韓國IT 서비스學會誌
第15卷 第3號
2016年 9月, pp.33-50

Journal of Information Technology Services
http://dx.doi.org/10.9716/KITS.2016.15.3.033

Shadow IT를 고려한 새로운 관리체계 도입에 관한 연구

유지연* · 정나영**

A Study on the New Management System Considering Shadow IT

Jiyeon Yoo* · Nayoung Jeong**

■ Abstract ■

In a dynamic IT environment, employees often utilize external IT resources to work more efficiently and flexibly. However, the use of external IT resources beyond its control may cause difficulties in the company. This is known as "Shadow IT." In spite of efficiency gains or cost savings, Shadow IT presents problems for companies such as the outflow of enterprise data. To address these problems, appropriate measures are required to maintain a balance between flexibility and control.

Therefore, in this study, we developed a new information security management system called AIIMS (Advanced IT service & Information security Management System) and the Shadow IT Evaluation Model. The proposed model reflects a Shadow IT's attributes such as innovativeness, effectiveness, and ripple effect. AIIMS consists of five fields: current analysis; Shadow IT management plans; management process; education and training; and internal audit. There are additional management items and sub-items within these five fields. Using AIIMS, we expect to not only mitigate the potential risks of Shadow IT but also create successful business outcomes. Now is the time to draw to the Light in the Shadow IT.

Keyword : Shadow IT, BYOD(Bring Your Own Device), AIIMS(Advanced IT Service & Information Security Management System), ISMS(Information Security Management System), ITSMS(IT Service Management System)

Submitted : July 30, 2016 1st Revision : August 20, 2016 Accepted : August 26, 2016

* 상명대학교 일반대학원 지식보안경영학과 조교수, 주저자 · 교신저자
** 상명대학교 경영대학원 사이버보안경영학과 석사과정

1. 서 론

클라우드와 빅데이터, 사물인터넷(IoT) 환경이 확대됨에 따라 직원들은 보다 유연하고 생산성 있는 업무 환경 구축을 위해 다양한 IT 자원을 사용하게 되었다. 따라서 예전에는 IT 부서나 기업이 정보시스템 등의 IT 자원 소비를 주도했다면, 오늘날에는 직원들이 직접 외부자원에 접근하여 업무에 필요한 자원을 구매하는 등 적극적인 소비자로 변모하여 IT 자원 소비를 주도하게 되었다.

기업을 둘러싼 환경이 변화하면서 기업의 공식적인 IT 자원이 아닌 외부에서 가져온 스마트폰, 태블릿, 노트북 등의 사용이 기업 내 업무를 수행하는데 큰 부분을 차지하게 되었으며, 대부분의 기업들은 직장에서 이를 허용하고 관리하기 위한 정책을 채택하게 되었다(Dhingra, 2015).

그러나 외부 IT 자원의 사용이 점차 증가하면서 직원들은 조직의 명시적인 승인 없이도 정보기술 시스템과 솔루션 등을 구축하고 사용하게 되었는데, 이렇게 기업의 통제 영역을 벗어나 외부 IT 자원을 이용하고 스스로의 업무 환경을 구축하게 되는 현상을 'Shadow IT'라고 한다(CXO Unplugged, 2012). 직원들은 Shadow IT를 통해 업무 수행 능력, 시간과 공간의 유연성 및 편의성의 향상 등 여러 이점을 취할 수 있으나 이 과정에서 그들은 기업의 정보시스템(IS) 및 데이터에 대한 보안 위협을 발생시킬 수 있다(Haag, 2015). 실제로 시장조사 업체인 가트너에서는 2020년까지 기업이 경험하는 보안 공격의 1/3이 Shadow IT를 통해 이루어질 것이라고 전망하고 있으며 이러한 보안 위협을 관리하는 것은 단순한 보호 역할뿐만 아니라 성공적인 비즈니스 성과를 만들기 위해 필요하다고 주장하고 있다(Cio Korea, 2016).

그러나 이러한 전망에도 불구하고 국내에서는 아직까지 Shadow IT에 대한 개념 인식뿐만 아니라 이를 사용할 때 얻을 수 있는 효과성 및 위험성에 대한 자각이 여전히 부족한 상태이다.

따라서 본 논문에서는 Shadow IT의 개념을 정의하고 기업에 미치는 영향과 발생할 수 있는 보안 위협 등의 문제점을 파악하여, Shadow IT를 포함해 IT 서비스 및 정보보호 관리가 효과적으로 이루어질 수 있는 관리체계 연구를 목적으로 한다.

이에 전체적인 구성에 있어서 제 2장에서는 Shadow IT와 관련 용어의 개념을 파악하고, 다른 IT 자원과 구별되는 Shadow IT의 속성을 식별한다. 제 3장에서는 Shadow IT 관리의 필요성을 제시하고, 기존에 존재하는 관리체계가 Shadow IT 관리에도 유효하게 사용될 수 있는지 검토한다. 제 4장에서는 효과적인 관리체계 구축을 위해 요구되는, 기업 내 관리하고자 하는 Shadow IT의 식별 및 평가를 위한 Shadow IT 평가 모델을 제시한다. 마지막으로 제 5장과 제 6장에서는 분석과 평가를 통해 도출된 Shadow IT 관리 요구사항 및 평가 모델을 활용하여 새로운 관리체계로써 AIIMS (Advanced IT service & Information security Management System)를 구축하고 그에 따른 세부 관리 항목을 함께 제안한다.

2. Shadow IT 개념 및 특성

2.1 개념 정리

2.1.1 Shadow IT 정의

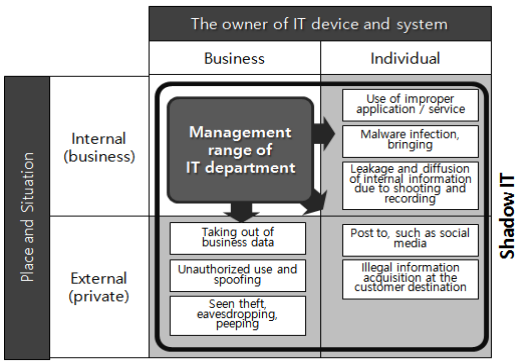
Shadow IT는 새로운 현상이라기보다는 중요성이 강조되는 최근의 추세를 의미하는 용어이다 (Rentrop et al., 2011).

Shadow IT와 유사한 의미의 용어로, 조직 내 정보시스템 부서의 관리 범위가 아닌 비즈니스 프로세스 어플리케이션을 'Shadow System'이라 하였다 (Wikipedia "Shadow System"; Sherman, 2004). 'Shadow IT'라는 용어는 Bayan(2004)에 의해 관리되지 않는 IT의 위험으로 언급되며 처음 등장하였다. 그리고 Raden(2005)이 '기업의 업무를 수행하기 위해 IT 기능을 수행하지만 공식적인 IT 조직에는 속하지 않는 도구(Raden, 2005)'로 정의하였다(Shumarova and Swatman, 2008).

이후 IT 소비자화(IT consumerization)로 인해 대부분의 기업 업무 및 활동에 개인 IT 기기 및 서비스가 활용되면서 이러한 Shadow IT의 의미는 '기업 내의 일반 사용자인 직원이 IT 조직의 공식적인 승인 없이 외부의 IT 서비스 및 IT 장치를 이용하여 효율적인 업무 수행이 가능한 환경을 구축하는 것(CXO Unplugged, 2012)'으로 확장되었다.

Shadow IT에 대한 다양한 학자들의 정의를 정리하면 다음의 <Table 1>과 같다. Shadow IT는 관리와 통제의 어려움이 강조되어 기업의 '위험요소'로만 평가되었으나, 최근에는 Shadow IT 활용이 확대되고 또한 효율적으로 활용하게 되면서 기업의 이익 및 가치 향상으로 이어져 조직의 '기회'로 부상하게 되었다(Protiviti, 2014).

Shadow IT에 대한 개념 범위와 이를 통해 확대되는 IT 관리 및 통제 영역을 정리하면 <Figure 1>과 같다. 기존에 기업 내의 IT 관리와 통제는 기업 내부에서 업무용으로 사용되는 기업 소유의 IT 자원만을 대상으로 하였으나 현재는 보이지 않는 IT 자원이지만 기업에 영향(위험 혹은 이익 및 가치 향상)을 미치는 범위까지 IT 관리와 통제의 대상으로 요구되고 있다. 기업 내부에서 사용되는 개인 소유의 IT 자원뿐만 아니라 기업 외부에서 사적으로 활용되는 기업 소유의 IT 자원, 그리고 개인 소유의 IT 자원 등 Shadow IT를 포함한다.



※ Source : ITR, 2012.

〈Figure 1〉 Concept of Shadow IT

〈Table 1〉 Definition of Shadow IT

Reference	Definition
Sherman (2004)	Data shadow systems are not built to an overall design or architecture, e.g., Excel- or Access-based systems, used to add information to reports, which are not supplied from the official IT.
Bayan (2004)	Shadow IT is as ominous as it sounds. Detached from corporate IT, running its own systems, and covertly implementing its own rules and policies, a shadow unit can quickly become a sinister threat to the company's security infrastructure.
Raden (2005)	Shadow IT, those people performing IT functions but not part of the mainstream IT organization, have been found to be as much as 78% of the size of the total official IT staff. The existence of Shadow IT implies a failure on the part of IT to provide all of the services to meet their clients' needs, and the problem is universal.
Schaffner (2007)	Shadow IT is the un-official IT group that people have learned to depend on to get things done. Shadow IT is the bane of formal IT's existence. Just go ask your IT manager about shadow IT and watch the veins in their forehead pop out. Shadow IT can really be a problem for a company.
Shumarova and Swatman (2008)	"Shadow CIT" solutions are employee autonomous: they are not implemented as part of the organi-sational IT infrastructure, and have not received any targeted investment.Often, without being able to articulate why, users appear to shun enterprise CITs and "good" architecture in favour of the ability to get their work done through autonomous "shadow" solutions.
Dols (2009)	"Shadow IT" or "Rogue IT" is usually defined as the 'unofficial' usage of IT hardware and software in the workplace and a term used in IT for any application or transmission of data relied upon for business processes but which is not under the jurisdiction of a centralized IT department.
Rentrop et al. (2011)	Business departments have a multiplicity of other hardware, software and IT employees. Generally these exist without the awareness, acceptance and support of the IT department. The resulting, autonomous developed systems, processes and organizational units are usually characterized as "Shadow IT"
Crump (2014)	Shadow IT is a term describing users or whole lines of business who go outside of their organization's IT group to meet their IT needs. A disconnect often exists between what IT users feel they need and what the IT services group is prepared to deliver. Shadow IT's destination is often the cloud, where a company credit card can access all kinds of IT as a service, including cloud-based file-sync-and-share, laptop data protection, CRM, project management, or back-office software.
Haag (2015)	By applying the shadow IT concept to our cloud service context, we define shadow sourcing of cloud services as employee's voluntary, intentional usage of public cloud services in the workplace via any personal or company device instead of the use of organizational information systems or services that are mandatory.

2.1.2 BYOD 의미

Shadow IT가 가지는 최대의 위험으로서, 기업에서 나타나는 가장 대표적인 IT 사용 현상으로는 BYOD(Bring Your Own Device)가 있다. BYOD란 직원들이 기업의 업무를 수행할 때 개인 소유의 태블릿 PC, 스마트폰, 노트북 등의 정보통신기기를 활용하는 것을 일컫는 말이다. 직원들은 개인 소유의 IT 자원 활용을 통해 시간과 장소의 유연성, 편리성, 장치의 휴대성을 증가시킴으로써 업무의 생산성 및 개인의 만족도를 향상시켰으며 기업은 BYOD의 활용으로 인해 장치 및 데이터 관리 계획에 고가의 돈을 지불하지 않아도 되는 등 경제적인 혜택을 누릴 수 있게 되었다(Dhingra, 2015).

그러나 BYOD 활용으로 인한 시간과 장소의 유연성은 직원의 업무를 가중화시키며(Yun et al., 2012) 개인 및 업무 데이터의 혼재, 프라이버시 보호 문제 등 부작용을 일으킬 수 있는 위험을 가지고 있다(Anderson, 2013).

한편 클라우드, 사물인터넷(IoT)의 확대와 같은 환경 변화에 따라 직원들은 단순한 장치뿐만 아니라 어플리케이션, 네트워크 등 IT 자원을 조직으로 끌어들이기 시작했는데 이에 따라 BYOD는 타사의 어플리케이션을 사용하는 BYOA(Bring Your Own Apps), 클라우드 서비스 사용을 의미하는 BYOC(Bring Your Own Cloud), 네트워크 사용을 의미하는 BYON(Bring Your Own Network) 등의 개념으로 확산되었다(TechTarget, 2014).

2.1.3 Shadow IT와 BYOD 비교

Shadow IT와 BYOD는 기업 내부의 공식적인 IT 시스템, 프로세스, 조직 구성단위 등을 보충하며 업무의 효율적인 수행을 위해 다양한 IT 자원을 사용한다는 점에서는 유사한 점을 지닌다.

그러나 BYOD는 개인이 활용하던 모바일기기를 업무에 그대로 활용하는 것을 의미하는 것과 달리, Shadow IT는 외부의 IT 자원을 활용하거나 직접 개발하는 것을 의미한다는 점에서 차이가 있다.

또한 기업 보호 · 제어 측면에서도 차이점이 나타난다. BYOD는 기업측면에서 IT 자원을 허용하고 이를 관리하기 위한 정책을 수립하여 통제를 받게 된다. 이때 정책에서 나타나는 조직의 제어 수준은 매우 낮은 편인데 이는 직원에게 IT 자원에 대한 선택의 자유를 제공함으로써 만족도 및 업무의 생산성을 증가시킨다. 그러나 장치에 대한 보호책임 또한 직원에게 있기 때문에 보안 위협의 발생 가능성이 존재한다(Brodin, 2016).

따라서 지난 몇 년간은 BYOD 정책이 큰 인기를 끌었지만 최근에는 외부 IT 자원의 사용으로 인한 보안 위협이 주요 관심사로 떠오르면서 기업이 직접 보안 · 업무 솔루션을 탑재한 모바일기기를 미리 마련해 직원에게 선택할 수 있도록 제공하는 CYOD[1]로 관리 방법의 패러다임이 변화하게 되었다(DigitalTimes, 2014).

한편 Shadow IT의 경우, 그 사용이 기업의 명시적인 승인이나 통제 없이 직원에 자발성에 의해 이루어지기 때문에 BYOD 정책과 같이 직원에게 선택 및 보호책임을 모두 주는 것은 보안 위협이 발생할 가능성을 증가시킨다(CXO Unplugged, 2012). 따라서 BYOD의 관리 패러다임이 기업이 적절한 통제수준을 구현하는 CYOD로 변화하는 것과 같이 Shadow IT 또한 위험 요소를 식별하고 보호하기 위해 기업의 적절한 통제 영역에 들어올 수 있도록 해야 한다. 즉 기업의 IT 부서가 Shadow IT를 효과적이고 안전하게 관리 할 수 있는 환경을 먼저 구축하고, 그 안에서 사용자들의 선택권 및 자율성을 보장해줄 수 있는 관리 방법에 대한 고민이 필요하다.

2.2 Shadow IT 속성

2.2.1 혁신성

Shadow IT는 업무 수행에 필요한 IT 자원 자체의 한계, 또는 IT 부서의 지원 부족과 같은 직원

1) CYOD(Choose Your Own Device) : 역할 기반의 리스트 접근 방식이 완화되어 적용되는 관리 방법

들의 불만족으로부터 등장하게 되었다(Haag, 2015). 직원들은 불만족을 해결하고, 업무의 효율성 및 편의성을 높이기 위해 IT 부서의 승인 없이 클라우드 서비스, 스마트 디바이스와 같은 외부 IT 자원을 스스로 채택하고 사용하게 되었는데 그 효과성이 기업에까지 알려지게 되면서 Shadow IT는 혁신적이고 중요한 자원으로 인정받게 되었다.

따라서 기업은 Shadow IT를 무조건적으로 통제하는 대신 배포할 수 있는 기회를 적극적으로 제공하여 업무의 효율적 완수 및 신속한 서비스 개발을 지원하거나(Protiviti, 2014), 미래에 기업에서 공식적으로 사용될 IT 자원에 대한 프로토타입(Prototypes)으로도 사용하게 되었다.[2] 그러나 기업의 IT 거버넌스 효과가 없는 상태에서 무분별한 Shadow IT의 사용은 기업의 중요한 정보가 기업 외부에 저장되거나 유출되는 등 보안문제 발생의 위험이 크다(TechTarget, 2013).

2.2.2 비용-업무의 효율성

최근 스마트폰과 클라우드 컴퓨팅 서비스 등의 기능이 급속도로 발전하기 시작하면서 이를 기업의 업무에 도입하여 성능 향상 및 IT 비용 절감을 도모하려는 움직임이 나타나고 있다(Kobayashi, 2011).

특히 최근에는 성능 향상 및 IT 비용의 절감을 보장하는 클라우드 서비스의 수요가 계속해서 증가하고 있다(Haag, 2015). 이러한 웹기반의 기술은 낮은 초기 비용으로 이용할 수 있으며, 서비스를 사용하기 위해 모바일 및 웹 환경의 새로운 구성, IT 부서에 대한 지원 요청 없이도 바로 시작할 수 있기 때문에 간편하게 접근할 수 있다는 장점을 가지고 있다. 또한 그 자체로 훌륭한 IT 서비스를 얻을 수 있다(Rentrop and Zimmermann, 2012a). 이처럼 Shadow IT는 저비용으로 신속하게 사업을 추진할 수 있는 효과적인 수단처럼 보인다.

그러나 업무상 바람직하지 않은 응용 프로그램이나 서비스가 이용 될 가능성이 있으며 클라우드 컴퓨팅에 대한 수요가 계속적으로 증가하면서, 큰 규모의 클라우드 사용 및 관리 비용이 상승하는 등 비용효율성을 달성하기 어려운 문제에 직면할 가능성이 있다. 따라서 Shadow IT의 사용 및 관리 비용이 얻을 수 있는 이익을 넘어서지 않도록 하는 모델이 필요하다(Cui et al., 2014).

2.2.3 파급성

파급성이란 Shadow IT의 사용이 업무 수행뿐만 아니라 기업 전체 비즈니스의 긍정적, 부정적 측면에서 영향을 미치는 것을 의미한다. 이 때 영향을 미치는 방향은 'IT 소비자화(IT consumerization)'라는 큰 시대적 흐름과 밀접하게 연결되어 IT 부서에서 직원으로 내려오는 하향식(top-down) 방식이 아니라 직원으로부터 기업 전체로 올라가는 상향식(bottom-up) 방식이라는 특징을 가지고 있다(ITR, 2012).

그러나 이러한 IT 자원 자체에 대한 위험은 시스템을 구성하는 요소의 위험으로 연결될 수 있으며 결국 기업 전체의 비즈니스 위험으로 그 영향이 증가할 수 있다(JIPDEC, 2014c). 따라서 부정적 측면의 Shadow IT 파급성을 감소시키기 위해서는 각 수준에 맞는 위험 관리 및 대응 방법을 구축해야 할 필요가 있다.

3. Shadow IT 관리체계 필요성 및 적합성

3.1 Shadow IT 관리 필요성

Shadow IT를 사용하여 작업의 효율성을 향상시키는 과정에서 기업의 정보들은 헤아릴 수 없는 위험들에 노출되어 있다. 직원이나 관리자는 회사에서 제공하는 부족한 IT 시스템을 교체하거나 보충함으로써 작업 효율성을 향상시키고자 하는데 이 과정에서 그들은 의도적이거나 비의도적으로 기업의 IT 정책을 위반함에 따라 정보시스템(IS) 및 데이터 보안을 해칠 수 있다. 특히 클라우드 서

2) Wikipedia, "Shadow IT"(accessed June 27, 2016). https://en.wikipedia.org/wiki/Shadow_IT.

비스의 이용은 기업의 민감한 데이터 및 문서가 공유되고 저장되는 등 기업의 안전한 벽을 넘어 외부에 존재하는 3자에게로 이동할 가능성이 있다. 이렇게 기업 내 업무 환경과 사회의 상호작용은 기업의 보안을 위협할 수 있는 부주의를 자극할 가능성이 있다(Haag, 2015).

따라서 기업 및 비즈니스 리더들은 민감한 데이터의 보호 등 기업의 위험을 최소화하면서도 외부 IT 자원을 적극적으로 이용, 더욱 생산성 있는 작업을 할 수 있도록 하기 위한 정책을 만들고, 지원해야한다. 다시 말해 기업이 성공적인 Shadow IT 관리 정책을 도입하기 위해서는 업무의 유연성과 기업의 제어 사이에 올바른 균형을 유지해야 한다(McAfee, 2013).

Shadow IT 관리에서 요구되는 사항들을 정리하면 다음의 <Table 2>와 같다.

〈Table 2〉 Requirements of Shadow IT Management

Reference	Requirements for management of Shadow IT
ITR (2012)	1. Identify the use of shadow IT in the company and its progress status
Computer Weekly (2012)	2. Mandatory audit upon introduction of new IT resources(compliance to rules etc)
Computer Weekly (2012)	3. Change and release activities of IT resources
Rentrop and Zimmermann (2012a)	4. Collection of successful shadow IT management cases and development of consolidated and scientific approach encompassing the relationships with other IT management elements and business tasks
McAfee (2013)	5. Minimization of corporate risks and protection of data
Cui et al. (2014)	6. Utilization of existing IT management processes
JIPDEC (2014b)	7. Strengthening the capabilities and professional knowledge of employees operating and managing shadow IT
JIPDEC (2014c)	8. Continuous provision of IT services
Haag (2015)	9. Strengthening of employees' security awareness on the organizational security policy

3.2 새로운 관리체계 도입의 타당성

앞의 절에서는 Shadow IT의 사용으로 인해 발생하는 기업의 위험을 제거하고 업무의 효율성을 증가시키기 위해 관리의 필요성 및 요구사항을 제시하였다. 따라서 본 절에서는 Shadow IT를 관리하기 위한 적절한 체계를 식별하기 위하여 기존에 존재하는 IT 자원 관리체계와 Shadow IT의 요구사항을 비교·분석하였다. 비교 항목으로는 <Table 2>에서 제시한 Shadow IT 관리 요구사항을 요약 정리한 <Table 3>을, 비교 대상으로는 기업 대상의 관리체계인 ISMS(Information Security Management System)[3]와 ITSMS(IT Service Management System)[4], CSMS(Cyber Security Management System)[5]를 사용하였다.[6]

3) ISMS(Information Security Management System) : 정보통신망의 안전성 확보를 위하여 수립·운영하고 있는 기술적·물리적 보호조치 등 종합적인 관리체계에 대한 인증제도로 5단계 관리과정(정보보호정책수립, 정보보호 관리체계 범위설정, 위험관리, 구현, 사후관리), 문서화, 정보보호대책에 대하여 조직의 특성 및 환경에 부합되도록 적절하게 수립·구현하여, 체계적으로 관리·유지하고 이행하는지를 평가하는 제도이다.

4) ITSMS(IT Service Management System) : IT 서비스 관리시스템으로 IT 서비스를 운영하기 위한 프레임워크를 확립하고 3자에 의한 적합성 평가 제도를 구축하여 조직의 IT 서비스 운영 관리 품질의 지속적 향상 및 IT 서비스 전체의 신뢰성 향상에 기여하는 것을 목적으로 한다. ITSMS 적합성 평가 제도는 ISO/IEC 20000-1을 인증 규격으로 2007년 4월부터 본격 운용하고 있다.
특히, 최근에는 다양한 IT에 대한 통합 관리 시스템 차원에서 ISMS에서 ITSMS 전략으로의 전환이 요구되고 있다(Hasegawa and Nakano, 2012).

5) CSMS(Cyber Security Management System) : 세계 최초 ISMS을 기반으로 한 일본의 제어시스템 보안 관리 시스템(CSMS) 인증 제도로 제품 및 조직 관리 체제 측면을 중요시하여 국제 표준인 IEC 62443-2-1 : 2010을 기반으로 CSMS 인증 기준(IEC 62443-2-1)을 수립, 2014년 4월부터 개시하였다.

6) 비교할 관리체계의 선정은 일본의 JIPDEC을 참고하였다. JIPDEC, "Information Management"(accessed June 27, 2016). http://www.jipdec.or.jp/project/isms_itsms_bcms.html.

〈Table 3〉 Requirements of Shadow IT Management(summary)

Requirements for management of Shadow IT(Summary)	<Table 2> Connectivity
Shadow IT Assessment	1
Service Continuity	8
Integrated Management	4
Change Management	3
Information Security	5
Utilization of Existing IT Management Processes	6
Utilizing Successful Management Case	4
Internal Audit	2
Strengthening the Capabilities and Professional Knowledge of Employees	7,9

〈Table 4〉 Comparison of Shadow IT Management Requirements and the Existing Management System

Requirements for management of Shadow IT	ISMS		ITSMS		CSMS	
Shadow IT Assessment	◎	Identification of information assets and risk assessment	○	Analysis of IT service management activities		
Service Continuity	◎	Business continuity planning and maintenance management	◎	Service continuity and availability management	◎	Business continuity plan
Integrated Management			◎	Organization cross-sectional and comprehensive approach	◎	Including internal/external parties of organization in management system
Change Management	○	Change management	◎	Change and release process	○	Modification and improvement according to review
Information Security	◎	Protection of the organization's major information assets	◎	Information security management	◎	Information and document management
Utilization of Existing IT Management Processes			◎	Providing existing service and utilization of management methods		
Utilizing Successful Management Case			◎	Application of successful cases such as ITIL®		
Internal Audit	◎	Internal audit	◎	Internal auditing	◎	CSMS monitoring
Strengthening the Capabilities and Professional Knowledge of Employees	◎	Information protection training and improvement of perception	◎	Perception of capabilities and training	◎	Employee training and security awareness
	- Management report and approval - Review of compliance to legal requirements - Managing the operation status of management system - IT disaster recovery plan - Establishing comprehensive management plans such as managerial, physical and technological protection of information system		- Involvement of management - Minimize discrepancy between internal policies and actual operation - Setting and measurement of service management objectives and the key performance indicators(KPI) of each process - Business relationship and supplier management		- Identification and assessment of cyber-threats faced by organization - Planning and action on security incidents	

◎ : Identical elements existing inside the management system.
○ : Similar elements existing inside the management system.

위의 <Table 4>는 Shadow IT 관리 요구사항과 여러 관리체계의 구성 요소의 비교를 수행하고 난 후의 결과표이다. 비교 수행 시, 각 관리체계 내에 Shadow IT 관리 요구사항과 동일한 수준의 구축 요구사항 및 프로세스가 있을 경우에는 '◎표', 일부 유사한 수준의 구축 요구사항 및 프로세스가 있을 경우에는 '○표'로 기입하여 많은 동일 · 유사점을 가지는 관리체계를 새로운 관리체계의 기본 틀로 사용하고자 하였다. 그 결과 ISMS를 포함하는 기존의 관리체계는 Shadow IT의 특성 및 관리에 필요한 사항을 모두 갖추지 않고 있기 때문에 새로운 관리체계가 필요함을 알게 되었다.

따라서 본 논문에서는 그 중 제일 많은 표를 얻은 ITSMS를 기반으로 하고 Shadow IT의 특성 및 관리 요구사항을 추가한 새로운 관리체계를 구축하고자 한다.

4. 관리체계 적용을 위한 평가모델

Shadow IT는 기업이 기존에 가지고 있는 통제 및 위험 관리 구조의 영향을 받지 않기 때문에 새로운 관리체계가 요구된다.

특히 새로운 관리체계 및 세부사항을 제시하기 이전에 우선적으로 Shadow IT가 기업 내부에서 얼마나 진행되고 있으며 어느 정도 수준의 관리가 필요한지 식별할 수 있는 과정이 절대적으로 필요하다.

따라서 본 장에서는 기업 내부의 구체적인 Shadow IT 상태를 분석하기 위해 Shadow IT의 속성과 관련한 평가 기준의 개발 및 활용 방법에 대해 제시하고 제 5장에서 제시될 Shadow IT 관리체계의 필수항목으로 구성하고자 한다.

4.1 평가기준의 개발

본 평가기준은 Rentrop and Zimmermann(2012b)의 연구에서 제시된 'Shadow IT 평가모델(Shadow IT Evaluation Model)'의 주요 및 세부 기준을 기반으로 하고, 제 2장에서 제시한 Shadow IT의 속성과 제 3장에서 제시한 관리 요구사항을 추가하여 구성하였다.

기존의 연구는 Shadow IT로 인해 발생하는 위험을 해결하기 위해서는 Shadow IT에 대한 식별 및 평가의 과정이 절대적으로 필요함을 주장하였으며 Shadow IT와 위험 관리, IT 거버넌스, IT 서비스 관리와의 상호작용으로부터 도출해낸 관련성, 품질, 크기, 혁신적인 잠재력, 병렬과 같은 항목을 평가 기준으로 설정하였다. 그러나 항목명 자체에 Shadow IT의 속성이 잘 드러나지 않고 주요 항목이 품질, 크기 등 물리적 속성에 초점이 맞춰져있기 때문에 통합적 관점에서 평가할 수 있는 항목으로의 수정이 필요하다.

따라서 본 논문에서는 Shadow IT가 미치는 영향력에 가까운 기존의 항목에 Shadow IT의 속성을 추가하고, 이를 관련성, 효과성, 파급성으로 나누어 재배치한 후 그에 따른 하위 항목을 구성하였다.

평가항목의 주요 기준 및 세부 기준을 정리하면 <Table 5>와 같다.

〈Table 5〉 Shadow IT Evaluation Criteria

Shadow IT assessment criteria		
Criteria	Tier1	Tier2
Relationship	Overall	Strategical relevance
	Detailed	Business process
		IT security
		Regulations
		IT service management
Effectiveness	Quality	System quality
		Service quality
		Information quality
		Business processing quality
	Efficiency	Business efficiency
		Cost efficiency
Influence	Quantitative	Use of resources
		Use of professional capabilities
		Required whether it is used
		No. of users
	Qualitative	Possibility of innovation

※ Source : Rentrop and Zimmermann, 2012b 재구성.

4.1.1 관련성

관련성이란 각 Shadow IT와 기업 활동의 관련 정도에 대한 평가 항목이다. 기업은 비즈니스 활동뿐만 아니라 위험관리 활동을 통해 기업의 이익 창출을 저해하는 요소를 제거함으로써 기업의 가치를 향상시킨다. 따라서 본 평가 항목을 통해 기업 전체의 전략적 관련성뿐만 아니라 세부적 측면에 대한 평가를 모두 수행하고 위험 여부와 그 정도를 측정하고자 한다.

- 전체적 관련성 : Shadow IT가 IT 인프라와 관련한 기업 전체의 전략과 전략 결정에 어떠한 영향을 미치는지를 평가하는 항목이다. Shadow IT가 전략적 관련성에 미치는 영향의 정도와 기업 전체의 전략적 가이드라인 및 세부 지침에 대한 일관성 유지 정도에 따라 추후 기업의 전체적인 전략을 변화시킬 가능성이 있다(Rentrop and Zimmermann, 2012b).
- 세부적 관련성 : Shadow IT의 사용은 기업의 통제의 영역을 벗어남에 따라 쉽게 위험에 처할 수 있다. 즉 직원들은 업무 수행 편의성, 효율성만을 고려해 IT 자원을 사용하기 때문에 의도적이거나 비의도적으로 기업의 정보시스템(IS) 및 데이터 보안을 해칠 수 있으며 조직의 IT 정책을 위반하기도 한다. 더욱이 오늘날의 작업장 환경은 네트워크 연결을 통한 외부와의 상호작용을 통해 이러한 부주의를 자극할 가능성이 있다(Haag, 2015).

따라서 기업의 비즈니스 프로세스, IT 보안 및 규정, IT 서비스 관리 활동과 Shadow IT의 관련성 평가를 통해 위험성을 인지하고 관리하여야 한다.

4.1.2 효과성

효과성이란 Shadow IT 사용을 기업의 이익 및 가치 향상을 촉진시키는 요소 중 하나로 인식하고, 유연성 있는 사용을 보장하는 관리방법을 구축하기 위해 도입된 평가 항목이다. 효과성을 평가하기 위한 관점은 IT의 품질 및 조직 측면에서의 효율성으로 나누고 각각의 하위 항목을 구성하였다.

- 품질 : Shadow IT를 사용하여 기업 내 업무 처리할 때 그 효과성을 측정하기 위한 항목으로 기술적인 시스템 품질 뿐만 아니라 IT 서비스 및 그로 인해 생성된 정보의 품질 모두를 포함한다(Rentrop and Zimmermann, 2012b).

〈Table 6〉 Component for Quality

Tier2	Contents	Evaluation method
System quality	Refers to the measurement of the information system's performance in terms of technology and design; it can be assessed by dividing into hardware, software and engineering processes	Maturity model, capabilities maturity model (CMMI), quality criteria
Service quality	Refers to the quality of IT service connected to shadow IT.	Comparative evaluation through successful IT service management cases
Information quality	Refers to the data quality realized as a result of shadow IT.	Data integrity and consistency assessment
Business processing quality	Evaluates the quality of processes related to the use of shadow IT.	Maturity models such as business process maturity model (BPMM)

- 효율성 : 효율성은 Shadow IT 자원이 업무 수행 및 비용 절감에 주는 효과성의 정도를 평가하는 항목이다. 하위 항목은 업무 수행 시 기존에 사용하던 IT 자원과 비교하여 Shadow IT가 제공하는 편의성, 정확성, 완전성에 대한 평가를 수행하는 업무 효율성과 IT 자원을 이용 및 유지하는데 소요되는 비용에 대한 비교를 통해 Shadow IT의 효율성을 평가하는 비용 효율성으로 나눌 수 있으며 평가의 수행은 기존에 존재하는 기업 내 IT 자원과의 비교를 통해 이루어진다.

4.1.3 파급성

기업에서 Shadow IT를 관리하기 위한 보안 대책을 검토할 때에는 우선적으로 Shadow IT가 자사에서 어느 정도 사용되고 어떠한 위치를 차지하고 있는지 정확하게 파악하는 것이 요구된다(ITR, 2012). 따라서 Shadow IT의 크기 및 혁신적 가능성 평가를 통해 기업 내에 사용되고 있는 각 Shadow IT의 사례를 분석하고자 한다.

- 정량적 파급성 : 직원에 의해 결정되는 Shadow IT의 사용은 그 결과로 나타나는 효율성과 전체 및 개인의 작업 환경, 기업 내 규범에 영향을 미치는 정도에 의해 보안 위험 수준이 결정된다. 이를 관리하기 위해 Shadow IT를 사용하는 사용자의 의도와 실제 사용행동에 대한 평가가 필요하다(Haag, 2015). 따라서 본 세부 항목 평가를 통해 기업의 특정 Shadow IT의 사용 및 파급성 정도를 추정할 수 있다.

〈Table 7〉 Component for Quantitative

Tier2	Contents
Use of resources	Item for evaluating how many employees, technology resources and application programs are required for the implementation and maintenance of shadow IT
Use of professional capabilities	An evaluation item on whether an employee with some degree of professional capabilities performs tasks by using shadow IT.
Required whether it is used	Refers to the degree of contribution to tasks; an item for evaluating the degree of implementing essential functionalities required when performing certain tasks
No. of users	Indicates how broad shadow IT is used inside the company; can be also expressed as the share of shadow IT from the IT resources used in a company.

- 정성적 파급성 : 정성적 가능성이란 개별적인 Shadow IT의 혁신적인 잠재력의 정도를 평가하는 항목이다. 본 세부항목의 평가를 통해 Shadow IT가 지닌 혁신적인 가능성 정도에 따라 ① 기업 내 기존 IT 자원의 보완재 역할, ② 기업의 새로운 기술 또는 프로세스 도입을 위한 프로토타입(Prototypes) 역할, ③ 기존에 존재하는 IT 자원의 대체재 역할 등 수준을 나누어 적용하는 등 기업의 IT 자원 관련 의사결정에 도움을 줄 수 있다(Rentrop and Zimmermann, 2012b).

4.2 평가 방법 및 활용

상기에서 기재된 기준을 가지고 평가를 수행하기 위해서는 평가 이전에 기업 전체와 IT부서의 정책, 전략과 같은 기본 정보의 수집이 필요하며 평가가 진행되는 동안 IT부서와 같은 관련 직원들과의 충분한 커뮤니케이션이 이루어져야 한다.

한편 각 기준에 대한 개별적인 평가 후 이를 기업의 상황에 맞게 의미 있는 결과로 활용하기 위해서 각 기준에 대해 가중치를 추가할 수 있다. 주요 평가기준 중 관련성, 품질과 그 하위 항목은 기업의 상황을 고려하여 개별적으로 가중치를 둘 수 있으며 그 후에 각각의 하위 평가 기준은 0점부터 10점으로 평가된다. 또한 사용자 평가, 효율성, 혁신적인 잠재력의 주요 기준은 Shadow IT의 개별 사례에 대해서만 평가된다.

모든 하위 항목은 점수는 해당 주요 평가 기준 점수에 축적되며, 최종적으로 점수가 합산된 평가 결과를 가지고 Shadow IT의 점수가 높은 항목에 대한 우선순위 설정 및 관리가 이루어져야 한다.

5. 새로운 IT 관리체계 구축 : AIIMS

ICT 환경의 확대와 클라우드 컴퓨팅 등 고기능을 갖춘 단말의 보급이 증가하면서 정보서비스의 대규모 증가 및 다양화로 인한 혼란이 가중되었다.

따라서 많은 기업들은 IT 자원의 사용으로 인한 보안 위협을 완화시키기 위해 다양한 정책, 절차, 프로세스, 기술 전략 등을 수립하였으나 역동적으로 변화하는 환경에 초점을 맞추어 전사적으로 접

근하는 관리방법의 개발 및 지원에는 실패하였다(Kushwaha, 2016).

이러한 상황 속에서 기존에 존재하는 기업의 관리 정책의 영향을 받지 않는 Shadow IT의 등장은 기업에 새로운 IT 관리체계의 도입을 촉구하였다.

IT 관리체계를 구축할 때에는 조직 및 개인의 요구사항을 포함하여 통합, 및 사용이라는 두 가지 관점에서의 접근이 필요하다. 통합적 관점이란 각 IT 자원에 대한 보호뿐만 아니라 IT 관리의 다른 요소와 업무, 외부 환경과의 관계에서 나타나는 위험을 관리할 수 있는 통합적이고 과학적인 관리 체계의 개발을 의미하며(Rentrop and Zimmermann, 2012b) 사용의 관점에서는 Shadow IT가 혁신성, 효율성, 파급성의 특징을 가지며 기업의 이익 및 가치를 향상시키는 방법으로 사용되기 때문에 저변이 넓은 강력한 관리 방법을 통해 질서 있고 보호되는 '서비스의 구현' 중심의 관리가 필요하다는 것을 의미한다(Hasegawa and Nakano, 2012).

따라서 본 장에서는 이 두 가지 관점을 모두 포함할 수 있는 ITSMS 체계를 기본 틀로 하여 Shadow IT의 특성 및 관리 요구사항을 반영・보완한 새로운 IT 관리체계로써 AIIMS(Advanced IT service & Information security Management System)를 구축・제시하고자 한다.

5.1 ITSMS 정의 및 효과성

5.1.1 ITSMS 정의

IT 기술의 고도화에 따라 이를 활용 한 IT 서비스가 생활의 구석구석까지 침투하고 있다. 마찬가지로 클라우드 컴퓨팅, BYOD, 스마트폰 등의 등장으로 기업의 업무에 사용하는 IT 기술이 고도화되고 이를 둘러싼 환경이 더욱 복잡해지면서 안정적인 IT 서비스 사용이 요구되었다(JIPDEC, 2014c).

이러한 요구에 따라서 기업은 안전하고 효과적인 IT 서비스를 제공, 관리하고 지속적으로 개선해 나가기 위한 구조를 확립하게 되었는데 이것이 바로 IT 서비스 관리 시스템(IT Service Management System, ITSMS)이다. ITSMS는 ISMS(Information Security Management)의 진전된 형태로(Hasegawa and Nakano, 2012), 조직, 프로세스, 고객 관점에서(Kim, 2011) IT 활용을 통해 제공되는 IT 서비스를 PDCA (Plan-Do-Check-Act) 사이클에 따라 관리함으로써 기업의 IT 서비스의 품질을 보장・향상시키는 구조로 경영진의 깊은 관여와 관리 프로세스의 지속적인 개선에 초점을 맞춘 통합적인 프레임워크 구축을 목적으로 한다(JIPDEC, 2014b).

본고에서는 ITSMS가 비즈니스 및 IT 서비스의 지속적인 제공을 위해 사전(proactive) 및 사후, 기업 내・외부 환경에 대한 관리를 모두 포함하는 통합적인 관리 시스템이라는 점에 초점을 맞추어 새로운 IT 관리체계 구축의 전체적인 틀로 사용하고자 한다.

5.2 관리체계 구성

새롭게 제안하는 IT 관리체계의 항목은 ITSMS의 기본 구성에 Shadow IT의 속성 및 관리의 필수 요소를 수정・추가・재배치하여 구성하였다. 관리 체계의 주 분야로는 현황 분석, Shadow IT 관리 계획, Shadow IT 관리 프로세스, 직원 교육 및 훈련, 내부 감사로 구성되어있으며 다시 각각의 관리 항목과 세부 항목을 설정하였다.

5.2.1 현황 분석

대부분의 Shadow IT에 대한 연구는 조직차원에서의 관리 방법에 대해 다루고 있다. 그러나 Shadow IT는 최종 사용자인 직원이 업무 수행을 위한 수단을 직접 선택하고 사용하는 상향식(bottom-up)서비스라는 특성을 지니고 있기 때문에 개인적인 차원에서도 기업의 Shadow IT를 인식해야할 필요성이 있다(Haag, 2015).

이러한 관점에서 내부 현황 분석은 Shadow IT 및 기존의 IT 관리 방법 식별, 그 격차에 대한 분석, 우선순위 설정으로 이루어진다. Shadow IT

식별 항목의 경우 제 4장에서 제시된 Shadow IT 평가 모델을 통해 수행될 수 있으며, 이 분야는 관리 체계 구축 및 수행의 가장 기초적인 단계로 기업의 크기 및 IT 자원 관리 수준에 관계없이 Shadow IT가 사용되는 모든 조직에서 필수적으로 이루어져야 한다.

5.2.2 Shadow IT 관리 계획

경영자를 포함한 조직 전체가 Shadow IT를 효과적으로 사용하고 관리하기 위해서는 관리체계에 필요한 요구사항을 식별하고, 식별된 관리 요구사항을 바탕으로 어떠한 방법, 절차에 의해 관리를 수행할지 계획하는 등 기본적인 정책, 규정, 지침 등의 수립이 필요하다. 관리항목은 관리체계 요구사항 식별 및 관리 계획 수립으로 이루어지며 그에 다른 세부 항목으로 구성된다(JIPDEC, 2014b).

- 관리체계 요구사항 식별 : 관리체계 요구사항은 Shadow IT 속성이 포함된 관리 요구사항 및 직원의 요구사항, 기업 비즈니스 측면의 요구사항을 모두 충족시킬 필요가 있으며 위험 관리 측면에서 대응하기 위한 요구사항 또한 포함되어야 한다.
- 관리 계획 수립 : 관리 계획의 수립 시에는 관리를 적용할 Shadow IT의 범위 및 관리 목적을 명확히 설정해야 하며 그에 따른 기업 구성원의 역할 및 책임을 할당해야 한다. 또한 정책, 규정, 지침 등은 Shadow IT의 사용을 제한하기 보다는, 기업의 보안 및 가치를 손상시키지 않으면서 효율적인 업무 수행을 위해 사용할 수 있도록 유연성과 제어 사이의 균형을 유지하도록 수립되어야 한다(McAfee, 2013). 또한 위험관리 측면을 강조하여 Shadow IT의 사용을 통해 지속적인 업무의 효율성 향상을 목표로 해야 한다.

다만 Shadow IT 관리 계획 수립 시 기존의 IT 관리시스템을 완전히 배척하거나 대체하는 것이 아니라 조화 관계에 있는 관리시스템을 보완 · 통합하여 보다 강력한 관리체계의 구현을 가능하도록 구성해야 한다(Hasegawa and Nakano, 2012).

5.2.3 Shadow IT 관리 프로세스

Shadow IT 관리계획의 효과적인 구현을 위해서는 이를 지원하는 구체적인 관리 프로세스가 수립이 필요하다. 따라서 관리 프로세스의 항목으로는 지원 프로세스, 보고 프로세스, 관계 프로세스, 해결 프로세스, 제어 프로세스, 릴리스 프로세스로 이루어지며 각 프로세스는 다시 세부 항목으로 구성된다.

- 지원 프로세스 : 가용성 측면에 초점을 맞춘 프로세스로, Shadow IT가 지원하는 기능 및 품질 수준을 식별한 후 직원이 원할 때 언제든지 사용할 수 있도록 연속성 및 가용성을 보장하고, 품질 수준의 유지를 위한 예산 및 회계 관리, 기업의 데이터 보호활동을 위한 보안 관리가 수반되어야 한다(JIPDEC, 2014a).
- 보고 프로세스 : Shadow IT 관리체계에는 경영진의 의지가 필요하다. 따라서 경영진의 의사결정 및 효과적인 의사소통을 위한 정보를 보고하기 위해 문서화 및 보고 체계 수립이 필요하다.
- 관계 프로세스 : Shadow IT를 사용하는 직원과 그 IT 자원을 제공하는 외부자, 기존 IT 관리 프로세스 및 업무와의 관계를 관리함으로써 Shadow IT 사용을 통해 업무의 효율적인 수행이 보장되어야 한다. 특히 기존 IT 관리 프로세스와의 관계에서는 기능 및 목적의 관련 정도에 따라 에너지 소비를 최소화하고 규모의 실패를 해결하기 위해 새로운 관계 프로세스를 기존의 프로세스를 보완하는 형태로 통합할 수 있다(Cui et al., 2014).
- 해결 프로세스 : 위험관리 측면의 프로세스로 Shadow IT 사용으로 기업의 보안 위험이 발생했을 때 위험의 유형, 정도를 파악하여 빠르게 조치를 취하고 그 보안 위험이 발생하는 원인에 대한 확인 및 분석을 통해 관리함으로써 비즈니스 중단을 최소화하는 사고 관리, 문제 관리프로세스를 포함한다(JIPDEC, 2014a).
- 제어 프로세스 : Shadow IT를 효과적으로 제어하기 위해 구성 요소를 파악하고, 새로운 Shadow

IT가 도입될 때 마다 그에 대한 평가, 승인, 구현, 검토 등 변경사항에 대한 관리가 반드시 수행되어야 한다(ComputerWeekly, 2012)

- 릴리스 프로세스 : 기업 내부에서 Shadow IT에 대한 변경사항을 관리하기 위해 직원의 Shadow IT 사용에 대해 추적할 수 있어야 한다.

Shadow IT 관리 프로세스 항목의 세부항목을 정리하면 <Table 8>과 같다.

5.2.4 인적관리

Shadow IT는 직원에 의해 직접적으로 선택, 구축, 사용되는 특징을 가지고 있으며 그 IT 자원 자체에 대한 보안 위험 발생 시 그를 통해 수행되는 업무 및 기업 전체의 비즈니스와 시스템의 위험으로까지 연결되는 파급성을 가지고 있다. 따라서 운영 및 관리를 수행하는 직원들에 대한 관리가 매우 중요하다(JIPDEC, 2014c). 인적관리에 해당하는 프로세스는 직원의 역량 평가, 교육 및 훈련으로 구성된다.

- 직원 역량 평가 : Shadow IT의 비용-업무 효율성으로 직원은 IT 부서의 승인이나 직원 없이도 간편하게 접근하여 업무를 수행할 수 있지만 IT 자원의 안전한 사용 방법이나 위험에 관한 전문지식 없는 무분별 사용은 기업의 중요 정보가 기업 외부에 저장되거나 유출되는 등 보안 문제의 발생 위험이 크다(TechTarget, 2013).

〈Table 8〉 Shadow IT Management Process

Process item	Sub-item	Description
Support process	Continuity and availability management	Verifying the IT continuity and availability that can be satisfied in any situation the employees are to use.
	Budget and accounting management	Budget and accounting management on IT resource usage costs
	Information security management	Corporate data protection activities should be performed in an effective manner when using shadow IT
Report process	Management execution report	Generate reliable and accurate reports and establish a reporting system for management's decisionmaking and effective communication
Relation process	Employee management	Based on the understanding of IT resource usage by employees, the employees should be managed in away that maintains the balance between the guarantee on requirements and convenience, and the efficiency of tasks and costs
	Supplier management	Good relationship with the supplier has to be maintained in order to guarantee that IT resources of good quality are supplied in a seamless manner
	Existing IT processes	Energy consumption is minimized and new processes consolidated to supplement existing processes to solve the problem of failure of scale
Solution process	Accident management	IT resources that have experienced failure have to be recovered for usage to enable seamless operation
	Problem management	Minimizing business interruption by managing problems through prior identification and analyzing the cause of accidents
Control process	Consolidated management	Performing consolidated management through collection of successful shadow IT cases and identifying other elements of IT management
	Configuration management	Accurate configuration information has to be managed and maintained to control the identified shadow IT resources.
	Change management	All changes should be managed to enable evaluation, approval, implementation and review.
Release process	Change details management	Adequate management should be performed in terms of cost and quality upon introduction of new shadow IT or its modification.

따라서 각 Shadow IT의 사용 정도, 업무 기여도, 전문 지식 필요 여부 등을 식별하여 사용하는 직원이 이러한 자격을 갖추었는지에 대한 역량평가가 수행되어야 한다.

- 훈련 및 교육 : 직원의 Shadow IT 사용은 업무 수행 방법을 결정하고, 그 결정은 전체 및 개인 작업 환경, 규범에 미치는 영향과 보안 위험의 수준이 결정된다. 이러한 조직의 규범과 가치, 개인의 보안의식을 일치시키기 위해서는 조직적 인식의 변화가 필요하다. 따라서 직원의 직급, Shadow IT 사용의 수준에 따라 적절한 교육 및 훈련 방법이 계획되고 실행되어야 한다(Haag, 2015).

5.2.5 내부감사

내부 감사란 Shadow IT 관리가 관리 시스템 및 프로세스를 기반으로 제대로 수행되고 있는지를 검토 및 개선하기 위한 항목으로 감사 계획 및 방법 수립, 수행 및 개선 프로세스로 구성된다.

수행 및 개선 항목의 경우 감사 후 연간 관리 보고서, 내부 감사 결과 보고서와 같은 증적 자료가 요구된다.

새로운 IT 관리체계인 AIIMS의 주요 영역 및 세부 관리항목을 정리하면 <Table 9>와 같다.

5.3 도입 시 고려사항

새로운 IT 관리 체계인 AIIMS를 기업의 관리 정책으로 도입하기 위해서는 여러가지 사항이 고려되어야 한다. 먼저 관리 체계의 도입 시 가장 크게 고려해야 될 사항은 사용자 경험에 대한 배려이다. Shadow IT 자체가 직원의 자발성에 의해 선택되고 사용되는 IT 자원이기 때문에 본래의 기능과 사용성을 크게 저해하는 규칙을 강요해서는 안 된다. 대신, 업무 이용 시 허용되는 범위를 명확하게 보여주는 것이 더 중요한데 우선 Shadow IT의 보안 위험을 밝혀 내 보안 정책으로 기재해야 할 항목을 분명히 한 후, 각 항목에 대한 부분

〈Table 9〉 Configuration of AIIMS(Advanced IT service & Information security Management System)

Management area	Management item	Sub-item
Status analysis	Internal status analysis	Shadow IT identification
		Identification of existing IT management methods
		Gap identification
		Setting of priorities
Shadow IT management plan	Identify management system requirements	Shadow IT management requirements
		Employee requirements
		Business requirements
		Risk actions
	Establish management plan	Scope of application and setting of objectives
		Assigning roles and responsibilities
		Establishing policy/ regulations/guidelines
Shadow IT management process	Support process	Change management
		Continuity and availability management
		Budget and accounting management
		Information security management
	Report process	Management performance report
	Relationship process	Employee management
		Supplier management
		Existing IT management process
	Solution process	Accident management
		Problem management
	Control process	Consolidated management
		Configuration management
		Change management
	Release process	Release management
Employee training	Employee capabilities assessment	Assessment of IT resources usage capabilities
	Training	Improving security awareness
		Improving capabilities and professional knowledge
Internal audit	Review of shadow IT management plan	Establish audit plan and methodology
		Implementation and improvement

을 추가로 추가하는 것이 일반적이다.

두 번째는 개인 정보에 대한 배려가 필요하다. 관리자는 AIIMS를 통한 관리를 수행할 때 수집되는 개인 정보에 대해 어떤 정보가 수집되었으며 이를 어떻게 안전하게 관리할 것인가 하는 구조를 제대로 명시하고 그 초기 단계에서 이용자 간의 합의를 도모 할 필요가 있다. 또한 직원과의 커뮤니케이션을 강화하여 개인정보에 대한 확인 및 변경 요구사항이 있으면 취득한 정보를 공개하는 등 투명성을 유지하는 노력이 요구된다(ITR, 2012).

6. 결 론

본 연구는 최근 IT가 기업조직의 전부분에 확대되고 이용자중심으로 체계가 전환되고 있고 IT의 환경도 동태적으로 변화함에 따라 나타나는 Shadow IT를 개념적으로 파악하고 관련 논의들을 분석함으로써 Shadow IT 속성에 따른 관리 요구사항과 관리체계를 개발하고자 추진되었다.

본 연구의 요약을 연구 결과와 시사점 차원에서 정리하면 다음과 같다.

먼저 기업을 둘러싼 IT 환경이 빠르게 변화하면서 직원들은 업무를 보다 더 빠르고 유연하게 처리하기 위하여 기업에서 제공하는 IT 기기 및 네트워크 외에도 외부의 IT 자원을 사용하기 시작했다. 특히 모바일과 클라우드 환경이 확대됨에 따라 IT 자원이 기업의 적절한 감시나 통제영역을 점차 벗어나게 되었는데 이를 Shadow IT라고 한다.

이러한 Shadow IT는 혁신성, 비용-업무의 효율성, 파급성과 같은 속성을 지니고 있어 오늘날 기업의 이익 및 비즈니스 가치 향상에 기여하는 조직의 기회요소로 부상하게 되었으나 보안에 대한 낮은 인지나 무심코 사용하는 행위 등은 보안 취약점을 드러내는 등 위험을 지니고 있다. 따라서 기업에서 발생하는 Shadow IT의 문제점을 해결하고 비용-업무의 효율성과 같은 이점을 얻기 위해서는 새로운 접근의 관리방안이 요구된다.

즉 Shadow IT를 어둠(shadow)에서 빛(light)으로 이끌어내기 위해서는 기업 내부의 보안인식을 강화하고 IT 자원에 대한 적절한 관리가 이루어져야하는데 이를 위해 본고에서는 Shadow IT 평가 모델 및 새로운 IT 관리 체계(AIIMS, Advanced IT service & Information security Management System)를 제시하였다.

Shadow IT 평가 모델의 경우에는 Rentrop and Zimmermann(2012b)의 연구에서 제시된 평가 모델을 기반으로 구성한 새로운 필수 도입요소이지만 AIIMS(Advanced IT service & Information security Management System)는 기존의 기업 대상의 IT 관리체계인 ISMS, ITSMS와 동떨어진 별도의 관리체계가 아니라 ITSMS(IT Service Management)의 관리항목 기반에 Shadow IT 요소를 고려한 진화한 형태의 관리체계이다. 이렇게 구현된 평가 모델 및 관리체계는 Shadow IT의 기능 및 사용성을 크게 저해하지 않고 정보관리가 충실하게 이행될 수 있는 형태로 기업에 도입되어야 할 필요가 있다.

이상에서와 같이 본 연구는 Shadow IT 개념 논의를 체계화하였다는 점에서 학술적 관점에서 의미가 있다고 판단하며 Shadow IT 관리를 포함하여 비즈니스 효과적인 관리체계를 제시하였다는 점에서 실무적으로도 기여가 있을 것으로 기대한다.

다음에는 Shadow IT 뿐만 아니라 이를 사용하는 기업을 크기, 비즈니스 성격, IT 관리 수준에 따라 단계별로 분류하고 각각의 단계에 맞는 적절한 수준의 관리가 이루어질 수 있도록 하는 발전된 관리체계에 대한 연구가 필요하다.

References

Anderson, N., “Cisco Bring Your Own Device-Device Freedom Without”, San Jose : Cisco Systems, Inc, 2013.

Bayan, R., “Shed Light on Shadow IT Groups”, Techrepublic.com, 2004. http://www.techrepublic.com article/hed-light-on-shadow-it-

groups/5247674(Checked on July 25, 2016).

Brodin, M., "BYOD VS. CYOD-What is the Difference?", *9th IADIS International Conference Information System*, 2016.

Cio Korea, "10 Security Forecast Released by Gartner", 2016, http://www.ciokorea.com/news/30244(Checked on July 25, 2016).

Computer Weekly, "Managing Shadow IT", September, 2012.

Crump, G., "Shadow IT : Data Protection and Cloud Security", *Gigaom Research*, 2014, https://gigaom.com/report/shadow-it-data-protection-and-cloud-security(Checked on July 25, 2016).

Cui, X., B.N. Mills, R.G. Melhem, and T. Znati, "Shadows on the Cloud : An Energy-aware, Profit Maximizing Resilience Framework for Cloud Computing", CLOSER, 2014.

CXO Unplugged, "Shadow IT-Should CIOs take Umbrage?", Retrieved, 2012.

Dhingra, M., "Legal Issues in Secure Implementation of Bring Your Own Device(BYOD)", *International Conference on Information Security & Privacy*, 2015.

Digital Times, "CYOD' focus", September, 16, 2014.

Dols, T., "Influencing Factors Towards Non-compliance in Information Systems", UAS Utrecht, 2009.

Haag, S., "Appearance of Dark Clouds?-An Empirical Analysis of Users' Shadow Sourcing of Cloud Services", 2015.

Hasegawa, T. and M. Nakano, "From ISMS to ITSMS", 2012.

ITR, "Mobile Security-Stand up to Hidden Use Shadow IT", ITR White Paper, 2012, https://www.itr.co.jp/library/whitepaper/ITR_WP_C12090043-pdf.html(Checked on July 25, 2016).

JIPDEC, "CSMS(Cyber Security Management System-Overview of the Conformity Assessment System)", 2014a.

JIPDEC, "IT Service Management System-Overview of the Conformity Assessment System", 2014b.

JIPDEC, "Prescription of as a Service era-IT Service Management System(Second edition)", 2014c.

Kim, H., "A Case Study on Realization of ITSM Performance Applying the Change Management Framework of ITSM", *Journal of Information Technology Services,* Vol.10, No. 3, 2011, 251-264.

Kobayashi, K., "Utilized for Business-consumer IT", *Nomura Research Institute IT Solutions Frontier*, Vol.12, 2011, 78-81.

Kushwaha, P., "Amalgamation of the Information Security Management System with Business-Paradigm Shif", *International Journal of Computer Science and Information Security(IJCSIS)*, Vol.14, No.1, 2016.

McAfee, "The Hidden Truth Behind Shadow IT-Six Trends Impacting Your Security Posture", Stratecast Frost & Sullivan, 2013.

Protiviti, "Making Shadow IT Work for You : What Financial Companies Can Do to Bring Grassroots IT Solutions Into the Fold", 2014.

Raden, N., "Shedding Light on Shadow IT : Is Excel Running Your Business?", DSSResources.com, 2005.

Rentrop, C., O. Laak, and M. Mevius, "Schatten-IT : Ein Thema Für Die Interne Revision", *Revisionspraxis-Journal für Revisoren, Wirtschaftsprüfer, IT-Sicherheits-und Datenschutzbeauftragte,* 2011, 68-76.

Rentrop, C. and S. Zimmermann, "Shadow IT : Management and Control of Unofficial IT",

ICDS 2012 : The Sixth International Conference on Digital Society, 2012a, 98-102.

Rentrop, C. and S. Zimmermann, "Shadow IT Evaluation Model", *Proceedings of the Federated Conference on Computer Science and Information Systems*, 2012b, 1023-1027.

Schaffner, M., "IT Needs to Become More Like 'Shadow IT", 2007. http://mikeschaffner.typepad.com/michael_schaffner/2007/01/we_need_more_sh.html(Checked on July 25, 2016).

Sherman, R., "Shedding Light on Data Shadow Systems", Information Management Online, 2004, http://www.information-management.com/news/1002617-1.html(Checked on July 25, 2016)

Shumarova, E. and P.A. Swatman, "Informal e-Collaboration Channels : Shedding light on "Shadow CIT", *eCollaboration : Overcoming Boundaries through Multi-Channel Interaction, 21st Bled eConference*, 2008, 371-394.

TechTarget, "NASA's shadow IT Issues with Cloud Computing all too Common", 2013.

TechTarget, "Bring Your Own Apps(BYOA)", 2014.

Yun, H., W.J. Kettinger, and C.C. Lee, "A New Open Door : The Smartphone's Impact on Work-to-Life Conflict, Stress, and Resistance", *International Journal of Electronic Commerce*, Vol.16, No.4, 2012, 121-152.

About the Authors

Jiyeon Yoo (yooo@smu.ac.kr)

Jiyeon Yoo is currently a Professor of Sangmyung University. She received her Ph.D. in Information Management Engineering from Korea University. Her current research interests include Information Strategy, IT Management System, and Cyber Security, etc.

Nayoung Jeong (nayoung9299@hanmail.net)

Nayoung Jeong is currently enrolled in a Masters degree in Graduate School of business, Sangmyung University. Her research interests are in areas of IT Management System, Risk Management, and Information Security.