Smartwork System을 위한 정보보호연구

천재홍* · 박대우**

*호서대학교 벤처대학원

Information Security Research for Smartwork System

Jae-Hong Cheon* · Dae-Woo Park**

*HOSEO GRADUATE SCHOOL OF VENTURE

E-mail : jhcheon@kei.re.kr, prof_pdw@naver.com

요 약

Cloud Computing시대가 도래하였다, 중요 자료는 Clouding하고, 단말기에 한정 받지 않고, 정보를 처리할 수 있다. 최근 Cloud와 Mobile의 접속으로 업무환경이 개선되고, 의사결정이 즉시적으로 이루어지고 있다. 하지만, 정부의 중요한 의사결정과 같은 경우에는 보안성이 필요하다. 본 논문에서는 IoT, Cloud, Bigdata, Mobile을 적용한 Smartwork System에서 네트워크 접근 및 통제를 연구한다. DB정보에 접속할 때의 인증, 권한, 보안 Level 별로 보안등급 서비스를 연구한다. 본 논문의 연구는 Smartwork System을 위한 정보보호로서 공공기관, 중요정보기관의 정보처리 및 의사결정시스템 설계 및 구축의 기초자료로서 이용될 것이다.

ABSTRACT

Computing loud arrival times were, important data Clouding and, without being limited to the device, may process the information. Recently, work environment and improved access to Cloud and Mobile, this decision has been made to take effect immediately. However, when such important decisions of the government, the security is required. In this paper, we study the network access and control in IoT, Cloud, Bigdata, Smartwork System applied to Mobile. Study the authentication, authorization, and security for each security level Level of Service to connect to the DB information. Research of this paper will be used as the basis for the information processing and decision-making system design and construction of public institutions and agencies as important information for the protection Smartwork System.

키워드

Smartwork, 정보보호, 망분리, 가상화

Ⅰ. 서 론

Cloud Computing시대가 도래하였다, 중요 자료는 Clouding하고, 단말기에 한정 받지 않고, 정보를 처리할 수 있다.

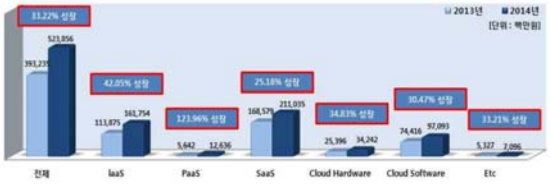

그림 1. 클라우드 모델별 매출액 증감 현황

특히 최근에 모바일 환경의 스마트단말기는 화면의 크기가 커지고, CPU 성능과 Memory 용량이 늘어나면서 다양한 업무에 활용할 수 있는 가용성이 높아졌다. Cloud와 고성능 Mobile 스마트 단말기의 활용을 통해 업무 수행환경이 개선되고, 신속한 의사결정이 가능하게 되었다.

하지만, 정부 등과 같은 기관에서의 중요한 의사결정과 같은 경우에는 보다 높은 보안성을 유지할 필요가 있다.

본 논문에서는 IoT, Cloud, Bigdata, Mobile을 활용된 Smartwork System에서 네트워크 접근 및

통제를 연구하고, DB정보에 접속할 때의 인증, 권한, Level별 보안등급 서비스를 연구한다.

본 논문의 연구는 Smartwork System을 위한 정보보호로서 공공기관, 중요정보기관의 정보처리 및 의사결정시스템 설계 및 구축의 기초자료로서 이용될 것이다.

II. 관련 연구

안전한 Smartwork System 구축을 위해 필요한 망 분리, 정보보호시스템, 스마트단말기, 가상화 등 제반 기술과 관련된 연구를 한다.

2.1. 망 분리

망 분리는 인터넷 망과 내부업무 망 분리를 통해 사이버 보안위협에 효과적으로 대응하기 위한 방안이다.

망 분리된 환경에서 내부망 전산장비의 인터넷 접속은 완전하게 차단되며, 망간 자료전송시스템을 통해 제한적으로 인터넷에 접속할 수 있다.

망 분리 방법에는 물리적 망 분리, 논리적 망 분리로 구분할 수 있으며, 논리적 망 분리는 CBC 방식과 SBS방식으로 구분된다.

- 물리적 망 분리

물리적 망 분리는 침입차단시스템, 침입방지시스템 등과 같은 정보보호시스템을 인터넷망과 내부 업무망에 독립적으로 설치 운영하고, 사용자는 두 대의 단말기로 각각 인터넷 망과 내부업무 망을 사용하여야 한다.

- 논리적 망 분리

논리적 망 분리는 인터넷 망 또는 내부업무 망을 가상화 기술을 사용하여 한 대의 단말기에 구축하여 사용하는 방법이다.

논리적 망 분리 방식은 PC가상화(CBC), 서버 가상화(SBS)로 구분할 수 있다.

2.2. 정보보호시스템

침입차단시스템, 침입방지시스템, 유해사이트차단시스템, 서비스거부공격 차단시스템, 안티바이러스시스템 등 정보보호시스템을 인터넷 망과 내부업무 망에 각각 독립적으로 설치하여 사이버보안 위협에 대응하여 안전한 업무환경을 제공하여야 한다.

2.3. 스마트단말기

ICT 기술의 발달에 따라 고성능 CPU, 대용량 Memory가 탑재된 단말기로, 기본적인 음성통신 외에도 무선을 이용한 인터넷 접속이 가능하고, 사용자가 필요로 하는 다양한 어플리케이션을 설치할 수 있는 단말기 이다.

2.4. 가상화(Virtualization)

가상화는 충분한 CPU, Memory 등의 자원을 탑재한 전산장비의 가용성을 최대한 활용할 수 있도록 하는 기술이다.

탑재된 자원을 이용하여 가상의 서버, 스토리지를 논리적으로 만들어 활용함으로써 전산장비의 효용성을 높일 수 있다.

2.5. Smartwork System

Smartwork System은 무결성, 가용성, 부인방지 등 보안성이 강화된 환경에서 단말기 및 시간과 장소등과 같은 물리적 환경에 따른 장애를 최소화하여 신속한 의사결정을 행위하기 위한 시스템이다.

III. Smartwork System의 보안설정 설계

3.1 사용자에 대한 보안 Level 설정

조직에서는 업무의 권한과 직책에 따라 업무의 범위와 내용에 대한 접근을 통제한다. 따라서 사용자의 직책이나 책임에 맞는 권한과 가용성에 따른 보안레벨을 설정하여야 한다.

데이터베이스 접속에 대한 권한을 부여하고, 가용성에 맞도록 보안 Level을 설정한다.

보안 Level은 개인정보보호법이나 정보통신망 관리법과 관련 보안규정에 따라 설정하고, 시스템의 관리적, 기술적, 물리적, 인적 보호조치를 수행하여야 한다.

정보시스템과 정보자산의 안전한 보호를 위한 계획 수립 후 각 사용자에 대한 보안Level에 의한 접근통제와 권한을 설정하고, DB의 수정 실행, 저장 권한에 대한 등급을 부여한다.

3.2 Smartwork System의 보안설계

데이터베이스 접근과 권한에 따른 읽기, 쓰기 등을 수행하고, 수행된 정보를 로그 기록에 남겨 접근통제와 권한에 따른 수행 등을 감사할 수 있는 감사기록을 남기도록 설계한다.

또한 정보시스템에 대해 관리적, 기술적, 물리적, 인적 보호조치를 수행 할 수 있도록 설계를 한 후 CEO, CISO의 통제에 따라, 사용자 전체에게 공지를 한다.

이와 함께 개인정보에 관한 수집 및 이용목적에 대한 동의 절차를 마련하고, ISMS 인증을 위한 보안설계와 함께 중장기 전략을 마련한다.

3.3 네트워크 접근 및 통제 설계

정보자원 시스템의 관리적, 기술적, 물리적, 인적인 보호조치를 효과적으로 수행할 수 있도록 네트워크 보호조치를 설계한다.

침입차단시스템, 침입방지시스템, 침입탐지시스템, 네트워크 모니터링시스템, 라우터 등에 대한 각각의 보안설정을 통해 정보시스템 및 정보보호시스템에 대한 접근통제 등의 정보보호 조치를 수행한다.

네트워크 접속에 관한 로그 감사기록과 실시간 접근통제를 위한 접속차단 및 제어 정책을 설계

한다.

3.4 인증, 권한, 보안서비스 설계

조직의 관련 규정에 따라 사용자와 이해 관계자들에 대해 관리적, 인적 정보보호 조치를 설계하고, 관련 정보시스템에 대한 기술적, 물리적, 관리적 정보보호 조치를 설계한다.

정당한 사용자의 직책과 권한에 맞는 접근과 통제 및 안전한 인증을 위해 이중인증 체계를 설계하고, 접속정보의 노출을 방지할 수 있도록 전송구간과 데이터베이스의 접속정보는 관련 규정에 따라 암호화조치 하도록 설계한다.

또한 개인정보의 보호를 위해 사용자와 정보처리관리자의 수행 계획과 전략을 책정한다.

Ⅳ. Smartwork System의 보안구축

4.1 Smartwork System의 인증, 접근통제 설정

인터넷을 통해 접속하는 사용자의 권한 확인을 위해 아이디, 패스워드 및 PKI, OTP 등의 추가적인 인증도구를 사용하여 정당 사용자 유무를 검증한다.

또한 접속정보 유출 등과 같은 보안 위협에 대응하기 위해 사용자 접근정보는 암호화 통신함으로써 접속정보 유출에 따른 보안위협에 대응한다.

정당한 권한이 있는 사용자라 할지라도 5회 이상 비밀번호를 잘못 전송한 경우 보안성 유지를 위해 접속을 강제 차단조치하고, 운영자에 의해 해제 될 수 있도록 한다.

인증 후 시스템에 접속한 사용자는 업무 권한 및 범위, 직책에 따른 부여된 보안 Level에 따라 정보시스템을 사용할 수 있다.

4.2 Smartwork System 보안구축 Model

정당한 권한을 갖고 있는 사용자는 인터넷에서 노트북 등 휴대용 단말기 또는 스마트단말기를 통해 망 분리된 조직에 구축된 독립된 인터넷 망으로 접속한다.

인터넷 망에 접속한 사용자는 이중 인증 등을 통해 정당한 사용자임이 확인된 후, 침입차단시스템, 침입방지시스템, 침입탐지시스템 등 정보호호 시스템을 경유하여, 내부업무 망에 접속한다.

내부업무 망에 접속된 사용자는 업무 범위, 업무 권한 및 직책에 따라 할당된 보안 Level에 따른 사용권한에 따라 내부 데이터베이스 및 정보시스템을 이용하게 된다.

인터넷 망과 내부업무 망간 자료 및 데이터 교환은 TCP 기반이 아닌 국가정보원 인증을 받은 별도의 프로토콜을 사용하는 자료전송시스템만을 사용한다.

사후 감사를 위해 인증 정보와 내부업무 망 접속 정보 및 정보보안 Level 권한에 따라 수행된 정보를 로그 기록하여 접근통제와 권한에 따른 수행 등을 감사기록시스템에 기록한다.

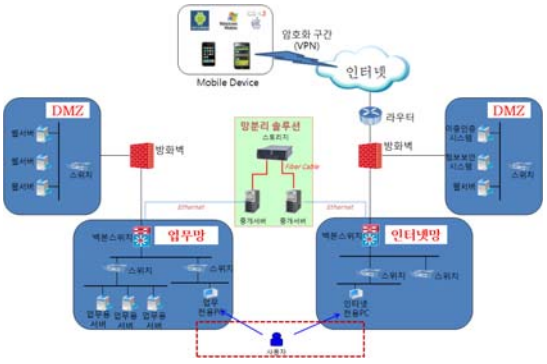

그림 2. 물리적 망 분리 모델

Ⅴ. 결 론

내부 자료유출을 방지하고, 다양한 사이버보안 위협에 대응하기 위해 공공기관, 주요정부기관 및 금융기관들이 망 분리 사업을 진행하였다. 인터넷 망과 내부업무 망의 분리로 의사결정권자들의 신속한 의사결정이 곤란한 상황이 발생하고 있다.

본 논문에서는 정당한 사용자가 노트북 등 휴대용단말기와 스마트단말기 등을 이용하여 망 분리로 인한 의사결정 장애 및 업무불편을 극복하여, 인터넷을 통해 내부업무 시스템에 접근하여 업무를 수행할 수 있는 Smartwork System을 구축하였다.

Smartwork System에는 악성코드로 인한 내부 자료 유출 및 파괴를 방지하고, 사이버보안 위협에 대응하기 위해 정당한 사용자 인증을 위한 이중인증 체계, 정보보안시스템 구축, 접속구간 암호화, 접속정보 및 수행 정보의 로그 기록을 통한 감사시스템을 설계하였다.

향후에는 물리적 망 분리 상태에서의 이중인증 체계 구성, 자동 권한 Level 설정 및 가상화 기술을 활용하여 사용자 단말기를 통한 정보유출 차단 방안을 연구할 계획이다.

참고문헌

[1] 민영기, 유명호, 한승한, 전한구, 이영석, “2014년 클라우드 산업 실태조사 결과 요약보고서”, 정보통신산업진흥원, pp.14, 2016년3월

[2] 이기홍, 김태훈, 엄영익, “가상화와 원격제어를 이용한 망분리 기법”, 한국정보과학회 학술발표논문집 39(2A), 2012년11월

[3] 정연서, 남기동, “공공기관 망분리 솔루션 고찰”, 한국통신학회 학술대회논문집, 2011년6월

[4] 유수상, “클라우드 컴퓨팅 현황과 활성화 과제” 한국IT서비스산업협회, 2011년1월