

안전한 Ubiquitous-Campus를 위한 학사정보시스템의 종합정보보안 체계 구축에 관한 분석

Analyses of Total Information Security Infrastructure of School Affairs Information System for
Secure Ubiquitous-Campus

김정태, 이준희*,
목원대학교, 세종사이버대학교*

Jung-Tae Kim, Jun-Hee Lee*
Mokwon Univ, SejongCyber Univ.*

요약

차세대의 통신 환경은 디지털들이 통합되는 컨버전스 시대를 맞이하여 인터넷 통신의 환경과 유선망과 무선망과 컴퓨터네트워크 망들이 통합되는 유비쿼터스 환경으로 접어들고 있다. 따라서 현재의 대다수의 교육기관에서는 Intranet을 통한 정보시스템을 구축하고 있으나 유비쿼터스 환경에서 모든 정보는 Extranet을 통해 유무선망을 통해 외부에서 접근 가능한 시스템으로 관리되고 있다. 따라서, 본 논문에서는 유비쿼터스 환경하에서의 학사정보시스템의 설계 방법에 대하여 제안한다.

Abstract

E-learning has increased on importance as people realize that the use of technology can improve the learning process. Consequently, new learning environments have been developed. However, in general they are oriented to address a specific e-learning functionality. Therefore, in most of the cases, they are not developed to interoperate with other e-learning tools, which makes the creation of a fully functional e-learning environment more difficult. We analyses of total information security infrastructure of school affairs information system for secure ubiquitous campus

I. 서론

유비쿼터스 환경에서의 안전한 학사종합시스템을 위한 종합정보시스템의 보안 체계 연구에 관한 연구이다. 현재의 유비쿼터스 시대에는 유선망과 무선망이 통합되고 있으며, 또한, 통신과 방송의 통합화가 가속되고 있다. 이러한 음성 및 데이터의 통합 및 멀티미디어 통합의 실현으로 디지털 컨버전스(Convergence) 환경이 가속화되고 있으며, 사람과 컴퓨터, 사물이 상호 소통하는 네트워킹으로 발전되고 있다. 이러한 유비쿼터스 사회에서는 언제 어디서나 물체의 흐름과 정보의 흐름을 통합할 수 있는 새로운 환경으로 진화가 이루어지고 있다. 현재의 인터넷과 달리 음성망, 방송망이 통합된 차세대네트워크는 지능화된 단말과 결합하여 서비스의 고도화, 지능화, 개인화 등의 특징을 가진 유비쿼터스 환경으로 진화하고 있다. 이러한 유비쿼터스 환경에서 데이터의 수집이 광범위하게 이루어지고, 그 양도 폭발적으로 증가함에 따라 다중, 다량의 데이터가 하나의 시스템에 집중화되는 현상이 심화되고 있다.

또한, 2004년 연말부터 국내 홈페이지의 변조 사고가 급속히 증가되고 있으며, 2005년도 접어들어 급격히 증가하고 있는 실정이다. 홈페이지의 변조 피해업체들은 대부분 한 서버에서 다수의 웹사이트를 관리하는 중소기업의 웹 호스팅 관련

시스템으로, 대부분의 홈페이지 변조의 공격은 해외 해커그룹에 의해 이루어지고 있으며, 홈페이지는 단순한 홍보 목적뿐만 아니라 사이버공간에서 학사정보관리시스템에 접근을 위한 주요 수단으로 자리를 잡고 있다. 또한, 학사관리시스템 내부의 데이터베이스와 연동되어 학교의 자산 및 학생의 정보를 보호하기 위한 대책을 강구하여야 한다. 이러한 웹 애플리케이션의 보안 취약점을 이용한 해킹사고의 증가는 Symantec사의 [Internet Security Threat Report(2004년9월)]에서도 확인할 수 있다. 이러한 안전한 홈 서버를 구축하기 위한 네트워크, 호스트, 애플리케이션 등의 각 계층을 보호할 수 있는 다단계의 보안 기법이 요구되므로 이에 대한 정보보호의 위험 요소를 알아보고 이에 대한 대책을 분석하고자 한다.

따라서 본 논문에서는 기존의 학사정보시스템에 대한 자원관리 관점에서만 이루어지고 있는 시스템을 분석한다. 일반적인 학사정보시스템의 구축 범위는 정보화의 초기단계인 시스템 구축과 데이터베이스를 위한 자료처리, 그리고 관련된 자원만을 대상으로 하였으나, 오늘날과 같은 디지털 컨버전스(Digital Convergence)로 발전함에 따라 유비쿼터스 환경에서는 다양한 정보기술을 활용한 다양한 서비스들이 추가되고

있으며, 그에 따라 이들의 상호 의존성은 증가하고 있는 실정이다. 본 논문을 통하여 안전한 유비쿼터스 환경에서의 학사 정보시스템의 종합정보보안체계를 분석하기 위하여, 대학의 ERP 시스템, 가상강좌 교육 시스템, 사이버대학 시스템, 모바일 포털서비스, 지식경영시스템, 시스템 관리시스템에 대한 정보보안에 대한 요구 분석을 정의하고 해결 방법 및 대책을 제시하고, 추후에 구현되고자 하는 시스템의 규격을 제시하고자 한다.

II. 선행연구

종합학사행정시스템은 각급 교육기관의 학사정보와 행정정보를 구성원이 공유할 수 있도록 운영되는 인트라넷 시스템으로, 일반적으로 학사관리를 포함하여 예산관리, 업적관리, 자산관리, 기자재관리, 구매관리 등이 포함된 대단위 시스템으로 확충, 개발되어 사용되고 있는 일반적인 정보통신 체제의 시스템이다. 대부분의 교육기관에서는 학사 종합정보시스템을 통하여 관리 운영되고 있는 업무로서는 대학의 학사 및 행정에 관련된 대부분의 업무가 포함됨으로써 명실 공히 인트라넷 시스템으로 자리 잡고 있다. 이러한 방대한 정보를 안전하게 관리 운영하기 위해서는 시스템의 모든 사용자에 대한 전체적인 정보보호는 물론 개인정보의 엄정한 관리가 무엇보다도 중요한 사안이다. 정보의 누출 혹은 부정 침입자에 의한 도용으로 빚어질 수 있는 엄청난 침해는 국내외의 여러 사례로부터 이미 잘 알려져 있다. 일반적으로 종합정보시스템의 정보보호 혹은 보안관리를 위한 적절한 제도를 마련하고 고성능의 도구를 도입, 적용해야 하지만, 무엇보다도 개인정보의 보호에 관한 구성원의 인식 확산과 개인의 ID 및 비밀번호의 엄정한 관리가 기본적인 중요한 사안으로 판단된다. 기존의 시스템의 경우 단일 인증 시스템을 통한 종합정보시스템의 접근으로 인하여 시스템 간의 통합 인증시스템으로의 구축이 요구되어지고 있다.

가. 계정관리시스템 운영 현황

- ○ ID 신청과 Plaza, 슈퍼컴퓨터 및 대량디스크 등의 서비스 신청, 패스워드 변경, 사용자 정산 등을 관리
- ID 신청은 교직원(자체직원 포함), 재학생에 한하여 가능함
- ID 신청 가능 인적정보는 신청자가 아닌 시스템에서 자동등록
 - 교직원 및 학생은 통합행정정보시스템의 인사 데이터 베이스에서 동기신호를 받아 인증을 함
 - 자체직원, 타 대학 사용자 등은 계정관리시스템으로 인

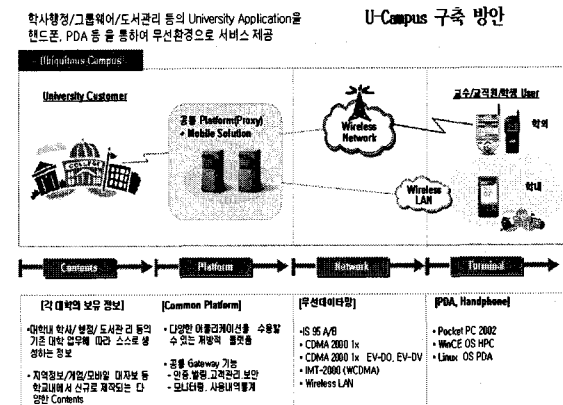
적정보 등록이 가능함

- 계정 관리시스템 기능으로 정보보안에 대한 취약점이 발생함

나. 인증시스템 운영 현황

- 2개 인증시스템을 별도 운영 중이며, 인증정보는 LDAP에 저장하여 각 정보시스템에 대한 통합인증(Single Sign On)과 단독인증을 지원하도록 설계가 되어 있음
- 3가지 유형의 인증 인터페이스를 이용하여 학내 주요 정보시스템 인증지원 가능 여부를 분석
 - SSO 인스턴스는 포털 내 연동된 정보시스템의 통합 인증을 지원하며, 애플리케이션에서 필요한 사용자 정보 제공
 - LDAP1 인스턴스는 ID/PW만으로 인증요청만 처리
 - LDAP2 인스턴스는 ID/PW 기반으로 인증요청 처리 및 애플리케이션에 필요한 사용자 정보 제공

유비쿼터스 환경의 모바일캠퍼스 구성 및 서비스



▶▶ 그림 1. U-Campus 환경에서의 학사정보시스템 구성도

III. 연구의 목적

가. 정보 환경의 변화

- 정보 기술의 발전을 토대로 통합된 인프라를 구축하여 각종 시스템을 통합하는 IT 환경으로 변화가 이루어지고 있음
- 통합된 IT 환경을 지원하기 위한 통합인증관리(SSO : Single Sign On)와 중앙집중적 접근권한관리(EAM : Extranet Access Management)를 통해 사용자 편의 증진 및 관리비용 효율 증대를 기대할 수 있음

나. 사용자 ID 통합, 인증 및 접근제어를 위한 일괄된 관리 체계 수립 필요

- 종합정보시스템의 정보시스템용 사용자 ID를 학내의 모든 정보시스템에서 이용할 수 있는 통합 ID 사용자 기반으로의 확대가 요구되어짐
- 각 종합정보시스템에 대해 사용자 등록에서 삭제까지 인증 및 접근제어를 일괄되게 관리할 수 있는 체계의 수립 및 분석이 필요

다. 학내 인증시스템 통합하여 단일화 필요

- 기존의 정보화포털 및 추후 구축 예정중인 학내 표준 LDAP 구축 시 인증시스템을 구축하여 통합하지 못하고 대다수의 인증시스템 별도 운영 중임
 - 정보화포털 구축 시 대부분이 교육기관에서 도입중인 Oracle SSO 솔루션은 Oracle 제품 외에 타 상용솔루션 및 학내 정보시스템 인증 지원이 용이하지 못하는 단점을 가지고 있음
 - 학내 표준 LDAP 구축 시 개발한 인증인터페이스는 단일 시스템 인증지원으로 보안 및 적절한 접근제어 부족함
- 학내 단위기관 또한 구축 시스템에 따라 개별적으로 구축하여 운영 중이므로 통합 관리가 요구됨
- 인증시스템의 산재는 학내 사용자 불편 초래 및 보안 취약성을 내재할 가능성이 많아 통합 관리가 요구됨

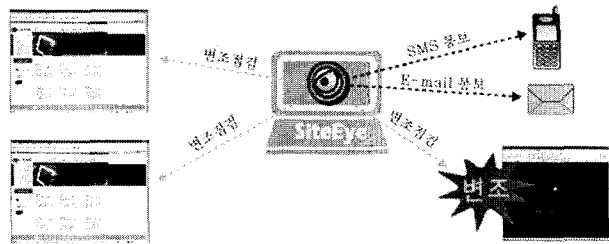
라. 사용자 인증 및 접근제어 보안 강화 필요

- 통합 ID 사용자 인증 체계 강화가 요구됨
 - 통합 ID 사용 대상자가 향후 졸업생 및 일반인까지 확대됨
 - ID/PW 기반의 인증방식 외에 사용자 신분 및 정보시스템의 중요도에 따라 다양한 및 다차원 인증방식 차등 적용 체계 수립이 요구됨
- 애플리케이션들에 대한 접근제어 강화 필요
 - 대다수의 현재 개발되어 사용 중인 인증시스템은 응용 애플리케이션의 사용자 인증 요청 시 필요한 정보만 접근하도록 운영되고 있는 실정임
 - 허용한 정보만 접근하도록 제어하는 통제체계가 미흡하여 요청 이외의 데이터 접근 가능성 존재
- 통합 ID 사용자 체계적인 권한관리 체계 수립 및 강화 필요
 - 웹기반 서비스는 사용자 신분에 따라 서비스 접근 통제 정도로만 제어

- 통합행정정보시스템 클라이언트/서버 프로그램의 경우 직무 및 직제를 혼용하여 관리체계의 구체적인 규정 없이 현재의 상황 및 관행에 따라 권한관리 규칙을 생성하여 업무 담당자를 지정하도록 되어 있어 관리자의 정보보안에 대한 사고가 부족함

- 유비쿼터스 환경에서의 무선 포털서비스를 위한 정보보안 대책 수립 분석
- 웹 페이지 변조 시스템에 대한 요구 분석

해커 등이 불법적으로 시스템에 접속하여 장애를 일으키거나 정보를 유출하는 행위 외에 최근에는 홈페이지 등의 내용을 부적절한 내용으로 변경하는 행위가 자주 발생하고 있다. 그러나, 불법 침입을 알아내기가 쉽지 않으므로 홈페이지를 방문하는 외부 사용자에 의해 먼저 발견된 사례가 많으며, 장애 상황보다 더욱 큰 피해를 입히고 있다. 한국정보보호진흥원(KISA) 인터넷침해사고대응지원센터에 따르면, 2005년 8월 현재 홈페이지 변조사고는 전월대비 174.7%가 증가하고 있으며, 지속적인 피해가 예상되고 있다.

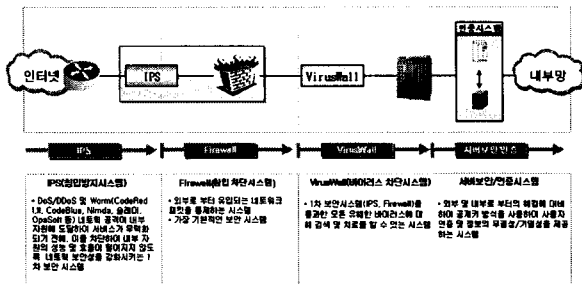


▶▶ 그림 2. 홈페이지 변조시스템 구성도

IV. 정보보안시스템의 구성도

- 유비쿼터스 환경에서의 학사행정망 시스템의 융복합 간의 정합과 정보보호 대책 분석
- 유비쿼터스 환경에서의 유무선 통신망에서의 정보보호 메카니즘 분석
- 통합 ID 사용자 관리, 인증 및 권한관리를 위한 체계 분석
- 사용자 ID 통합 관리를 위한 효율적인 계정관리시스템 구축 방안 분석
- 통합인증 및 권한관리(EAM: Extranet Access Management) 시스템 구축 방안 분석
- 학사행정망의 홈페이지 변조를 방지하기 위한 방법 분석
- 유비쿼터스 환경에서의 포털서비스를 위한 인증 시스템 구축 및 정보보안 대책 분석

정보보안 시스템 전체 구성도



▶▶ 그림 2. 일반적인 정보보안시스템 구성도의 예

V. 기대효과

본 논문을 통하여 안전한 유비쿼터스 환경에서의 학사정보 시스템의 통합구축에 따른 포털 서비스 제공을 위해 안전한 통신이 되기 위한 정보보안 체계에 대한 분석을 통하여, 향후 교육전산망의 효율적인 운용계획과 발전 방향 수립을 위한 기초 자료로 활용이 될 수 있다. 또한, 대학의 정보화 요구에 대한 정보보호의 지침을 수립하고, 학사행정 정보 등의 응용 애플리케이션을 개발하여 정합할 시 용이하게 개발이 될 수 있으며, 전산센터의 개발 직원들의 업무 생산성을 향상시킬 수 있으며, 시스템의 확장성 및 상호 관련성을 지속적으로 유지할 수 있도록 학사행정 정보시스템의 개발에 활용이 될 수 있다. 다음은 그 주요한 연구의 기대효과이다.

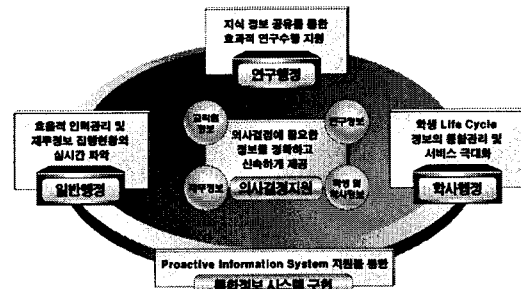
- 통합행정 등의 행정시스템 및 각종 정보시스템 대한 접근 통제 강화로 정보보호 향상을 가져옴
- 학내 단위기관 정보시스템 개발 시 인증 및 권한관리에 대한 비용 및 관리 인력 절감 효과를 가져옴
- 통합 ID 사용자 관리, 인증 및 권한관리를 위한 체계를 수립함
- 학내 각 정보시스템 현황 분석을 통해 통합 ID 사용자 관리체계, 인증체계 및 권한관리 체계 수립함
 - 학의 사용자 ID 관리, 신분변경관리, ID 삭제 등 ID 관리의 원칙 및 기준, 정책관리 및 운영, 정보시스템별 서비스요청 관리 처리 절차 제시
 - 사용자 인증 및 통합인증 대상 시스템 분류와 적용 정책 수립
 - 현 학내 정보시스템에 적용할 수 있는 권한관리의 원칙 및 기준, 적용범위, 정책관리 및 운영, 업무 처리 절차를 제시
- 학내 정보시스템을 위한 사용자 관리, 인증 및 권한관리의 모델을 제시하고, 단계적인 구축 방안을 수립함
- 통합 ID 사용자 인적정보 무결성 유지를 위한 효율적인

방안을 수립함

- 향후 도입 및 구축되는 정보시스템 및 상용 패키지의 인증 및 권한관리를 위한 개발 지침을 제시함
- 홈페이지 변조에 대한 즉각적인 대처를 통하여 사이트 운영기관의 신뢰성을 제고 할 수 있음
 - 관리자 부재 시에도 SMS 등을 통해 즉시 웹페이지 변조 사실을 시스템 관리자에게 알려 줌으로써 신속한 상황 대처가 가능
 - 동시에 여러 사이트에 대한 점검이 가능하므로 중복 관리의 불편함을 해소
 - 원격으로 운영 중인 사이트에 대해서도 중앙 집중적인 관리를 통해 효율성 의 증대를 가져옴

학사/행정 정보 시스템

효과적인 대학 통합 정보시스템 구축



▶▶ 그림 3. U-Campus 환경에서의 통합학사정보시스템 구성도

VI. 결론

차세대의 통신 환경은 디지털들이 통합되는 컨버전스 시대를 맞이하여 인터넷 통신의 환경과 유선망과 무선망과 컴퓨터 네트워크 망들이 통합되는 유비쿼터스 환경으로 접어들고 있다. 따라서 현재의 대다수의 교육기관에서는 Intranet을 통한 정보시스템을 구축하고 있으나 유비쿼터스 환경에서 모든 정보는 Extranet을 통해 유무선망을 통해 외부에서 접근 가능한 시스템으로 관리되고 있다. 이러한 학사관리시스템의 모든 정보는 통합관리시스템으로 융합하여 사용자의 인증을 위한 인증 메커니즘과 외부의 무선 환경에서의 학사정보시스템의 접근에 대한 정보보안 체계를 구축하여 향후 교육전산망과의 정합을 위한 기초 자료로 활용될 수 있다. 또한 학내의 홈페이지 관련하여 시스템의 해킹 등을 확인하고자 하는 방법에 대한 연구가 필요하다.

■ 참고 문헌 ■

- [1] 도용태외 3인, 인공지능-개념 및 응용, 사이텍미디어, 2001.
- [2] 최형일, “감성 인터페이스 에이전트”, 정보과학회지, Vol.18, No.5, pp.36-40, 2000.
- [3] The IPSEC Working Group. Ip security protocol (ipsec) charter. <http://www.ietf.org/html.charters/ipsec-charter.html>.
- [4] The Network Working Group. Point-to-point tunneling protocol(ppp), 1999. RFC 2637.