중소기업정보기술융합학회 논문지 제2권 제2호 pp.43~49, 2012

기업 정보화 서비스를 위한 보안 모델 설계

정윤수[1*]
[1]목원대학교 정보통신공학과

Design of Security Model for Service of Company Information

Yoon-Su Jeong[1*]
[1]Department of Information Communication Engineering, Mokwon University

요 약 최근 기업이 다양한 IT 기술을 기업 업무에 적용하면서 기업에서 처리되는 정보화 서비스의 안전성도 점점 요구되고 있다. 기업에서 요구하는 다양한 IT 기술이 기업의 정보화 서비스에 적용되면서 기업에서 보호해야 하는 정보가 타 기업에 유출되는 보안 사고가 증가하고 있지만 기업의 정보화 서비스 보호에 대한 대응방법이 미흡한 실정이다. 본 논문에서는 기업에서 중요시 되는 정보를 권한별로 분류하여 사용자의 접근제어를 통해 정보 유출과 같은 보안 사고를 줄이기 위한 기업 정보화 보안 서비스 모델을 제안한다. 제안된 모델은 정보에 접근하는 사용자의 권한과 역할을 관리자가 중앙 관리하여 정보에 접근하는 사용자가 이상징후가 포착되면 정보 접근을 차단한다. 또한, 제안 모델은 재난으로부터 기업 정보를 보호하고, 신속하고 체계적인 복구 및 운영 연속성 전략을 수립함으로써 기업의 정보화 서비스 구축에 활용할 수 있다.

키워드 : 기업, 정보화, 보안 서비스, 사용자 인증

Abstract Recently, the safety of being processed in a corporate enterprise with a wide range of IT skills applied to the Corporate Affairs information services are increasing requirement. Businesses that are required by various IT corporate information technology services to companies that need to protect information being leaked to other companies, a security incident has been applied and is growing, but is lacking about how to respond to the protection of corporate information services. In this paper, the information that is important in the corporate authority by the user's access control model to reduce the number of security incidents such as information leakage and security services for enterprise informatization is proposed. The proposed model can be used in order to block the access of the users to access information managed by a central administrator role and the rights of users to access information any abnormality has been captured. In addition, the proposed model can take advantage of protecting corporate information from the systematic recovery and operational continuity strategies to build your company's information services.

Key Words : Company, Information, Security Service, User Authentication

1. 서론

최근 정보화 사회가 진행됨에 따라 기업에서도 정보화 사업이 확산되어 기업 내부 업무프로세스 및 대외서비스 등이 정보시스템을 통해 수행되고 있다. 기업내 정보가 지속 및 확장됨에 따라 기업내 정보시스템의 의존도는 과거보다 더욱 심회되고 있으며 정보 시스템이 중단되는 사태가 발생된다면 기업 전체 업무가 마비될 수

*정윤수(bukmunro@mokwon.ac.kr)
접수일(2012년 11월 10일), 심사완료일(2012년 11월 30일)

도 있는 위험성을 안고 있다[1,2].

기업의 정보화 서비스를 위해서는 독립적인 정보화 관련 부서가 존재하여야 하며, 기업 CEO의 정보화에 대한 의지가 중요하다. 특히, 기업의 정보화 서비스는 기업의 영업 파일 및 개인의 민감한 데이터 파일을 정확하고(무결성) 안전하게(기밀성) 관리되어야 한다. 이러한 사회적 요구사항을 반영하여 기업은 IT 기술 기반의 정보화 서비스를 사용자에게 안전하게 제공하여야 하며 개인 PC나 기업의 서버에 개별적으로 저장해 두었던 프로그램이나 문서의 접근제어를 수행해야 한다.

기업의 정보화 서비스는 기업이 보유하고 있는 기술적인 측면, 정보화를 도입하고 유지하는 경영적 측면, 타 기업과의 전자적인 연계 또는 인증을 위한 사회적 측면, 정부의 제도적 지원 및 각종 규제 등의 정책적 측면에서 서비스 구조가 서로 다르기 때문에 기업 정보의 무결성 및 서버의 인증 문제에 대한 보안 위협에 취약점이 존재한다.[3].

모바일 클라우드 컴퓨팅은 기존 클라우드 컴퓨팅 환경에서 제공되는 자원의 레벨에 따라 IaaS(Infrastructure as a Service), PaaS(Platform as a Service), SaaS (Software as a Service) 모델로 클라우드 서비스가 분류되며, 클라우드 서비스 특성에 따라 가상화, 자원공유 및 집중화, 정보위탁, 단말의 다양성 등으로 분류되어 서비스되고 있다.

모바일 클라우드 컴퓨팅에서는 이동 사용자가 클라우드 컴퓨팅 서버로부터 필요한 자원의 일부 또는 전부를 직접 공급받기 위해서 서버는 클라우드 서비스의 인증 시스템을 활용하여 이동 사용자를 인증하고 있다. 또한, 모바일 클라우드 컴퓨팅은 이동 사용자가 자신의 환경을 간편하게 구성하고 수시로 변경이 가능하다.

본 논문에서는 기업내 정보를 사용자가 안전하게 서비스 받을 수 있도록 기업 정보화 서비스를 사용자 별로 서로 다른 레벨로 안전하게 서비스하기 위한 기업 정보화 서비스 모델을 제안한다. 제안 모델은 기업 정보 서비스를 요구하는 사용자 및 단말이 인증을 요청할 때 사용자별 다양한 접근 보안 정책을 적용할 수 있도록 사전에 역할기반의 접근권한 관리를 수행한다. 또한, 제안 모델은 정보에 접근하는 사용자의 권한과 역할을 관리자가 관리하기 때문에 사용자의 이상 징후에 따른 기업 정보의 접근을 차단한다. 제안 모델은 재난으로부터 기업 정보를 보호하고, 신속하고 체계적인 복구 및 운영 연속성 전략을 수립함으로써 기업의 정보화 서비스 구축에 활용할 수 있으며 사용자의 속성 정보를 이용하여 사용자 인증 전에 서비스를 처리하기 때문에 통신 오버헤드 및 서비스 지연과 같은 통신 장애가 최소화할 수 있다.

이 논문의 구성은 다음과 같다. 2장에서는 기업정보화 개념 및 보안 이슈에 대해서 설명한다. 3장에서는 사용자에게 기업 정보화 서비스의 안정적인 제공을 위한 서비스 모델을 제시하고, 4장에서는 제안 모델에 대한 평가를 분석한다. 마지막으로 5장에서는 이 논문의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

2. 관련연구

2.1 기업 정보화

기업 정보화는 현재나 미래의 활동에 있어서 어떠한 결정에 가치를 주는 자료인 정보가 조직 내에서 유용한 정보를 제공함으로써 일상의 운영, 경영관리, 분석 그리고 의사결정을 지원하는 시스템으로 정의되고 있다[2]. 기업이 정보화 시스템을 유지·보수·관리하기 위해서는 들어가는 비용과 서버의 구매 및 설치 비용, 시간·인력 등의 유지보수 비용 등을 고려해야 한다. 기업내 정보를 PC에 보관할 경우 하드디스크 장애 등으로 인하여 자료가 손실될 수도 있지만 기업의 정보화 시스템을 외부에 둘 경우 저장 공간의 제약을 극복할 수 있는 장점이 있다. 반면 서버가 해킹당할 경우나 제3자의 불법적인 접근으로 기업 정보의 유출 및 파기, 서버 장애 등이 손실될 경우 기업 서비스가 불가능하다는 단점도 있다.

2.2 기업 정보화에 영향을 미치는 요소 분류

기업의 특성 및 여건을 고려하여 기업 정보화는 많은 영향을 받는다. Power et. al[3]과 Raymond[4]는 기업의 정보화에 영향을 미치는 요인들을 [표 1]과 같이 정의하고 있다.

표 1. 기업 정보화에 영향을 미치는 요소[1]
Table 1. Factors affecting the Company informatization

	영향을 미치는 요소
Powers와 Dickson[3]	정보화 도입기
Raymond[4]	시스템 개발 방식
기타	시스템의 운영 종류, 응용업무, 지역(도시 또는 지방)

기업 정보화의 안정적인 서비스를 제공하기 위해서 [1]에서는 [표 2]처럼 평가요소를 독립변수와 종속변수로 나누어 평가 내용을 분류하고 있다.

표 2. 기업 정보화의 평가[1]
Table 2. Evaluation Factors of Company informatization

평가요소	내용
독립변수	· 정보화 경험 · S/W 개발방법 · 시스템 운영방법 · 적용업무의 수 · 컴퓨터 처리 방식 · MIS 부서의 조직 내 위치
종속변수	· 최고 경영자의 참여 · 전산부서 스탭과의 관계 · 전산부서 스탭과의 의사소통 · 전산부서 스탭과의 태도 · 전산부서 스탭의 기술능력 · 변경 요구의 처리 · 공급자(Vendor)의 지원 · 시스템의 응답시간 · 접근의 편리성 · 출력물의 정확성 · 출력물의 시간성 · 출력물의 정밀성 · 출력물의 신뢰성 · 출력물의 적절성 · 시스템에 대한 이해도 · 사용자 참여의식 · 시스템 교육 정도 · 시스템 이용 정도 · 시스템의 정기적 이용정도

2.3 정보화 시스템 분류

기업이 정보화 서비스를 안정적으로 사용자에게 서비스하기 위해서는 기업의 정보화 수준을 컴퓨터 응용분야, MIS 부서의 조직, MIS 계획 및 통제, 사용자의 태도와 능력, 경영층의 인식, DB와 네트워크의 활용 등으로 정보화 서비스 수준을 분류하여 서비스를 제공하여야 한다 [1, 3, 4]. 컴퓨터 응용분야에서는 타사와의 상대적 수준, 경쟁적 우위 시스템 개별 여부, 전사원의 업무(시스템) 통합화, 정보시스템 출력 정보 활용 수준, 고생산성도구 활용 여부 등으로 분류하여 서비스한다. XIS 부서의 조직에서는 조직 내 위치, 조직 내 역할 수준, MIS 부서의 참여 수준, 정보센터 조직 구성 여부, MIS 부서 업적 평가 수준, 전산 요원 수 및 기술력 확보, 개인별 기술관리 수준, 기술 및 업무 습득 교육, MIS 부서의 전문교육, MIS 부서의 역할 변화 등으로 분류하여 서비스한다. MIS 계획 및 통제에서는 정보시스템 중장기계획 구성, 정보시스템 단기계획 구성, 시스템 개발 우선 순위 구성, 시스템 감사 실시 여부, 시스템 용량계획, 프로젝트 관리 기준 운용, 업무의 표준화 구현, 시스템 효과 측정 등으로 분류하여 서비스한다. 사용자의 태도와 능력에서는 시스템 계획 입안에 사용자 참여, 시스템 개발에 사용자 참여, 데이터 발생 즉시 사용자 입력, 사용자의 적극적인 컴퓨터 활용, 신규개발 비용에 대한 사용자 인식, 일반 사용자 전산 수준, 사용자 전산교육 실시, 정보전략, 시스템 교육 수준, 사용자간 의사소통의 갭, 정보시스템을 통한 직무 연계 적극성 등으로 분류하여 서비스한다. 경영층의 인식에서는 최고경영진의 사업전략 명시, 기업의 조직 풍토, 정보시스템에 대한 경영자의 인식, 정보총괄임원 구성, 정보시스템의 정보전략 활용, 임원의 정보시스템 정기적인 교육, 실질적인 의사결정 수준, 정보시스템 부서 출신자의 임원 승진 여부, 정보시스템의 조직기능 개선 시기 적절성 등으로 분류하여 서비스한다. DB와 네트워크 활용에서는 기업 내 네트워크 실현, 기업 간 네트워크 실현, 네트워크 운용관리 체계, 데이터베이스 공개, 외부 데이터베이스 활용 수준, 데이터베이스 통합화 추진 부서 구분, 부서간 정보교환 수준, 그룹웨어 통합 진행 수준 등으로 분류하여 서비스한다.

3. 사용자 속성 기반의 기업 정보화 서비스 보안 모델 설계

이 절에서는 기업에서 중요시 되는 기업 정보를 사용자별 권한을 통해 사용자의 기업 정보 접근을 제어하여 기업 정보 유출과 같은 보안 사고를 줄이기 위한 기업 정보화 보안 서비스 모델을 제안한다.

3.1 보안 요구사항

기업의 중요 정보를 안전하게 보호하기 위한 기업 정보화 서비스의 보안 요구사항을 정리하면 [표 3]과 같다. 기업 정보화 서비스를 원활하게 운영하기 위해서는 [표 3]과 같은 보안 요구사항의 신뢰성과 타당성을 저해하는 항목을 배제하고 기업 정보화 서비스에 적합한 항목이 필요하다.

표 3. 기업의 보안 요구사항[5]
Table 3. Security Requirement of Company

항목	내용
IT 능력	변화와 요구에 적응할 수 있는 조직이 보유한 IT 자원 및 기술의 정도
조직 민첩성	조직이 시장/환경/고객요구의 변화에 빠르게 적응하고 반응하는 정도
조직원의 참여	조직 구성원의 정보보안정책 준수 및 보안행동의 정도
보안위험 경험	조직 내 보안 관련 문제 발생 경험의 정도
경쟁정도	기업이 참여하고 있는 산업 내 경쟁의 정도
파트너 의존도	파트너/협력기업들간의 기술적, 전략적 의존정도
IT 강도	산업 내 기업들간의 IT 활용도 및 혁신적 기술 도입의 정도
IT 불안정성	IT 기술의 빠른 발전과 변화의 정도
보안위험 관리인식	조직 구성원들의 보안위험관리의 중요성과 필요성에 대해 인식 정도
보안위험 관리 개발의지	조직의 보안위험 관리 강화를 위해 필요한 보안설계 등의 개발에 대한 의사결정 및 의지 정도
보안위험 관리수행	조직이 보안위험관리와 관련된 활동의 실행정도

기업 정보화 서비스 환경에서의 보안 문제는 [그림 1]과 같다. 기업 정보화 서비스는 [그림 1]처럼 사용자가 모바일 기기를 사용함으로써 상호호환성 이식성 및 불법 저작권 사용 문제, 이종 콘텐츠 융합 및 공급문제, 기기 인증 및 디지털 콘텐츠 저작권 문제 발생 등의 보안 문제가 발생 가능하며, 상호호환성 이식성 및 불법 저작권 사용 문제에서는 사용자가 사용하는 다양한 스마트 기기와 콘텐츠들은 모바일 클라우드 환경에서 안전하게 서비스를 제공하기 위해서 콘텐츠의 유통과 공유를 개인 및 사업자간 디지털 콘텐츠의 저작권 보호가 필요하다[4,5].

이종 콘텐츠 융합 및 공급문제에서는 단말들을 연계하여 컨텐츠를 제공하도록 디바이스의 접근 제어 기술이 필요하다. 모바일 환경에서 기기 인증 및 디지털 콘텐츠 저작권 문제에서는 서로 다른 기기를 사용하는 사용자를 모바일 클라우드 시스템의 인증서버에서 사용자의 역할 및 권한에 따라 컨텐츠 서비스를 제한하도록 인증을 수행해야 한다.

3.2 기업 정보화 서비스 모델 설계

기업의 정보화 서비스 모델은 [그림 2]와 같다. [그림 2]처럼 기업 정보화 서비스 모델은 외부 사용자가 기업의 정보를 제공받기 위해서 사용자와 서버 사이에 서비스 접근 보안 엔진을 통해 사용자의 권한 및 등급에 따라 서비스를 제공받는다. 접근보안은 사용자에 대한 신뢰성과 접근성을 통해 사용자의 개인정보 속성을 인증서버와 데이터베이스 사이에 저장되어 있는 정보의 비교분석을 통해 수행된다. 제안 모델에서 기업 정보를 관리하는 서버는 사용자를 인증하기 위해서 인증 서버에게 사용자의 인증정보를 확인하는 것이 아니라 접근 보안 엔진 내 데이터베이스에 저장되어 있는 사용자의 개인속성 정보의 인증 유·무를 통해 서비스 제공 여부를 확인한다. 이 과정을 통해 제안 모델에서는 프록시 기능을 통해 인증 서버의 오버헤드와 컨텐츠 서버의 서비스 지연을 최소화하는 효과를 얻는다.

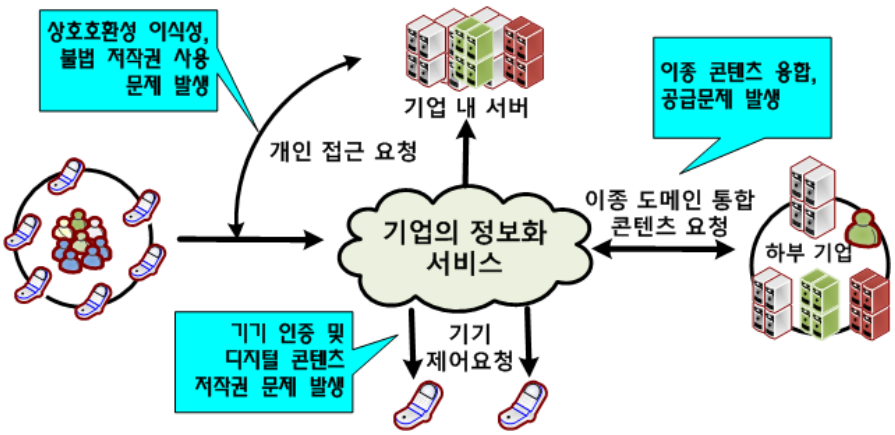

그림 1. 기업 정보화 서비스 환경에서의 보안 문제
Fig 1. Security Problem in Company Information Service Environment

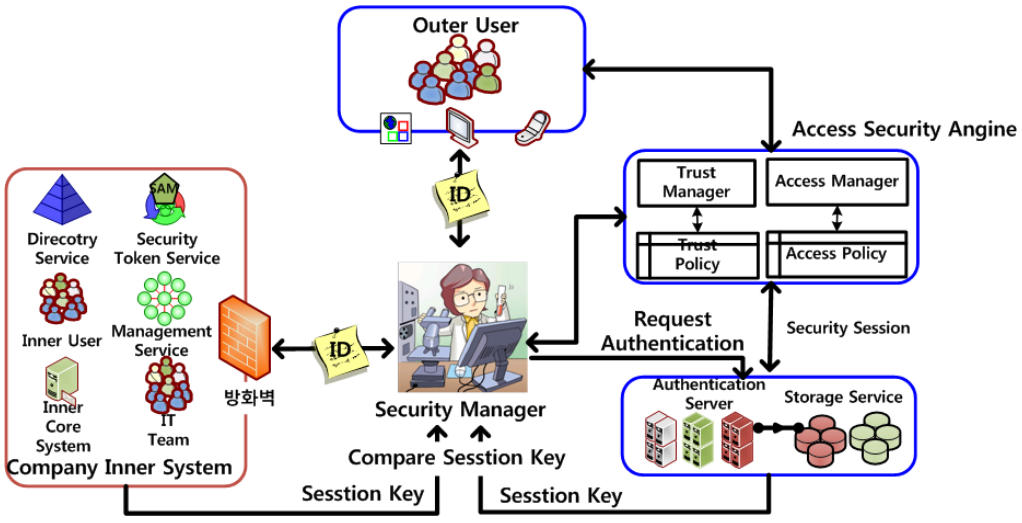

그림 2. 역할기반과 개인속성기반의 기업 서비스 보안 서비스 모델
Fig 2. Company Service Security Service Model based on RBAC and Personal Info.

표 4. 개인 속성 정보
Table 4. Personal Property Information

GID	*ID*	*AI*	*Time*	AIP	*GI*

표 5. 접근 관리 보안정보
Table 5. Access Management Secuirty Information

ID	*Grade*	*Time*	*PI*	*DI*

제안 모델에서는 기업 정보의 서비스 시간을 최소화하기 위해서 내·외부의 사용자가 기업 정보 시스템에 접근할 때마다 접근 보안 엔진을 통해 사용자의 권한 및 신뢰 등급을 확인하여 서비스 제공 유·무를 판단한다. 기업 정보 시스템에 접속한 사용자는 [표 4]처럼 접근 보안 엔진 내 사용자의 속성 정보를 이용하여 사용자와 인증서버내 저장되어 있는 사용자의 속성 정보화 비교분석을 통해 사용자의 신뢰성을 평가한다.

사용자의 개인 속성 정보는 [표 4]처럼 그룹정보, 사용자 인식자, 동기화 정보, 시간정보, 인증 확률 정보, 그룹 정보 등으로 구성된다.

*GID*는 개인 사용자가 속한 기업 그룹 인식자를 나타내고, *ID*는 사용자의 개인 인식자 정보를 나타낸다. *AI*는 인증서버와 동기화 유·무를 나타내는 정보로써 동기화가 정상적으로 수행되면 1, 정상적으로 수행되지 않으면 0으로 나타낸다. *Time*은 사용자가 기업 정보화 서비스를 요청한 시간을 나타내고, *AIP*는 사용자가 인증서버로부터 부여받은 인증 확률 비율로써, 이 값은 기업 정보 시스템에서 비정상적인 사용자의 접근을 제한하는 역할을 담당한다. GI는 현재 사용자가 속한 기업 정보화 서비스 그룹 정보로써, 사용자의 활동내역 정보를 나타낸다.

[표 5]은 기업 정보 서비스에 접근하는 사용자의 안전성을 보장하기 위한 접근 보안 엔진의 보안 정보를 나타낸다. [표 5]의 보안 접근 관리 정보는 사용자의 위치와 역할에 따라 기업 정보 서비스의 접근 제어를 체크하도록 사용자 인식자, 사용자 권한등급, 시간, 사용자 퍼미션 정보, 사용자 정보 즉 이동 기기, 유·무선 등 기업 정보 서비스에 접근하는 장비 정보 등으로 구성된다. 각 정보를 구체적으로 살펴보면, *ID*는 사용자의 인식자를 나타내고 *Grade*는 사용자의 권한 등급을 나타낸다. *Time*은 사용자가 기업 정보 서비스를 요청한 시간을 나타내고, *PI*는 사용자의 퍼미션 정보를 나타낸다. *DI*는 사용자 이동 기기의 정보를 나타낸다.

4. 평가

4.1 보안평가

4.1.1 프라이버시 예방(Privacy Protection)

제안 기법에서는 기업 정보를 사용자에게 서비스하기 전에 인증서버를 통해 사용자의 권한 정보를 사전에 수집하여 사용자가 기업 정보 서비스에 접근할 수 있는 지

에 대한 판별을 먼저 수행한다. 제안 기법에서는 사전에 등록된 사용자 정보를 이용하여 세션키를 생성하여 사용자와 관리자가 서로 독립적인 세션키를 공유함으로써 제3자가 불법적으로 기업 정보를 남용하지 않도록 하고 있다. 또한, 사용자와 관리자 사이에 각각 사전에 랜덤 값을 생성하여 인증서버에 등록할 때 사용자의 관리자의 랜덤 값을 비교분석하여 동기화하기 때문에 매 세션마다 보안 접근을 통한 사용자의 프라이버시가 보장된다. 만약 제 3 자가 동기화된 세션키를 유추하더라도 독립적으로 서로 공유된 세션키를 모두 추출하지는 못하고, 사용자의 인식자 ID를 해쉬함수 $h()$에 적용하여 익명의 인식자 AID를 생성하기 때문에 공격자가 특정 사용자를 식별할 수 없어 사용자의 프라이버시를 보장받는다.

4.1.2 정보노출방지

제안 기법에서는 기업의 정보노출을 방지하기 위해서 사용자의 서비스 요청때마다 관리자는 랜덤수를 생성하여 사용자의 익명 인식자 AID을 해쉬함수 $h()$에 적용한다. 관리자와 사용자의 정보 동기화를 위해 관리자는 사용자의 신원정보를 요청할 때마다 사용자와 관리자가 선택한 서로 소인 p와 q를 매번 생성하여 SI정보를 생성한다. 만약 제3자에 의해 기업의 서비스 정보가 노출될 경우 제3자는 사용자의 신원정보를 획득하여야만 한다. 그러나, 제안 기법에서는 제3자가 불법적으로 세션키를 유출할 수 없도록 사용자의 권한 및 역할에 따라 접근권한을 부여하여 매번 세션키를 생성하도록 하기 때문에 기업의 서비스 정보 노출을 사전에 예방할 수 있다.

4.1.3 재사용 공격

제안기법에서는 사용자가 관리자에게 기업 서비스를 요청할 경우 관리자는 사용자의 기업 서비스 요청을 처리하기 위해서 접근 보안엔진내에 저장되어 있는 사용자 정보를 검사한다. 제안기법에서 사용자의 권한 및 접근을 제어하기 위해서 접근 보안엔진은 제3자가 재사용 공격을 할 경우 관리자가 접근 보안엔진을 통해 사용자의 정보를 수집하여 기업 정보를 불법적으로 수집할 수 있다. 특히, 기업 정보 시스템에서는 사전에 등록된 사용자와 관리자의 랜덤수를 조합하여 세션키를 생성함으로써 제3자에게 도청되더라도 안전성을 보장받게 된다. 제안 기법은 관리자로부터 전달받은 기업 서비스 정보 중에서 임의의 한 개 원소를 추출하여 세션키를 생성하는데 사용되기 때문에 사용자와 관리자 사이에 서로 검증하기 때문에 재사용 공격에 안전하다.

4.2 성능평가

4.2.1 환경설정

이 절에서는 접근 보안 엔진을 통하여 사용자의 역할에 따른 인증서버의 오버헤드와 지연시간에 대해서 기존 기법과 비교 평가한다.

표 6. 실험 환경
Table 6. Experimental Environment

환경 변수	값
사용자(모바일 기기) 수	1,000
동시 최대 인식수	100
실험시간	3600 s
버퍼 크기	50 packet/s
패킷 드롭 확률	0.01
데이터 패킷 크기	100 bytes
쿼리 패킷 크기	25 bytes
헤더 패킷 크기	25 bytes

4.2.2 실험결과

[그림 5]는 접근 보안 엔진을 통해 기업 정보화 서비스를 제공받는 사용자의 지연시간을 기존모델과 비교평가하고 있다. 실험 결과, 제안 모델은 사용자 및 관리자의 역할에 따라 인증 정보를 기업 정보화 서비스 전에 접근 보안 엔진을 통하여 사전에 확인 및 처리하기 때문에 지연시간이 5.5% 향상된 결과를 나타내고 있다.

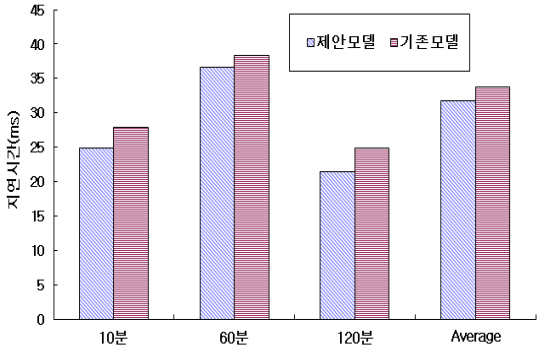

그림 5. 인증 지연시간
Fig 5. Delay Time of Authentication

[그림 6]은 사용자 수에 따른 인증서버의 오버헤드를 제안 기법과 기존 기법을 비교하고 있다. 실험 결과, 제안 기법은 접근 보안 엔진을 통하여 사용자의 권한 속성 정보를 통해 사용자 보안 인증을 사전에 수행하기 때문에 기존모델보다 인증서버의 오버헤드가 13.7% 낮게 나타내고 있다.

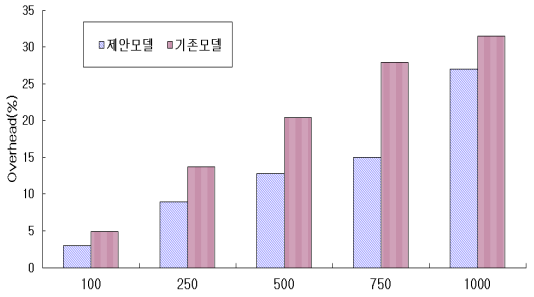

그림 6. 사용자 수에 따른 인증서버의 오버헤드
Fig 6. Overhead of Authentication Server through Number of User

5. 결론

최근 정보화 사회가 진행됨에 따라 기업에서도 정보화 사업이 확산되고 있다. 본 논문에서는 기업내 정보를 사용자가 안전하게 서비스 받을 수 있도록 기업 정보화 서비스를 사용자 별로 서로 다른 레벨로 안전하게 서비스하기 위한 기업 정보화 서비스 모델을 제안하였다. 제안 모델은 정보에 접근하는 사용자의 권한과 역할을 관리자가 관리하기 때문에 사용자의 이상 징후에 따른 기업 정보의 접근을 차단함으로써 지연시간과 오버헤드를 낮추었다. 실험 결과, 지연 시간은 기존 기법보다 5.5% 향상하였고, 사용자 수에 따른 인증서버의 오버헤드는 13.7% 낮게 나타났다. 향후 연구에서는 제안된 모델을 실제 환경에 적용할 수 있도록 구현하여 성능평가를 수행할 계획이다.

참 고 문 헌

[1] 하대용, 조용길, “중소기업 정보화 수준 측정 및 측정요인에 관한 연구 : 충북지역 제조업체를 중심으로”, 한국 중소기업학회, 25권 4호, pp. 201-225, Dec. 2003.

[2] 이진주 외, “사용자를 위한 경영정보시스템”, 다산출판사

[3] R. F. Powers and G. W. Dickson, “MIS Project Management : Myths, Opinions and Reality”, California Management Review, Vol. 15, No. 3, Spring, 1973.

[4] L. Raymond and N. Magnenat-Talmann, “Information Systems in Small Business : Are They Used in Managerial Decision?”, American Journal of Small Business, Vol. 6, No. 4, pp. 20-26, Apr. 1982.

[5] 김상현, 송영미, “기업의 정보시스템 보안위험관리 인식 및 개발의지에 영향을 미치는 내외부적 요인에 관한 연구 : 기술의존성 정도에 따른 차이분석”, 2012년 한국경영정보학회 & 한국정보시스템학회 춘계공동학술대회, Vol. 2012, No. 1, 2012년.

저 자 소 개

정 윤 수(Yoon-Su Jeong) [정회원]

- 1998년 2월: 청주대학교 전자계산학과 학사
- 2000년 2월 : 충북대학교 전자계산학과 석사
- 2008년 2월 : 충북대학교 전자계산학과 박사
- 2012년 3월 ~ 현재 : 목원대학교 정보통신공학과 조교수

<관심분야> : 유·무선 보안, 암호이론, 정보보호, Network Security, 이동통신보안