https://doi.org/10.33778/kcsa.2019.19.4.107

데이터보안인증을 위한 DSMS 프레임워크 구축 연구

유 승 재*

ABSTRACT

데이터보안(Data Security)이란 데이터 및 정보자산의 접근, 활용에 대한 적절한 인증과 권한의 감사를 위하여 보안 정책 및 절차를 기획, 구축, 실행하는 것이다. 또한 내·외부 네트워크, 서버, 어플리케이션 등을 통해 서비스되는 데이터는 정보보호의 핵심 대상으로서 데이터베이스와 데이터의정보보안의 범주에서 DB와 DB내에 저장된 데이터의 보호에 특화하여 집중하는 것이라 할 수 있다. 이 연구에서는 데이터보안 인증체계와 미국의 연방보안관리법(FISMA)을 기반으로 한 적절한 데이터보안관리체계(DSMS, Data Security Management System) 모델 설계를 위한 기초연구를 진행한다. ISO27001, NIST의 Cybersecurity Framework 등 주요보안인증 제도를 살펴보고 또한 현재 개인데이터 유출방지와 기업보안강화를 위한 보안플랫폼으로 구현된 데이터보안매니저 솔루션에 구현된 상태를 연구한다.

A Study on DSMS Framework for Data Security Certification

Seung Jae Yoo*

ABSTRACT

Data security is the planning, implementation and implementation of security policies and procedures for the proper audit and authorization of access to and use of data and information assets. In addition, data serviced through internal / external networks, servers, applications, etc. are the core objects of information protection and can be said to focus on the protection of data stored in DB and DB in the category of information security of database and data. This study is a preliminary study to design a proper Data Security Management System (DSMS) model based on the data security certification system and the US Federal Security Management Act (FISMA). And we study the major security certification systems such as ISO27001 and NIST's Cybersecurity Framework, and also study the state of implementation in the data security manager solution that is currently implemented as a security platform for preventing personal data leakage and strengthening corporate security

Key words : DSMS, Data Security, Security Policy

접수일(2019년 8월 30일), 게재확정일(2019년 9월 21일)

This paper was supported by Joongbu University Research & Development Fund, in 2019

* 중부대학교 정보보호학과

1. 서 론

데이터보안(Data Security)이란 데이터 및 정보자산의 접근, 활용에 대한 적절한 인증과 권한의 감사를 위하여 보안정책 및 절차를 기획, 구축, 실행하는 것이다. 또한 내·외부 네트워크, 서버, 어플리케이션 등을 통해 서비스되는 데이터는 정보보호의 핵심 대상으로서 데이터베이스와 데이터의정보보안의 범주에서 DB와 DB내에 저장된 데이터의 보호에 특화하여 집중하는 것이라 할 수 있다.

데이터보안(Data Security)이란 데이터 및 정보자산의 접근, 활용에 대한 적절한 인증과 권한의 감사를 위하여 보안정책 및 절차를 기획, 구축, 실행하는 것이다. 또한 내·외부 네트워크, 서버, 어플리케이션 등을 통해 서비스되는 데이터는 정보보호의 핵심 대상으로서 데이터베이스와 데이터의정보보안의 범주에서 DB와 DB내에 저장된 데이터의 보호에 특화하여 집중하는 것이라 할 수 있다. 데이터보안의 목적은 DB 내 데이터에 대한 내●외부 위협으로부터 기밀성, 무결성, 가용성을 유지하고 책임추적성을 확보하여 데이터 소유자의 권리를 보호하고 주장할 수 있도록 하는 것이다.

이 연구에서는 데이터보안 인증체계와 미국의 연방보안관리법(FISMA)을 기반으로 한 적절한 데이터보안관리체계(DSMS, Data Security Management System) 모델 설계를 위한 기초연구를 진행한다. ISO27001, NIST의 Cybersecurity Framework 등 주요보안인증 제도를 살펴보고 또한 현재 개인데이터 유출방지와 기업보안강화를 위한 보안플랫폼으로 구현된 데이터보안매니저 솔루션에 구현된 상태를 연구한다.

2. 관련연구

오늘날 기업의 데이터 유출사고는 막대한 비용부담을 유발하는 것은 물론 기업의 존폐를 위협할 정도의 심각한 이슈라 할 수 있다. 그로 인해 기업이 데이터 유출 피해를 처리하고 복구하기 위해 지불하는 비용은 해마다 급격히 상승하고 있는데, McAfee에 따르면 지난 2년 동안에만 23%이상의 상승을 보이고 있다.

데이터유출을 유발하는 가장 대표적인 원인으로 점점 진화되고 정교해지고 있는 악성코드를 꼽을 수 있다. 이에 대한 대응으로서 네트워크나 시스템에서 접근통제에 의존하는 그동안의 방편을 개선하여 강력한 암호화는 물론 엔드포인트에서부터 응용프로그램에 이르는 사용자에 대한 전반적인 보안관리체계 구축을 제시하고 있다. [11]

기업의 비즈니스 차원에서 데이터유출방지는 가장 기본적으로 요구되는 사안으로서 비즈니스의 차별화와 경쟁력 유지의 핵심적인 요소로 인식되고 있다. 특히 민감한 데이터 보호는 법적 또는 윤리적 이유 뿐 만 아니라 개인의 프라이버시 또는 비즈니스 명성 관리에 있어서 강조되고 있는 이슈이다.

CoSoSys에서는 이와 관련하여 데이터유출을 예방하기 위한 방법으로 보안기술 투자, 보안인식교육, 데이터 보호규정 준수, 정기적인 취약성 평가 및 데이터 위반대응 프로세스 구축 등을 프레임워크 구성요소를 제시하고 있다. [3][13]

일반적으로 데이터보안 강화를 위해 제시되는 방법으로 공통적인 이슈는 다음과 같이 데이터 보안 대책이 신뢰할 수 있는 승인된 당사자만 데이터에 액세스하도록 초점을 두고 있다.[8]

먼저 중요 데이터를 파악하는 것이고, 다음으로 관리자의 권한범위를 제한하고 안정적인 데이터베이스 관리를 위하여 크리덴셜 정리하는 것이다. 그 다음으로 Firewall, VPN, IPSec 기타 액세스관리도구를 이용하여 내부 보안경계선 관리를 엄격히 규정하며, 항상 데이터를 암호화 상태로 유지하고 사용자를 보호하는 것을 중요한 요소로 제시되고 있다.

데이터식별	가시성확보	정책위반문제해결
데이터보호기술	Data Protect/Leak prevention	
	Encryption	
데이터보안확장	Endpoint/Sever	
	Cloud Service	
보안정책간소화	Centric Security Management	
외부접근제어	Encryption Management	

[표 1]M사 데이터보안 프레임워크[9]

위 [표1]에서 보는 바와 같이 데이터보안관리를 위해 설계된 외산 M사의 주요 프레임워크는 데이터 보호

암호기술 구현과 데이터 보안 확장, 부당한 외부로부터 엑세스한 데이터를 사용할 수 없도록 하는 드라이브 잠금 및 암호화 관리 그리고 중앙보안관리 플랫폼에서 지원하도록 하는 정책의 간소화 등으로 구성되어 있다.

일반적으로 보안기술은 외부로부터의 침입이나 내부 사용자에 의한 데이터 유출을 네트워크 또는 시스템 레벨에서 차단하는 경계선 기반 보안 솔루션이 주를 이루고 있다, 하지만 대부분의 데이터유출은 내부직원, 퇴직자 또는 협력업체 직원 등을 통하여 발생되고 있어 경계선 기반 보안에 의한 대응으로는 데이터 자체를 원천적으로 보호하는데 한계가 있다고 할 수 있다. 따라서 데이터 자체에 대한 보안을 위해 데이터가 라이프사이클 상의 각 과정마다 개별 정책에 의해 보호될 수 있도록 하는 적절한 보안모델이 구현될 필요가 있다. 해야 합니다.

비정형데이터 자동분류 및 저장관리, 강력한 암호화 그리고 사용자 행동기반 분석의 주요기능으로 구성되어 있는 F사의 데이터보안 프레임워크는 다음 [표 2]와 같이 설계되어 있다.

Risk Management	리스크 분석 및 시각화		
	문서사용 모니터링 및 추적		
Policy Enforcement	예외정책관리		
	DRM		모바일 보안
	문서보안	PC	출력물 보안
		Sever	웹 콘텐츠 보안
		외부전달문서	화면 보안
Data Discovery	데이터 식별 및 분류		

[표 2]F사 Data Security Framework(1) [7]

데이터 보안 정책은 데이터 중심, 사용자 중심으로 적용하되 조직 내에 존재할 수밖에 없는 어떠한 예외정책에 의해서도 보안상 허점이 노출되니 않도록 관리가 수반되어야 할 것이다. 또한 [그림 1]의 프레임워크 다이아그램을 볼 때, 이 프레임워크는 APT 공격 등 지능형 해킹은 물론 내부자에 의한 위협에도 대응할 수 있는 데이터 중심 보안 및 사람 위주의 정책을 기반으로 하는 멀티 레벨 보안 아키텍처로 소개되고 있다.

[그림1]F사 Data Security Framework Diagram(2)[7]

Data Discovery 프레임은 여러 장소에 분산 저장되어 관리가 어려운 비정형 데이터들을 자동으로 찾아내고 분류하여, 중요 문서들을 지속적으로 보호하며 관리하는 기능이 포함된다. 그리고 Police Enforcement 프레임은 예외정책, DRM과 문서보안 영역으로 중요 문서 암호화와 사용자 또는 그룹 별로 권한/접근제어를 통해 데이터 보안 구현기능이 포함된다. Risk Management프레임은 위험분석, 문서사용 모니터링과 추적을 통해 사전에 위협에 대응할 수 있는 기능으로 구성된다.

3. 데이터보안 인증체계 동향

(1) FISMA

FISMA(Federal Information Security Management Act)는 2002년 제정된 연방 데이터 보안 표준 및 지침에 대한 가장 중요한 규정 중 하나이다. 정보 보안에 대한 연방 지출을 관리하면서 연방 정보 및 데이터에 대한 보안 위험을 줄이기 위해 도입되었다. [그림2]와 [표3]에서 볼 수 있듯이 이러한 목표를 달성하기 위해 FISMA는 연방 기관이 충족해야하는 일련의 지침 및 보안 표준을 설정했다.

[그림 2] FISMA Framework [12][14]

구분	내용
step1	손실의 잠재적 영향에 따라 정보 시스템의 중요도 / 민감도 정의
step2	정보 시스템을 보호하기 위해 최소 보안 통제를 선택; 적절한 조정 지침을 적용
step3	필요에 따라 맞춤형 보안 통제 기준을 보완하여 적절한 보안 및 실사를 보장하기 위해 위험 평가 결과를 사용
step4	정보보안 계획서, 정보시스템에 대한 보안 요구사항 및 계획되거나 시행 중인 보안 통제사항 문서화
step5	보안 통제 구현; 보안 구성 설정 적용
step6	보안 통제 효과 확인(예: 올바르게 구현된 제어 장치, 의도한 대로 작동, 보안 요구 사항 충족
step7	기관 운영, 기관 자산 또는 개인에 대한 위험 결정 및 허용 가능한 경우 정보 시스템 운영 승인
step8	보안 통제에 영향을 미치고 통제 효과를 재평가 할 수 있는 정보 시스템의 변경 사항을 지속적으로 추적

[표 3] FISMA Framework 구성[12][14]

그리고 FISMA 컴플라이언스 요구사항에는 정보 시스템 인벤토리, 위험 분류, 시스템 보안 계획, 보안 제어, 위험 평가 그리고 인증 및 인증 등이 우선적으로 포함되고 있다.

미국 연방정보보안관리법(FISMA)는 2014년 12월에 연방정보보안현대화법(FISMA2014)으로 개정되었었는데, 변경된 FISMA(Federal Information Security Modernization Act of 2014)는 기존의 FISMA를 현대화하여 개정하였음을 명명하도록 하기 위해 기존의 관리(Management)를 현대화(Modernization)로 용어 변경하였다.

주요변경사항으로는 국토안보부(DHS)장관에게 할당된 책임, 기관 보고요구사항, 보안사고에 대한 새로운 지침 및 보고요구사항, 데이터 유출 알림에 대한 정책 및 지침 등을 체계화 또는 신규적용한 점이 주요변경사항으로 파악된다. [6]

(2) NIST CyberSecurity Framework

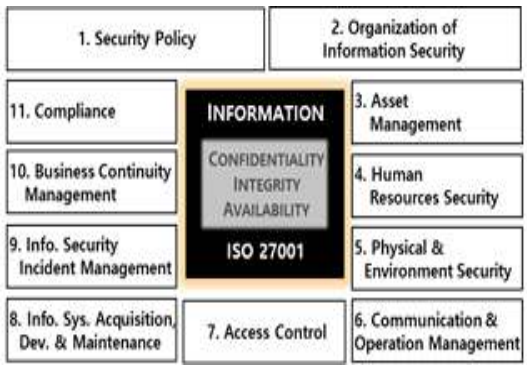
사이버 보안 프레임 워크를 구성하는 핵심요소는 프레임워크 코어, 구현계층, 프로파일이다. 아래 [그림 3]에서 볼 수 있듯이 사이버 보안 활동 및 결과를 나열하여 조직이 기존 정책 및 절차를 보완하면서 위험을 완화하게 하는 프레임 워크 코어, 조직에 사이버 보안 이니셔티브를 얼마나 적극적으로 추진해야하는지 결정하는 데 필요한 정보를 제공하는 구현 계층 그리고 조직의 목표, 요구 사항, 위험 식욕 및 자원을 원하는 프레임 워크 코어의 결과와 비교하여 고유하게 비교할 수 있도록 하는 프로파일로 구성되어 있다.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

[그림 3] NIST Cybesecurity Framework [5][6]

Framework Core는 식별, 보호, 감지, 응답 및 복구기능으로 구분되고 있다. 여기에는 22개의 관련 카테고리와 98 서브카테고리로 구분되어 있는데 일부 ISO 27001 Annex A의 구성과 유사한 부분이 있다 또한 각 서브카테고리에는 ISO 27001, COBIT, NIST SP 800-53, ISA 62443 및 CCS CSC와 같은 다른 프레임워크에 대한 몇 가지 참조가 있어 사이버 보안 요구사항의 이해와 구현 방법을 손쉽게 참조할 수 있다.
프레임 워크 구현 단계 (부분, 위험 정보, 반복 가능 및 적응)는 조직의 특성을 고려하여 사이버 보안 구현의 정도를 다양하게 조정할 수 있도록 한다.[5]
프레임 워크 프로파일(예 : 현재 프로파일, 대상 프로파일)은 조직이 현재 있는 상태, Framework Core의 카테고리 및 하위 카테고리와 관련하여 원하는 위치를 쉽게 파악할 수 있게 함으로써 선택적 계층적 실천 계획 수립을 용이하게 한다. NIST 사이버 보안 프레임 워크는 비용 효율적인 측면에서 장점을 가지고 있으며 이를 통해 조직은 강력한 보호 기능과 강화된 사이버 보안 정책 제공하는 프레임워크로 평가된다.

(3) ISO 27001에 기반한 데이터보안 전략
ISO27001은 [그림4]와 같이 정보보호관리시스템 요구사항을 정의한 국제표준으로 기업의 비즈니스 활동과 관련하여 창출된 유·무형의 정보들의 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)을 보장하여, 기업활동에 기여할 수 있도록 보장하기 위해 정보보안시스템을 수립하고 이행 및 운영하며 감시, 검토, 유지, 개선하기 위한 관리시스템이라 할 수 있다.



[그림 4] ISO27001 Framework

사업상의 손실 최소화와 비즈니스 연속성을 보장하여 전반적인 보안활동 개선, 지속적 개선에 기여, 수익 및 사업기회 증대에 기여하는 역할을 한다. 그럼으로써 국제 표준에 따른 정보보안 리스크 관리체계 개선을 통한 실질적인 정보보안 수준 향상하고 정보보안 관리시스템의 국제규격 부합여부를 제3자에 의한 독립적, 객관적인 평가/인증으로 고객의 신뢰감 향상 그리고 정보보안에 대한 법적 및 계약 요구사항에 대한 적합성 향상을 기대할 수 있다.
다음은 NIST의 사이버보안 프레임워크와 ISO27001 사이에 그 특징에 따른 공통점과 차이점을 살펴본 것이다.
사이버 보안 프레임 워크 (Cybersecurity Framework) 는 2013 년부터 미국 대통령의 중대 인프라 사이버 보안 개선 명령을 따르며, 중요한 인프라의 일부로 간주되는 미국 기업을 위해 처음 고안되었지만 사이버 보안 위험에 직면 한 모든 조직에서 사용하기에 적합하며 자발적이다.
ISO/IEC27001은 국제표준화기구(International Organization for Standardization)가 2005 년에 발표하고 2013년에 개정된 정보보안표준이다. 필수는 아니지만 대부분의 국가에서 정보 보안/사이버보안 구현을 위한 사실상의 기본 프레임 워크로 인정된다.
아래의 [표 4]는 Cyber Security Framework과 ISO27001 비교한 것이다.

특징	Cybersecurity Framework	ISO27001
장점	계획 및 구현과 관련하여 상대적으로 더욱 명확하게 구성	인증획득 함으로써 기관이 객관적으로 안전한 정보보호 신뢰확보
공통	▪ 조직에서 정보보안 또는 사이버보안을 구현하는 방법에 대한 방법론을 제공 ▪ 기술 중립적 ▪ 모든 유형의 조직에 적용 ▪ 법적 및 규제 요구사항과 모든 이해당사자의 요구 사항을 준수하면서 비즈니스 목표를 달성 ▪ 사이버보안 위험이 탐지 된 경우에만 보호기능을 구현하는 위험관리를 기반으로 함.	

[표 4] Cyber Security Framework과 ISO27001 비교

이들 둘 사이의 공통점으로 가장 중요한 것은 모두 조직에서 정보보안 또는 사이버보안을 구현하는 방법에 대한 방법론을 제공한다는 것이다. 둘 다 기술 중립적이며 모든 유형의 조직에 적용 할 수 있으며, 법적 및 규제 요구 사항과 모든 이해 당사자의 요구 사항을 준수하면서 비즈니스 목표를 달성하도록 한다. 그리고 양쪽 둘 다 사이버보안 위험이 탐지 된 경우에만 보호기능을 구현하는 위험관리를 기반으로 한다. 이들의 차이점으로는 Cybersecurity 측면에서 볼 때 계획 및 구현과 관련하여 상대적으로 더욱 명확하게 구성되어있다고 할 수 있다.

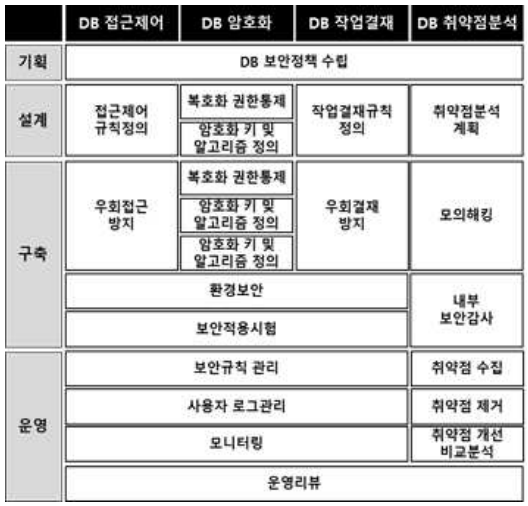
Framework Core, 프레임 워크 구현 단계, 프레임 워크 프로파일 등의 구성이 명확하여 사이버 보안 프레임 워크를 통해 최고 경영진뿐만 아니라 엔지니어 및 기타 IT 직원도 구현 대상과 그 격차를 이해하는 것이 용이하다. 그 차이점을 ISO27001 측면에서 볼 때 해당 기관이 인증을 받을 수 있다는 것으로서 대내외 관련 주체에게 정보를 안전하게 유지하고 있음을 객관적으로 입증하는 효과를 거둘 수 있다는 것이다.

또한 ISO 27001은 국제적으로 인정되고 인정되는 표준으로써, 미국 이외의 국가의 고객, 파트너 및 정부에 대한 능력을 입증하려는 경우 선택할 수 있는 프레임워크라 할 수 있다. ISO 27001은 Cybersecurity Framework와 달리 필요한 문서 및 레코드와 구현해야하는 최소값을 명확하게 정의한다.

마지막으로, 프레임 워크는 사이버 보안을 계획하고 구현하는 방법에만 초점을 맞추고 있지만 ISO 27001은 훨씬 광범위한 접근 방식을 취한다. 방법론은 PDCA(Plan-Do-Check-Act) 주기를 기반으로 함으로써 사이버 보안을 계획하고 구현할 뿐 아니라 전체 시스템을 유지 관리하고 개선하는 과정을 포함한다.[5]

(4) DQC-S (Data Quality Certification Security)

DQC-S는 한국데이터베이스진흥원에서 주관하는 데이터품질인증(DQC) 중에서 데이터베이스를 대상으로 [그림 5]와 같이 접근제어, 암호화, 작업결재 및 취약점분석 등의 전반적인 보안기술 요소를 인증하는 데이터보안인증이다.



[그림 5] 데이터 보안 프레임워크 [9]

4. 결론

앞에서 살펴보았듯이 ISO 27001은 다양한 정보 보안 방법론에 매우 적합한 프레임워크이며 Cybersecurity Framework는 다른 프로그램이나 시스템을 쉽게 보완할 수 있는 것으로 평가된다. 따라서 사이버 보안 프레임 워크는 구현 될 보안 영역을 구성 할 때와 달성해야 할 보안 프로파일을 정확하게 정의 할 때 경우에, 그리고 ISO 27001은 장기적이고 종합적인 설계에 효과적이라 할 수 있으므로 두 가지의 병행과 결합의 가능성에 따라 매우 적합한 효과를 발휘할 수 있을 것으로 기대된다. [5]

4차 산업혁명의 핵심키워드로 제시되는 IoT와 빅데이터 이슈는 엄청난 디지털 데이터를 생산의 요인이 됨이 자명할 것인데, 이러한 디지털데이터의 폭발적인 증가에 따른 적절한 대응전략이 요구된다. 특히 클라우드 환경에서의 민감데이터유출 위협은 데이터보안에서 필수적인 과제가 될 것이다. 나아가 글로벌스텐다드로 인정되는 EU의 개인정보보호규정 GDPR(General Data Protection Regulation)이 지속적으로 강화되고 있는 것 또한 데이터보안을 위한 프레임워크의 개선을 촉구하는 이유가 될 것이다.

반면 비즈니스 관점에서 개선되는 데이터보호 프레임워크 구성이 기업과 직원의 생산성에 반하는 결과를 초래하는 것은 부정적인 요인이 될 수 있음을 고려해

야 할 것이다. 데이터의 유형과 민감도를 고려한 적절한 관리시스템이 필요하며 규정준수와 제로트러스트 시각에서의 데이터 위반보호를 위한 조치도 반영된 프레임워크가 설계되어야 할 것이다

참고문헌

[1] 김민준, 김귀남 “정보보안거버넌스 프레임워크에 관한 연구”, 융합보안논문지 제10권 제4호, pp.13-19, 2015

[2] 노시춘, “BMO기법을 활용한 정보보안 비즈모델 평가시스템 소프트웨어 아키텍처 설계방법”, 융합보안논문지 제13권 제3호, pp.71-77, 2013.

[3] 2019년 데이터 유출 예방을 위한 5가지 방법 (http://blog.naver.com/cososyskorea/221461085833)

[4] 한국데이터베이스진흥원, “데이터베이스보안 가이드라인”, 2011

[5] https://advisera.com/27001academy/

[6] http://www.natlawreview.com/ & https://www.boho.or.kr/

[7] https://fasoo.com/solutions/fasoo-data-security-framework

[8] http://www.itworld.co.kr/news/99457

[9] https://www.mcafee.com/enterprise/ko-kr/solutions/prevent-data-breaches.html

[10] http://www.itworld.co.kr/news/99457

[11] https://www.mcafee.com

[12] Veracode, “Understanding NIST 800 37 FISMA Requirements” 2008.

[13] http://cososys.kr/

[14] https://linfordco.com/blog/fisma-compliance

〔저자소개〕

유 승 재 (Seung-Jae Yoo)
1988년 2월 동국대학교 이학사
1990년 2월 동국대학교 이학석사
1998년 2월 동국대학교 이학박사
1997년 3월 ~ 현재 중부대학교 정보보호학과 교수
email : sjyoo@joongbu.ac.kr