JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 18, No. 3 : 617~624 Mar. 2014

캠퍼스 환경에서 적응적인 정보보안을 위한 통합 보안정책의 설계

고봉구[1] · 박종선[2] · 정성종[1] · 조기환[2*]

A Design of Integrated Security Policies for Enabling Adaptive Security in Campus Environment

Bong-koo Ko[1] · Jong-seon Park[2] · Seung-jong Chung[1] · Gi-hwan Cho[2*]

[1]Department of Information Technology, Chonbuk University, Jeonju 561-756, Korea
[2*]Division of Computer Science and Engineering, Chonbuk University, Jeonju 561-756, Korea

요 약

대학전산망은 방화벽에 의한 접근제어를 근간으로 보안정책을 세분화, 다양화하고 있다. 그러나 정보의 탈취, 침해사고, 그리고 서비스 거부 등 보안위협이 줄어들지 않고 있다. 본 논문은 개방적 특성을 갖는 캠퍼스 전산망에서 정보보호 구성요소를 기준으로 보안대상에 적응적으로 보안을 강화할 수 있는 차등적인 보안정책 방안을 제시한다. 보안장비의 보안수준은 사용자와 보안대상의 사상에 의해 결정된다. 제안된 보안정책은 창의적인 캠퍼스 환경에서 비용 대비 보안효과를 극대화하고 사용자에게 빠르고 안정된 서비스 환경을 제공함을 목적으로 한다.

ABSTRACT

A campus network nowadays adapts the security policies in detail and even in variety, along with firewall based access control. Nevertheless, security threats, such as information hacking, intrusion and DoS, are not decreasing yet. This paper proposes an enabling method of discriminative security policies to enforce an adaptive security for security objects on basis of the security elements. The security level of a security devices is decided based on the mapping between the users and the objects. The proposed security policies could improve the security effect in terms of investment in creative campus environment, and aim to provide fast and stable services to users.

키워드 : 캠퍼스 전산망, 방화벽, 보안대상, 보안정책

Key word : Campus Network, Firewall, Security Objects, Security Policy

접수일자 : 2013. 12. 16 심사완료일자 : 2014. 01. 10 게재확정일자 : 2014. 01. 28

* **Corresponding Author** Gi-Hwan Cho(E-mail:ghcho@jbnu.ac.kr, Tel:+82-63-270-3437)
Devision of Computer Science and Engineering, Chonbuk University, Jeonju 561-756, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2014.18.3.617 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

정보기술의 발달은 무형의 정보자산을 지속적으로 증가시키고, 심지어 유형의 물리적 자산도 정보자산에 의존적으로 변해가고 있다. 또한 IT 산업은 주요 기술을 아웃소싱하여 운영하는 체제로 변화하고 있다. 하지만 정보통신 환경 변화에 대응하여 보안위협도 다양한 형태로 진화하고 있다. 특히 다양한 수준의 보안요구 특성을 갖는 사용자로 구성된 캠퍼스 환경은 각종 보안 위협에 쉽게 노출되어 있기 때문에 보안대상으로부터 효율적이고 체계적인 보안정책이 요구된다[1].

기존의 데스크탑 PC뿐만 아니라 스마트폰, 태블릿 PC, 아이패드와 같은 무선매체에 기반을 둔 기기들이 인터넷을 통한 서비스에 의존하고 있다. 인터넷을 통한 다양한 서비스 이용이 가능한 반면 해킹, 크래킹 기법을 통한 정보 유출과 같이 다양한 보안위협이 존재한다. 특히 분산 서비스 거부공격(DDoS : Distributed Denial of Service) 에 의한 인터넷 서비스의 중단, 서비스 중단 협박 등의 보안위협은 심각한 수준이다. 이와 같은 보안위협에 대응하기 위해 최근에는 정보보호 정책 최적화와 더불어 다양한 정보보안장비 도입이 추진되고 있다[2].

이러한 노력에도 불구하고 전산망 서비스를 중단하게 하는 다양한 원인들이 보고되고 있다. 특히 개방적인 특성을 갖는 캠퍼스 환경에서는 일반 기업의 전산망 사용자와는 달리 보안위협에 쉽게 노출될 수 있다. 따라서 캠퍼스 네트워크 환경 특성을 고려하여 보안위협을 적응적으로 대응할 수 있고 최적의 보안효과를 제공할 수 있는 보안정책 수립이 절실히 요구된다[3,4].

본 논문은 캠퍼스 전산망에서 사용자를 기준으로 보안대상을 고려하여 보안장비에 차등적인 보안정책 실현 방안을 제시한다. 전산망 사용자별로 접근해야할 장비와 정보의 수준이 다르기 때문에 정보자산의 식별 및 분류, 가치산정, 등급화를 통해 보호해야할 정보자산을 정확히 정의한다. 또한 침해 종류에 따른 보안대상을 분류한다. 즉 정보보호의 대상, 자산, 그리고 서비스(연속성 및 속도) 등의 다차원 관계를 정의함으로써 구성요소 각각의 정보보호 역할과 구조를 명확히 한다. 결과적으로 사용자를 기준으로 차등적인 보안정책 실현이 가능하고 보안대상의 보안을 적응적으로 강화할 수 있다.

또한 보안정책과 전산망 관리의 협업을 통해 사용자에게는 편리성을 제공하고 궁극적으로는 캠퍼스 네트워크 환경에 효율적인 보안정책 실현이 가능하다.

본 논문의 구성은 다음과 같다. 2장에서 기존의 정보보호 통합보안 체계에 대해 살펴보고 3장에서 캠퍼스 전산망 사용자를 구분하고 보호해야할 정보, 서비스를 지속하기 위한 보안대상 그리고 보안장비의 역할과 설치 위치, 보안정책에 대해 기술한다. 4장에서는 기존의 보안정책에 추가적으로 적용되어야 할 사용자 구분, 정보보호 대상, 통합적인 보안정책 설계에 대해 제안하고 5장에서 결론을 맺는다.

Ⅱ. 기존 캠퍼스 환경의 통합보안 체계

스마트폰을 비롯한 다양한 정보 기기의 보급은 사용자의 인터넷을 통한 업무 의존도를 높이고 다양한 서비스 이용이 가능하도록 정보통신 생태계가 날로 진화하고 있다. 하지만 응용 서비스 관련 통신 프로토콜과 운영의 취약점에 의한 악의적인 공격 형태와 방법도 지속적으로 진화하고 있다. 특히 캠퍼스 네트워크는 일반 기업에 비해 개방적인 특성이 강해 보안위협에 쉽게 노출되어 있다. 그럼에도 불구하고 캠퍼스 정보통신 환경에 적용되는 보안정책은 제한된 장비와 범위에서 관습적인 사용에 의해 정의된 틀 수준에서 벗어나지 못하고 있다[5].

기존의 보안정책은 침해사고 대응을 위해 먼저 보안대상의 위험도를 측정하는 것으로부터 시작한다. 그리고 보안대상이 되는 정보자산의 정의, 등급, 업무 중요도 등을 정의하고 주어진 보안대상의 취약성을 정량적, 정성적으로 정의한다. 정보자산은 정보보호 핵심 구성요소인 기밀성, 무결성, 가용성을 기준으로 보안등급을 평가한다. 추가적으로 자산의 구매비용 등 정량적인 척도를 반영하여 보안정책을 적용하고 있다[6,7].

기존 보안정책의 근본적인 한계는 서버 중심, 데이터 중심의 보안체계에서 나타난다. 그림 1은 대부분의 대학에서 현재까지 운영된 통합 보안체계를 보이고 있다. 그림과 같이 기존 통합보안 시스템은 서버와 데이터베이스 중심의 체계로 구성됨을 알 수 있다.

기존의 통합보안 체계가 갖는 문제를 해결하기 위해서는 사용자, 보호해야할 대상, 보안장비가 정보보호

그림 1. 기존 캠퍼스 환경에 적용되었던 통합 보안체계
Fig. 1 Integrated security system applied to the existing campus environments

요구수준에 따라 분류되어야 한다. 이러한 기준을 이용하여 침해사고 대응을 위한 종합 정보보호 체계로 정보보호 데이터 수집 방안, 위험도 관리 방안 등을 수립한다. 결과적으로 침해사고 대응체계를 사후대책 중심에서 예측방어 체계로 전환할 수 있다.

최근의 보안환경을 고려하면 고객 중심, 서비스 중심의 보안체계가 기존의 시스템에 실현되어야 한다[8,9]. 대표적인 예로 P2P(Peer-to-Peer) 서비스는 기존 보안체계에서 무시하고 차단해야하는 서비스였으나 최근에는 대표적인 사용자 서비스로 자리 잡고 있다. 웹, 메일 등에 부수적인 P2P 서비스를 통하여 많은 자료들이 사용자 사이에 교환되고 있다. 하지만 P2P 특성을 고려하면 이를 합법적이고 효율적으로 이용할 수 있도록 보안정책에 대한 조정이 필요하다. 또한 인터넷을 통한 화상강의는 캠퍼스 환경에서 매우 일반적인 서비스로 정착되어 가고 있으며 방대한 트래픽을 초래한다는 이유로 서비스를 일괄 차단하는 것은 옳지 않다. 따라서 이러한 환경변화에 적응적으로 대처할 수 있는 사용자, 서비스 중심의 보안정책이 필요하다[10].

Ⅲ. 통합 보안정책 수립을 위한 구성요소 분석

대학 캠퍼스 전산망은 기존의 방화벽을 이용한 침입차단/통제 시스템을 기반으로 폐쇄형 시스템과 입시관련 학사업무, 연구 협업, 인터넷 접속 등 개방적 시스템으로 구성되는 특성을 갖는다.

먼저 대학을 구성하는 사용자에 따라 표 1과 같이 교수, 직원, 학생, 전산원 직원, 일반인으로 사용자를 분류할 수 있다.

표 1. 대학 구성원 사용자 구분
Table. 1 User classification in university community

사용자 구분	용도
교수	연구
직원	행정
학생	교육
전산원 직원	업무 개발 및 운영
일반인	인터넷 이용

교수와 직원은 각각 연구와 행정이라는 비교적 제한적인 업무특성을 갖는 사용자로 분류할 수 있다. 학생의 경우 독자적인 PC를 사용하는 대학원생과 실습실처럼 공용 PC를 사용하는 경우로 분류할 수 있지만 학생으로 통합 분류한다. 전산원 직원은 보안 레벨이 다양하고 최고 레벨의 접근이 가능하다. 즉 전산원 직원은 데이터베이스 관리자(DBA: Database Administrator), 서버 관리자, 업무용 프로그래머, 네트워크 관리자, 보안 관리자 등으로 분류할 수 있다. 일반인의 경우는 단지 웹서비스를 허용한다.

표 2. 보호해야 할 보안대상
Table. 2 Security objects to be protected

보안대상
데이터베이스 (학사, 행정, 인사 등)
어플리케이션 (www, E-mail 등)
네트워크 서비스
서버
PC
개인정보

다음으로 보안대상을 정의한다. 표 2는 캠퍼스 환경에서 보호해야할 보안대상을 보이고 있다. 가장 중요한 보안대상은 학사, 행정, 인사 등 데이터베이스와 같은 정보 데이터를 들 수 있다. 또한 대학의 홍보를 위한 메인 홈페이지 서비스의 중단과 같은 사태가 발생하지 않도록 해야 한다. 홈페이지 서비스 중단은 여러 원인이 있을 수 있다. 외부의 해킹에 의한 서비스 중단, 홈페이지 내용 위변조, 분산 서비스거부 공격(DDoS: Distributed DoS) 등의 공격에 의한 서비스 중단, 또는 하드웨어 고장 등에 의해 서비스가 중단될 수 있다. 한편 DNS(Domain Name Server) 해킹과 같은 경우는 모든 전산망 서비스를 중단 시킬 수 있다. 보호되지 않은 PC는 바이러스 감염에 따른 외부 서버를 공격하는 좀비 PC가 되어 있는 경우가 발생한다.

표 3은 캠퍼스 환경에서 널리 적용되고 있는 보안장비를 보이고 있다. IT 기술의 발달과 더불어 다양한 기능은 물론 웹과 같은 어플리케이션 전용의 보안장비(웹방화벽 등)가 출연하고 있다. 캠퍼스 환경에 적절한 보안대상이 정해지고 보안정책이 수립되면 보안장비의 유효한 설치위치와 보호영역을 설정은 예산절감과 더불어 사용자 편리성을 크게 향상시킬 수 있다.

기존에는 보안장비를 단순하게 일렬로 배치하는 경향을 보였다. 특히 최상위 라우터 앞에서 운용되는 방화벽과 같은 장비의 서비스 단절은 방화벽 아래의 서버들의 모든 서비스를 중단한다. 방화벽은 침입차단 역할뿐만 아니라 내부 서버들의 구체적인 사항을 감추기 위하여 NAT(Network Address Translation)기능을 활성화하여 외부의 접근을 차단하기도 한다. 이런 경우를 대비하여 장비의 이중화를 통해 서비스 연속성을 확보할 수 있는 방안을 확보해야 한다.

표 3. 캠퍼스 환경에서 적용되는 보안장비
Table. 3 Security devices applied in campus environment

보호 장비	목적
방화벽	침입 차단
IPS(Intrusion Protection System)	침입 방지
IDS(Intrusion Detection System)	침입 탐지
웹 방화벽	침입 차단
접근통제	침입 차단
DDoS(Distributed DoS)	서비스 관리
TMS(Threat Mgmt System)	위협 관리
ESM(Enterprise Security Mgmt)	통합 관리
좀비탐지	PC 관리
백신	PC 관리
PMS(Patch Mgmt System)	PC 관리
VPN(Virtual Private Network)	접근 관리

그동안 보안을 강화하기 위한 일반적인 접근은 보안장비를 보강하는 정책이었다. 이는 보안체계의 경직성으로 인해 시스템 성능저하의 결과를 초래하는 것으로 알려져 있다[7,11]. 또한 방화벽, IDS/IPS, 웹방화벽, DDoS 방지장비 등을 순차적으로 배치하는 것은 임의 장비의 고장 시 모든 서비스를 중지하는 치명적인 장애 포인트가 되고 있다. 안정적인 캠퍼스 전산망 서비스를 위하여 처리속도, 사용자 편리성 등을 고려한 적절한 보안장비의 배치와 더불어 체계적인 보안정책의 적용이 요구된다. 각종 보안장비의 이중화를 통한 적절한 작업분담(로드밸런싱), 보안장비의 특성을 반영한 프록시로 운영, 그리고 보안장비의 병렬배치 등을 통해 서비스의 중단 없는 보안정책을 운용할 수 있다.

Ⅳ. 캠퍼스 통합 보안정책의 설계

개방된 캠퍼스 환경이 창의적 속성이 강한 다양한 사용자로 구성되는 특성을 고려하면 모든 사용자에게 보안대상으로부터 완벽한 정보보호 서비스를 제공하는 것이 쉽지 않다. 따라서 통합 보안정책 수립을 위해서는 각각의 정보보호 구성요소를 정의하고 이를 기반으로 적용 가능한 보안정책에 대한 설계가 필요하다.

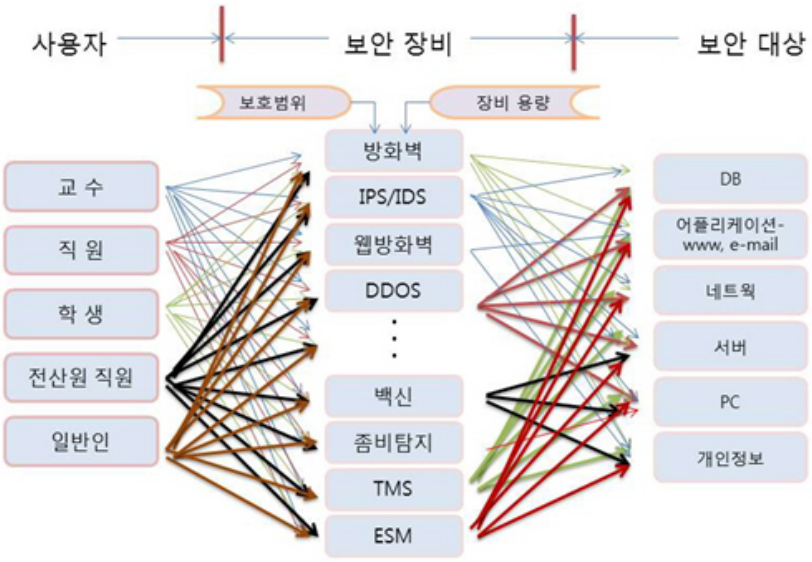

그림 2. 보안 구성요소 사이의 보안정책 사상
Fig. 2 A security policy mapping between the security elements

4.1. 정보보호 구성요소 사이의 보안정책

각각의 사용자가 주어진 보안정책을 인지하지 못할 정도의 편리함을 가지고 IT 서비스를 이용하는 것은 매우 어렵다[12]. 많은 예산과 인력을 투입하는 경우에도 비용만큼 보안위협에 대한 해결책이 제시되는 것은 아니다. 이러한 상황에서 정보보호 서비스를 효율적으로 제공하기 위해서는 캠퍼스 환경 고유의 통합 보안정책이 절대적이다. 그림 2는 본 논문에서 제안하는 캠퍼스 환경에 적응적인 통합 보안정책을 위한 정보보호 구성요소 사이의 개념적인 구조를 나타낸다.

먼저 통합 보안정책을 수립하기 위해 3장에서 정의한 사용자, 보안장비, 보안대상 사이의 보안관계를 정의한다. 각각의 보안관계에 해당하는 보안정책(보안장비, 개인정보 보호 수준, 서비스 속도, 서비스 중단 시 대처방법 등)을 설정한다. 보안정책은 소요예산, 업무의 중요성과 시급성, 법과 제도 등 다차원적인 보안정책 실현 요소를 감안하여 수립해야 한다. 그리고 이런 보안정책에 맞추어 네트워크나 서버의 운영정책을 수정하여 캠퍼스 환경에 적응적인 정보보호 환경을 실현하게 된다.

4.2. 정보보호 구성요소를 기준으로 적용할 수 있는 보안정책의 설계

사용자를 기준으로 하는 보안정책은 가장 보편적인 방법이다. 기본적으로 모든 서비스를 제한하고 특정 사용자에 대응하는 서비스에만 허용하는 형태로 운영된다. 그러나 캠퍼스 환경의 고유 특성으로 인해 소수의 보안 관리자와 많은 사용자 사이에 이러한 정책을 적용하는 것은 불가능하다. 따라서 대부분의 캠퍼스 환경은 기본적으로 모든 서비스를 허용하고 사용자 그룹에 허용되지 않는 서비스를 차단하는 정책을 적용한다. 공개성, 대중성의 특성을 갖는 대학의 연구, 교육 환경을 고려하면 당연한 선택이라 할 수 있다. 표 4는 사용자를 기준으로 적용될 수 있는 보안정책의 예를 보이고 있다. 연구 중심의 교수, 행정 중심의 직원, 교육 중심의 학생, 정보전산원 직원, 그리고 일반인에게 하는 보안정책은 다르게 적용되어야한다. 특히 캠퍼스의 중요한 정보에 접근하고 조작하는 정보전산원 직원의 경우는 더욱 세분화된 정책을 적용할 필요가 있다. 비록 캠퍼스 환경이 공개성을 기본으로 하지만 한편으로는 입시를 비롯한 사회적으로 매우 민감하고 강력한 보안이 요구되는 정보를 처리하고 있기 때문이다. 특히 핵심 데이터베이

스에 대한 접근과 수정은 안전한 인증수단을 이용하여 사용자의 접근을 통제함은 물론 담당자의 업무에 대응하는 역할에 맞게 적용될 수 있는 연산을 제한해야 한다[10,13].

표 4. 사용자를 기준으로 적용될 수 있는 보안정책 예
Table. 4 An example of security policy based on users

사용자	web	e-mail	telnet	ftp	인사 시스템	전자 문서
교수	○	○		○		○
직원	○	○			담장 직원	○
학생	○	○				
전산원 직원	○	○	○	○		○

표 5. 보안장비를 기준으로 적용될 수 있는 보안정책 예
Table. 5 An example of security policy based on security devices

보안장비	역할	대역폭 (bits/s)	설치 위치	적용범위
방화벽 1	IDC 서버	1G	IDC	IDC
방화벽 2	주요 서버	100M	시스템실	시스템
웹 방화벽	웹서버	1G	웹서버 앞	
백신서버	PC 보안	100M		캠퍼스 전체

보안장비를 기준으로 적용될 수 있는 보안정책은 보안장비의 고유의 보안정책을 정확히 이해하고 장비의 성능을 파악해야 하며 적용범위에 따른 적응적인 보안정책을 수립하여한다. 표 5는 보안장비를 기준으로 적용될 수 있는 보안정책의 예를 보이고 있다.

웹 방화벽은 80번 포트를 제어하고 심지어 컨텐츠까지 점검하는 과정에서 많은 부하가 걸린다. 따라서 다수의 인터페이스를 제공하지 않는 것이 고유의 특징이라고 할 수 있다. 이런 장비를 방대한 캠퍼스 네트워크의 맨 앞단에 위치하게 하여 모든 웹서비스를 통제하는 것은 투자에 대비하여 효과도 적고 관리도 어려울 수 있다. 즉 보안장비의 서비스 범위와 역할에 맞는 정확한 보안정책이 필요하다. 보안장비를 기준으로 하는 보안정책은 보안장비의 능력, 위치, 그리고 적용범위에 따라서 해당 장비의 망분리, 추가 보안장비 투입, 설치 위치와 적용범위 등을 조정할 수 있다.

표 6. 보안대상을 기준으로 적용될 수 있는 보안정책 예
Table. 6 An example of security policy based on security objects

보안 대상	방화벽	IPS	웹방화 벽	D DoS	백신	PMS	TMS
DB 서버	○			○			○
웹서버	○	○	○	○			○
mail 서버	○			○			○
네트 워크				○			○
PC					○	○	

보안대상을 기준으로 적용될 수 있는 보안정책은 보안대상이 제공하는 서비스의 성격에 대응하는 보안정책의 수립이 요구된다. 데이터베이스 보안은 단순히 방화벽에 한정하여 보안정책을 수립하기 어렵다. 데이터베이스의 암호화, 전용장비 도입, 로그처리 장비 등을 고려해 볼 수 있다. 표 6은 보안대상을 기준으로 적용될 수 있는 보안정책의 예를 보이고 있다.

단순히 보안장비의 설치 및 확장으로 운영되는 보안정책보다는 네트워크 관리자, 서버 관리자와의 협업을 통해 전산망 운영정책, 전산망 구조변경, 그리고 서버의 운영정책 변경을 통해 적응적인 보안정책을 운영할 수 있어야 한다는 점이다. 예를 들어 망분리 정책, 보안장비의 적절한 위치변경, 사용자의 역할 재정의 그리고 서버의 집중화가 있다.

캠퍼스 전체에 산재해 있는 모든 서버에 방화벽 혹은 웹방화벽과 같은 보안장비를 운영하는 것은 비용에 비해 매우 비효율적이다. 서버를 특정지역에 집중하거나 특정 지역으로 분리하는 집중화 전략의 정보보호 효과는 큰 것으로 알려져 있다[14]. 업무행정 서비스인 인트라넷의 경우 보안을 위하여 망을 물리적 혹은 논리적으로 분리하여 NAT 기반의 사설 IP 주소를 운영할 필요가 있다. 캠퍼스 전체에 일괄적인 보안정책 적용은 예산낭비는 물론 효율성 감소, 사용자 속도저하와 같은 부작용을 동반한다. 그러나 보안정책을 사용자, 보안장비, 보안대상을 기준으로 운용정책을 구분하고 적당한 보안정책을 연결함으로써 적응적이고 효과적인 서비스가 가능하고 궁극적으로 예산을 절감할 수 있다.

4.3. 논의

대부분 캠퍼스의 정보보호 환경은 방화벽을 인터넷 연결 지점에 배치하는 형태로 캠퍼스 전체적인 트래픽 통제함으로써 악성 트래픽을 통제하는 방식을 사용하고 있다. 이는 캠퍼스 내의 서비스에 대한 전체적인 이해와 정보보호 구성요소 사이에 복잡한 정책적 사상관계를 전제로 가능하다. 결과적으로 방화벽을 통한 블랙리스트 IP 주소에 대한 통제만이 이루어지고 있다. 일부 대학에서는 별도의 정보보호 서비스 정책을 적용한 접근정책을 실시하고 있으나 전산망 속도의 저하로 인한 사용자 불만을 야기하고 있다.

효율적인 외부 접근 통제를 위해서는 내부 각 구간에 대해 네트워크를 분리하고 각각의 로컬 방화벽을 구축함으로써 해당 구간에서 서비스되는 정보보호 대상을 보호해야 하며 로컬 방화벽을 위한 관리자가 필요하다. 네트워크 분리에 따른 방화벽 설치는 장비구매와 관리에 많은 비용이 소요된다. 투자비용과 함께 보안정책운용의 효율성을 위해서는 정보보호 대상을 정확히 선택하고 특정 물리적 영역에 유사한 특성을 갖는 정보보호 대상을 집중 배치하는 전략을 적용할 필요가 있다.

V. 결 론

본 논문에서는 개방적인 특성이 강한 캠퍼스 네트워크 환경에서 적응적이고 효율적인 정보보안을 위한 통합보안정책에 대해 논의하였다. 개방된 캠퍼스 환경이 창의적 속성이 강한 다양한 사용자로 구성되는 특성을 고려하면 모든 사용자에게 모든 보안대상으로부터 완벽한 정보보호 서비스를 제공하는 것이 쉽지 않다. 따라서 통합 보안정책 수립을 위해서는 각각의 정보보호 구성요소를 정의하고 이를 기반으로 적용 가능한 보안정책에 대한 설계가 필수적이다.

제안한 보안정책은 캠퍼스에서 이루어지는 서비스의 흐름을 분석하여 보안장비 설치 위치를 적절히 변경하면 보안장비 설치비용 대비 보안효과를 극대화시킬 수 있다. 또한 사용자에게는 보다 빠르고 안정적인 서비스 환경을 제공할 수 있다. 향후에는 정보의 중요도를 반영하여 등급을 구분하고 등급에 따른 세밀하고 정량적인 보안정책 방안에 관해 연구할 계획이다.

REFERENCES

[1] M. G. Kang and S. S. Kim, “Design and Implementation of Security Solution Structure to Enhance Inside Security in Enterprise Security Management System,” *Journal of the Korea Contents Association,* vol. 5, no. 6, pp. 360-367, Dec. 2005.

[2] K. Y. Kim, S. W. Lee, and J. H. Kim, “A Security Monitoring System for Security Information Sharing and Cooperative Countermeasure,” *Journal of the Institute of Electronics Engineers of Korea*, vol. 50, no. 2, pp. 60-69, Feb. 2013.

[3] Y. J. Kim, S. Y. Lee, H. Y. Kwon, and J. I. Lim, “A Study on the Improvement of Effectiveness in National Cyber Security Monitoring and Control Services,” *Journal of the Korea Institute of Information Security and Cryptology*, vol. 19, no. 1, pp. 103-111, Feb. 2009.

[4] KISA, “A Manual of Establishing and Managing a CERT,” KISA Guide, no. 2010-13, Jan. 2010.

[5] Y. T. Kim, O. J. Kwon, J. M. Lee, and T. S. Kim, “Implementation and Design of Policy Based Security System for Integration Management,” *Journal of the Korea Multimedia Society*, vol. 10, no. 8, pp. 1052-1059, Aug. 2007.

[6] G. J. Mun, Y. M. Kim, and B. N. Noh “A Performance Comparison of Network Attacks based on Selecting Statistical Criterion,” *Review of KIISC*, vol. 19, no. 2, pp. 16-25, Apr. 2009.

[7] G. H. Lee and C. G. Lee, “A Risk Evaluation and Real-time Alert Alarm Generation for Responding Cyber Attacks in the Cyber Environment,” *Review of KIISC*, vol. 18, no. 5, pp. 112-124, Oct. 2008.

[8] J. H. Yoo, J. H. Kim, G. R. Kim, and J. C. Na, “A Standardization Status of the Integrated Security Management and Cyber Trace Technologies,” *TTA Journal,* no. 118, Aug. 2008.

[9] Cisco, “Integrated Security Architecture Framework,” White paper.

[10] J. C. Ahn, “A Government Agency Environment Protects Information System Design using Intrusion Prevention System and Role-base Security Policy,” *Journal of the Korea Institute of Information Security and Cryptology*, vol. 14, no. 6 pp. 91-103, Dec. 2004.

[11] H. H. Choi and T. M. Chung, “Study on Generalization of Security Policies for Enterprise Security Management

System," *The KIPS Transactions*, vol. 9, no. 6, pp. 823-830, Aug. 2002.

[12] J. D. Kim, K. W. Kim, and Y. D. Lee, "The Concept and Approach of Convergence Security," *Review of KIISC*, vol. 19, no. 6, pp. 68-74, Dec. 2009.

[13] W. S. Seo and M. S. Jun, "A Study on Building an Optimized Defense System According to the Application of Integrated Security Policy Algorithm," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 21, no. 4, pp. 39-46, Aug. 2011.

[14] W. S. Jang, J. Y. Choi, and J. I. Lim, "A study on method of setting up the defense integrated security system," *Journal of the Korea Institute of Information Security and Cryptology*, vol. 22, no. 3, pp. 575-584, Jun. 2012.

고봉구(Bong-Koo Ko)

1992년 2월 : 전북대학교 전자통신공학과 졸업
1999년 2월 : 전북대학교 컴퓨터공학과 석사
1999년 3월 ~ 현재 : 전북대학교 컴퓨터공학과 박사과정
※ 관심분야 : 컴퓨터통신, 보안, 무선네트워크

박종선(Jong-Seon Park)

2009년 2월 : 조선대학교 전자공학과 졸업
2012년 2월 : 전북대학교 전자정보공학부 석사
2012년 3월 ~ 현재 : 전북대학교 전자정보공학부 박사과정
※ 관심분야 : 대용량데이터전송, 센서네트워크, 무선네트워크, 무선네트워크보안

정성종(Seung-Jong Chung)

1975년 2월 : 한양대학교 전기공학과 졸업
1981년 2월 : 휴스턴대학교 전자공학과 석사
1988년 2월 : 충남대학교 전자공학과 박사
1985년 ~ 현재 : 전북대학교 IT 정보공학과 교수
※ 관심분야 : 인터넷 응용기술, 지능공학

조기환(Gi-Hwan Cho)

1985년 2월 : 전남대학교 계산통계학과 졸업
1987년 2월 : 서울대학교 계산통계학과 석사
1996년 2월 : Newcastle대학교 전산학과 박사
1987년 9월 ~1997년 8월 : 한국전자통신연구원 선임연구원
1997년 9월 ~ 1999년 2월 : 목포대학교 컴퓨터과학과 전임강사
1999년 3월 ~ 현재 : 전북대학교 컴퓨터공학부 교수
※관심분야 : 이동컴퓨팅, 컴퓨터통신, 무선네트워크, 무선보안