비넷 설치여부 (20%)
4.2.2.1 개인정보의 수집 동의	□ 관련규정 (30%) ■ (고지 완료 부서/고지 대상 부서)*70 (70%)

데이터를 출력 및 수정하기 위한 기능을 수행한다. 관리자는 해당 모듈을 통해 수집되는 데이터의 신뢰성을 확보하고 에러를 최소화한다.

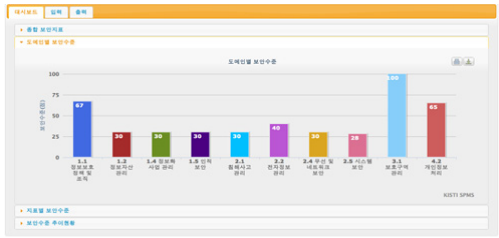


[그림 12] 제안 모델의 프로토타입

4.3 구현 결과

4.3.1 도메인별 보안수준

제안 모델을 도메인별 보안 수준을 평가한 결과 [그림 13]과 같다.

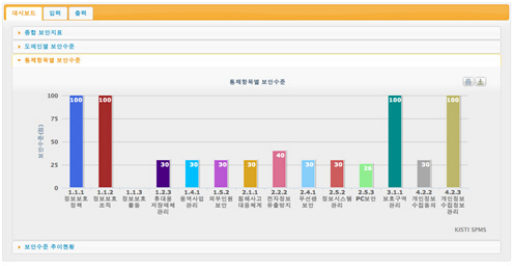


[그림 13] 도메인별 보안수준

[그림 13]은 도메인별 보안수준을 수치화 한 대시보드로써, 프로토타입 구현에 사용된 도메인은 총 10개이며, 각 도메인별 평균 점수를 막대그래프를 이용하여 나타내고 있다.

4.3.2 통제항목별 보안수준

제안 모델의 통제항목별 보안수준은 [그림 14]과 같으며, [그림 14]은. 총 14개의 통제항목이 구현을 위해 사용되고 있다.



[그림 14] 통제항목별 보안 점수

5. 결론

정보의 지능화・다양화로 인하여 사이버 위협이 점점 증가되고 있는 상황에서 정보보호시스템 구축 등 기술적인 분야 뿐만 아니라 정보보호 정책 및 규정, 정보보호 조직 등 관리적인 분야도 고려해야 한다. 본 논문에서는 기업의 실제적인 보안강화를 위해서 기업 환경에 적합하고 상시적 대응 및 관리가 가능한 정보보호 관리 모델을 제안하였다. 제안 모델은 기존 관리체계 모델의 문제점을 분석하여 각 관리체계별로 상이한 평가지표들을 통합하고 분류하여 상시적으로 대응 및 관리가 가능하도록 하여 기존 기업의 보안 관리 체계의 문제점을 개선하였다.

향후 연구에서는 기업의 정보보안 관리 서비스에 대한 연속성을 확보하기 위해서 정보보안 관리 시스템을 구축하고 이에 따른 업무영향분석을 설계할 계획이다.

참 고 문 헌

[1] 정보보호 관리체계(ISMS) 인증, http://blog.naver.com/p1ngp1ng?Redirec t=Log&logNo=120040448210.

[2] 국내: G-ISMS, http://ju12.tistory.com/327.

[3] 개인정보보호 관리체계(PIMS, Personal Information Management System) 인증에 대하여, http://privacy.naver.com/80116523634..

[4] “망분리 란?”, 안철수 연구소, http://m.ahnlab.com/kr/site/securityinfo/secun ews/secuNewsView.do?seq=14140&curPage=1

[5] “우리 회사에 적합한 망분리 솔루션은?”, 안철수 연구소, http://blog.naver.co m/PostView.nhn?blogId=moping75&logNo=90122504502&redirect=Dlog&widgetTypeCall=true

[6] ISO/IEC 27001 정보보안경영시스템 개요, http://ksaqs.blog.me/110113695631

[7] KISA(2011), “KISA G-ISMS 인증안내서”, KISA.

[8] 한국정보사회진흥원(2008),“국가기관 망 분리 구축 가이드”, 행정안전부, 국가정보원.

[9] KISTI 정보보안 정책 및 지침.

[10] ENISA Activities "What does ENISA do?", http://www.enisa.europa.eu/abou t-enisa/activities

[11] [알아봅시다] 해외 주요국 개인정보보호 정책, http://www.dt.co.kr/contents.ht ml?article_no=2012071002011860785002

[12] E.B. Lee, J.Y. Kim,“A Study on Information Security of Network Partition Based”Proc. of the KIISC Conference, vol.20, no.1. pp.39-46, Feb. 2010. (in Korean)

김 재 경

・2005년 2월 : 광운대학교 컴퓨터과학과(석사)
2011년 3월~현재 : 한국과학기술정보연구원기술원
・관심분야 : 정보보안, 개인정보보호, 포렌식
・E-mail : kjk@kisti.re.kr

정 윤 수

- 2000년 2월 : 충북대학교 대학원 전자계산학 이학석사
- 2008년 2월 : 충북대학교 대학원 전자계산학 박사
- 2009년 8월~2012년 2월 : 한남대학교 산업기술연구소 전임연구원
- 2012년 3월~현재 : 목원대학교 정보통신공학과 조교수
- 관심분야 : 센서 보안, 암호이론, 정보보호, Network Security, 이동통신보안
- E-Mail : bukmunro@gmail.com

오 충 식

- 2009년 2월 : 충북대학교 컴퓨터공학과 박사수료
- 2004년 2월 : 충북대학교 전자계산학과 이학석사
- 1986년 3월~현재 : 한국과학기술정보연구원 책임연구원
- 관심분야 : 보안, USN, 개인정보보호, 재난관리
- E-Mail : ocs@kisti.re.kr

김 재 성

- 1999년 2월 : 포항공과대학교 산업공학과석사
- 2003년 2월 : 포항공과대학교 산업공학과 박사
- 2003년 3월~현재 : 한국과학기술정보연구원 선임연구원
- 관심분야 : 정보화, 슈퍼컴퓨터
- E-Mail : jaesungkim@kisti.re.kr