Regular paper

Journal of the KIECS. pp. 601-608, vol. 13, no. 3, Jun. 30 2018, t. 89, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2018.13.3.601

정보보안과 개인정보보호 간의 이원화 보안범주의 상호연계 및 통합에 따른 보안성 증대에 대한 연구

서우석*

A Study on Increasing Security Following Mutual Interaction and Integration of Dualized Security Category between Information Security and Personal Information Protection

Woo-Seok Seo*

요 약

공공기관 개인정보보호에 관한 법률이 제정되고 개정 되는 단계를 거치는 동안 정보보안에 관한 지침과 법률은 특정 기관에 중점적으로 반영되고 수축 및 실현되고 있었다. 상호 법률과 지침은 거시적인 정보라는 자산과 개인식별정보라는 자산에 대한 상호 다른 매체정보에 대한 보안을 목적으로 이원화 되어 적용되고 실현되어 왔다. 그러나 2017년 4차 산업혁명에 대한 정의와 방향 그리고 21세기 최고의 안전선을 확보하는 보안에 대한 다양한 제품과 솔루션 그리고 이런 모든 분야를 아우르는 제3의 기술을 제시하기 위해 IOT(: Internet of Things), ICT(Internet of Things), ICT Cloud, AI(: Artificial Intelligence) 등 마치 장난감 플라스틱 인형을 주물로 마구 만들어내 듯이 보안 시장에 쏟아져 들어오고 있는 상황이다. 이때 과거와는 다른 보안상의 범주에 두 가지 중요 영역에 준하는 정보보안과 개인정보보안 이라는 이원화된 물리적, 관리적, 논리적, 심리적 차이를 보이는 보안에 대한 상호연계성 보장과 통합적 관리 및 기술적용을 위한 보안성 증대에 대한 필요성이 대두되어짐에 따라 두 경우의 상호관계를 분석하고 이를 제안된 연구결과에 적용함으로써 최적의 보안성을 확보하는 연구를 하고자 한다.

ABSTRACT

While the legislation on the protection of personal information in public institutions was enacted and amended, the guidelines and laws on information security were focused, contracted and realized with focus on specific institutions. Mutual laws and guidelines have been applied and realized for the dual purpose of securing both the asset of macroscopic information and the asset of personally identification information, which are mutually different media information. However, in a bid to present the definition and direction of the fourth industrial revolution in 2017, a variety of products and solutions for security designed to ensure the best safety line of the 21st century, and the third technology with the comprehensive coverage for all these fields, a number of solutions and technologies, including IOT(: Internet of Things), ICT Internet of Things(: ICT), ICT Cloud, and AI (: Artificial Intelligence) are pouring into the security market as if plastic doll toys were manufactured in massive scale into the market. With the rising need for guaranteeing the interrelation for securities with dualistic physical, administrative, logical and psychological differences, that is, information security and personal information security that are classified into two main categories and for the enhanced security for integrated management and technical application, the study aims to acquire the optimal security by analyzing the interrelationship between the two cases and applying it to the study results.

키워드

Information Security, Interconnection, Integration, Personal Information Security, Policy, Safety Secure
정보 보안, 상호 연결, 통합, 개인 정보 보안, 정책, 안전 보안

* 교신저자 : 보안컨설턴트(프리랜서)
• 접 수 일 : 2018. 03. 28
• 수정완료일 : 2018. 05. 06
• 게재확정일 : 2018. 06. 15
• Received : Mar. 28, 2018, Revised : May. 06, 2018, Accepted : Jun. 15, 2018
• Corresponding Author : Woo-Seok Seo
Security Consulting, Gyeonggi-do R&D laboratory
Email : ssws2000@nate.com

Ⅰ. 서 론

2018년 각 종 포털사이트 및 기업에서 제공되는 전자적 사전에 따른 정보보안의 사전적 정의는 정보의 라이프 사이클에 따른 첫 단계인 정보의 수집을 시작으로 보유한 정보에 대한 2차 또는 3차 가공과 지속관리를 위한 저장 및 보유와 DB화한 정보에 대한 검색 그리고 상호 정보교류를 위한 업무 결과를 위한 송신과 수신의 통신과정과 파기에 이르기까지의 변조, 훼손, 노출, 유출 등과 같은 손실과 장애를 방지하기 위한 물리적이고 관리적인 부분과 논리적인 안전보장을 기반으로 하는 기술적 방법의 적용과 운영에 따른 유지관리를 의미한다[1-3].

이처럼 정보보안의 범주는 과거 단순한 판단과 1차원적인 현상에 대한 각각의 개별 안전성을 보장하는 단계에서 넘어선 상식선의 의미를 나타내는 사고 가능한 범주 이상의 광범위한 영역과 사고의 부분까지를 영역으로 정의를 하고 있다. 그러나 정보보안과 정보보안의 한 영역으로 자리 잡고 그 의미와 안전성 확보의 범주를 별도로 전문화한 개인정보보호는 정의뿐만 아니라 그 대상의 범주와 역할 그리고 관리와 기술적 보안의 성격과 형태가 이질적인 부분으로 상호 연계성이 다소 낮은 편이다.

그러나 두 가지 보안에 대한 연계성 또한 완전히 배제할 수 있는 부분은 아니며, 이를 상호 연계범주로 정의하고 이들이 공유하는 보안에 대한 정책을 상호관리 및 일원화함에 따라 정책적인 경비와 소요시간에 대한 부분을 효율성과 비례하게 관리하고자 한다[4-5].

따라서 본 논문에서는 이러한 공통된 보안정책에 대한 기준을 표준화하고 상호 보안을 유지하고 관리해야할 정보자산에 대한 기준 또한 정의하는 과정을 통해 이질적인 정책을 일원화하고 공통된 정책의 활용 절차를 표준화하는 부분을 제안하고자 한다.

이러한 제안과정을 본 논문에서는 1장에서는 연구의 개요와 목적을 2장에서는 상호 정보자산에 대한 보안의 이질적인 정책의 기반기술 현황과 3장에서는 보안정책 표준화와 일원화를 기반으로 발생 가능한 효율성의 극대화 성과를 제시하고 4장에서는 제안한 표준 정책을 실현하고 실무에 적용해 보는 과정을 실현함으로써 마지막 5장에서 제안결과를 최종 기술 및 제안하고자 한다.

Ⅱ. 관련연구

본 관련연구에서 제안하고자 하는 내용은 많은 기업과 기관에서 정보보안과 개인정보보호를 별개의 보안 정책으로 구성하고 물리적, 관리적, 논리적인 3차원의 관리 범주까지 별개로 구성하고 운영하는 그리고 관리 주체의 조직까지 이원화 하는 등의 일련의 행동 패턴과 정책적 부분의 관련 지침과 실현 및 적용을 개별적으로 이질화 시켜 준수하는데 발생하는 비효율적인 관리에 대한 부분을 하나의 공통된 자산관리 영역을 구성함으로써 공통 정보자산에 대한 공통정책을 제안하고자 하는데 있다.

2.1 정보보안의 이슈와 시장변화 현황

기관과 기업에서 언급한 정보보안의 정통적인 관리패턴은 정보자산의 목적, 운영, 유지, 파기 등과 같은 일련의 흐름에 따른 분류나 등급 등과 같은 세부적인 자산의 구분을 통해 각각의 단계별 보안성에 대한 분류를 세부 대응 정책 또는 지침을 정하고 이를 상황별 대응하는 단계가 아닌 개별 상황에서 발생되는 문제점들을 각각의 개별적인 정보자산에 대한 임의의 보안 및 자산등급을 부여하고 위험도와 중요도에 따른 관리를 시행함으로써 보안성을 확대 및 효율성까지 극대화하는 수준에 까지 이르게 되었다[6-7].

이와 같은 위험도와 중요도에 따른 정보자산에 대한 세부분류는 정보보안을 유지하고 관리하는 차원에서 정보자산에 대한 생성으로부터 최종 목적을 위한 결과를 도출한 이후 파기되는 라이프 사이클을 만들어서 관리하는 과정으로 발전했다.

다만, 정책과 지침 등은 가변성을 보존 가능한 계획 및 기획으로 가장 기본적인 필요조건에 해당되는 부분에 대해서만 라이프 사이클에 그 단계를 언급하고 있다. 이는 정보보안에 대한 기술적인 진보가 시시각각 변하는 시장의 상황을 반영한 정책적 실용성을 확보하고 적절한 최적의 대응과 안전성을 극대화하기 위한 방안으로 볼 수 있다.

*** 정보보안의 라이프 사이클과 개요**

1. 정보의 수집 : 정보시스템과 정보보호시스템 및 정보(중요도에 따른 기관과 기업 내부의 인위적인 구분 또는 식별 정보자산)의 모음을 의미

2. 정보의 가공 : 시스템으로부터 자동화 되어 생성된 자산에 대한 2, 3차 변형과 보완 및 수정에 따른 가공을 의미하며, 이는 업무 또는 활용을 통한 결과를 얻기 위한 일련의 과정을 의미하기도 함

3. 정보의 저장 : 정보의 저장은 단순 결과에 대한 원본 정보 저장과 지속적으로 실시간 가공되어 변형되는 정보자산의 저장으로 분리 구성하며, 저장의 궁극적 의미는 같음

4. 정보의 검색 : “3번”의 저장된 2가지 정보자산에 대한 검색을 의미 (* 단, 실시간 정보자산의 경우는 검색의 단계를 다시 2개의 단계로 특정시점 검색과 변형시점 검색으로 인위적 구분하는 기관도 있음. 따라서 다양한 검색의 논리로 접근이 가능함)

5. 정보의 통신(송신과 수신) : 단일 기관 내에서 정보시스템 간의 통신, 정보보호시스템 간의 통신을 의미 (* 원천적으로 대외 정보자산의 송 · 수신 불가)

6. 정보의 파기 : 개인정보와 같은 라이프 사이클에서 언급하는 파기의 경우는 정보 및 DB 상의 Instance를 의미하고 있으나, 정보보안의 경우는 다양한 정보 및 DB를 담고 있는 정보처리 시스템에 대한 물리적인 파기까지도 의미함 (* H/W, S/W 일괄 파기 의미)

표 1의 경우와 같이 정보보안의 Attack-Cycle의 경우는 5가지 위협요소에 대해서 변형도 기준에 따른 손실 도를 발생시키는 객관적 수치를 제시한다.

표 1. 정보보안의 Attack-Cycle과 개요(변형도 기준)
Table 1. Attack-cycle and outline of information security (based on degree of transformation)

division	Content
Damage	More than 95% loss due to deformation
Modulation	More than 80% loss due to deformation
Forgery	More than 100% loss due to deformation
Spill and Exposure	Losses due to objective outflow figures also need to be revalued

2.2 개인정보보안 형태의 안전성 지침 현황

정보보안과 이원화 되어 연계 및 융합된 공통정책의 수립과 운영을 통한 효율성 확보를 위해서는 과거 공공기관 개인정보보호에 대한 법률 등과 같은 공공기관이 시작한 개인에 대한 식별정보를 정보자산으로 분류하고 관리 및 안전성을 보장하던 법률과 지침이 개인정보보호법으로 제정되면서 6차례 이상의 개정과 변화를 통해 2018년 현재의 안전성을 확보하는 법률로 완성되어 적용되고 있는 부분에 대해서 명확하게 파악하고 그림 1과 같이 라이프 사이클을 기준으로 단계적으로 정보보안에 대한 정책들과의 비교와 확인 작업이 동반되어야 한다. 이를 상호연계 및 통합에 따른 물리적, 관리적 보안성을 보장하는 형태로 확장시키는 부분에 대한 검토 또한 필요하다[8].

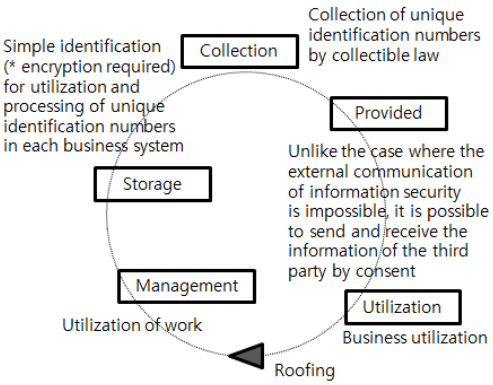

그림 1. 정보수집과 활용을 위한 단계적 절차
Fig. 1 Step-by-step procedures for collecting and using information

*** 개인정보보호 Attack-Cycle과 개요(위험도 기준)**

- 개인정보의 경우는 정보자산과는 달리 각 개별 개인에 대한 1:1 정보자산으로 위험도는 각 Attack-Cycle 대비 90~100%에 이르기까지 유사 위험도 발생

개인정보의 공격적 흐름에 따른 유사 위험도 비율에 대한 객관적 현황은 그림 2와 같이 5가지 공격과 위협에 따른 객관적 분포도를 갖는다.

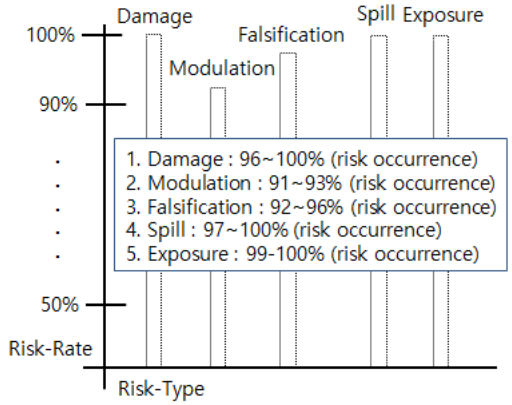

그림 2. 공격 흐름에 따른 유사 위험도 비율 분포도
Fig. 2 Distribution of similar risk ratio by attack flow

훼손으로부터 노출에 이르는 5가지 위험에 대한 사고결과에 대한 최소한의 위험도 지표는 10건과 100건 또는 그 이상의 건수와는 무관하게 위험도에 대한 2차적 위험도 발생을 유발하는 부분에 대해서는 위험에 따른 문제점 결과가 다를 바가 없음을 의미한다.

또한 정보보안과 개인정보보호의 상호 대비 물리적, 관리적, 논리적인 정책과 운영에 대한 비교지침들과 적용 법률에 대한 차이는 표 2와 같이 확인이 가능하다.

물론 상호 다른 보안을 위한 지침과 법률이 적용되어지고 있으나, 결론적으로는 각각 정보자산으로 식별한 정보에 대한 안전성을 확보하는 것이 목적으로 한다[9].

이는 정보보안의 보호 대상과 관리 위험이 개인정보보호를 위한 보호 대상과 관리 위험에 대한 상호 차이점이 있으나, 결론적으로는 하나의 정책과 지침을 통한 안전성 확보를 위한 관리적 환경과 운영 및 유지가 가능함을 의미하기도 한다.

표 2. 정보 보안 및 개인 정보 보안 지침 및 법적 상태
Table 2. Information security and personal information security guidelines and legal status

division	Instructions, legal, etc
Information Security	1. ISMS (Information Security Management System) Certification Audit Status 2. Indicators and guidelines for checking the status of critical facilities according to national infrastructure 3. Other necessary information security requirements
Personal Information Security	1. Personal Information Protection Act 2. Enforcement Decree of the Personal Information Protection Act 3. Enforcement Rules of Personal Information Protection Act 4. Safety Standards 5. Guidance and enforcement

2.3 정보보안과 개인정보보안의 실현과 구현 및 정보자산의 차이

정보보안과 개인정보보호의 가장 큰 차이점은 표 3과 같이 2가지 구분이 가능한데, 첫 번째는 정보자산의 차이와 정보자산이 보유한 또는 인위적으로 선정되어진 위험도에 따른 등급의 차이가 가장 큰 대비적 차이점으로 확인 가능하다.

다만, 공통된 부분에 대한 지표로써 앞서 언급한 정보자산 또는 개인정보 자산과 위험도 등급을 적정한 분류 조건에 따른 일원화된 지표로 활용 가능한 소구분으로 제시되어 진다[10].

이처럼 정보보안과 개인정보보호에 대한 각각의 목적과 운영 그리고 관련 정책 및 지침, 법률에 대한 해석과 비교를 통해 현실적인 차이를 명확히 구분하고 비교에 따른 향후 운영과 관리, 유지를 위한 방향성 제시가 가능해 진다.

표 3. 정보 보안 및 개인 정보 보안 지침 및 법적 상태
Table 3. Information security and personal information security guidelines and legal status

division	Information assets and evaluation
Information Security	1. Information assets: information systems, information protection systems, information 2. Asset class: Classification within an enterprise or agency based on confidentiality, integrity and availability
Personal Information Security	1. Information assets: resident registration number, passport number, driver's license number, alien registration number (* added: personal information, etc.) 2. PROPERTY GROUP: The unique identification number of this measure is an artificial classification (X)

III. 보안정책의 종류와 정보자산의 구성에 따른 정책 적용범주의 차이 극대화 기반 보안성 증대 제안

3.1 보안정책의 공통요소 및 공통 적용가능 환경 제안

기관과 기업의 내부 정보보안 자산과 개인정보보호 자산을 분류하고 이를 등급별로 위험도와 중요도를 재조정함으로써 기준이 되는 자산의 척도를 객관적인 값으로 구성하고 이를 공통된 보안 지표 및 표준 지표에 적용하는 방식으로 보안정책의 이원화를 공통 정책의 범주로 포함시킨다.

즉, 정보보안이 현행에서 활용하고 있는 보안 위험도 평가를 통한 DoA(Degree of Assurance, 허용 가능 위험도) 설정을 기준으로 개인정보보호를 일원화하기 위한 범주의 연계 또는 범주의 관리 영역의 변화가 필요하다.

따라서 공통 지표 및 표준 정책의 지표가 많아질 수 있도록 지속적인 일원화는 최종 동일한 지표를 구성할 수 있지는 않지만 최적화를 통한 간결화와 안전성을 확대 가능한 지표를 표준화가 가능하도록 구성할 수 있다.

3.2 보안정책의 순차적 적용에 따른 정보보안과 개인정보보안의 적용 시점 기준 제시

표준정책의 적용 시점은 각 주요 핵심 정보보안 정책과 개인정보보호 정책의 중요도에 따라 시점을 상호 비례하게 적용한다.

서로 다른 점검 지표를 운영하고 있었으나, 이를 하나의 정보자산과 같은 분류로 일원화하고 통일 또는 공통 점검지표로 1차적 분리와 각각의 정보보안과 개인정보보호를 위한 세부 분류로 지표를 분리하는 등의 과정이 사전에 수반되어지고 이를 통한 위험 또는 위협에 대한 적절한 안전성을 확보 가능한 점검척도로써의 지표 운영 여부를 재분석하는 과정이 필요하다.

따라서 각각의 기존 점검지표를 재분석하고 이를 통합하는 과정에서 유사 또는 연계 지표들을 재분류하고 새로운 안전성 확보 지표를 생성하는 들의 정책적 과정도 필요하다.

IV. 정보보안 정책 표준절차에 대한 검증과 구현에 따른 안전성 확보

4.1 보안정책 실현과 구현

보안을 위한 보안 정책의 이중화와 이원화는 보안성을 확보하기 보다는 중복된 보안 정책으로 인해 오히려 위험도가 가중되는 현상을 초래한다.

따라서 가장 기준이 되고 기본이 되는 안전성확보 조치 기준을 만드는 정책의 중요성과 일원화 지표를 구성하는 보안시행 정책 기관과 기업의 반영 결과를 표 4와 같은 공통 관리 기준을 재확인한다.

표 4. 정보보안과 개인정보보호 라이프 사이클 간의 공통 관리 기준
Table 4. Common management standards between information security and privacy protection life-cycle

division	Content
Collection	Collection of information or unique identification numbers that you want to use first
Storage	Means to store the results of processing or supplementing or modifying collected information or unique identification numbers
Management	uses (Search, communication)

4.2 표준 보안정책 적용에 따른 최적화 안전성 기준 확보

주요 핵심 보안정책 적용을 위한 최적화 안전성 기준의 제시가 본 논문의 핵심사항으로 정보보안과 개인정보보호의 기업 또는 기관의 내부 중요성에 따른 등급 반영도를 반영한 지표를 기준으로 제시한다.

표준지표의 경우 정보보안 5단계 라이프 사이클 대비 개인정보보호 라이프 사이클 3단계 공통 Cycle 공통기준으로 그림 3과 같이 활용한다.

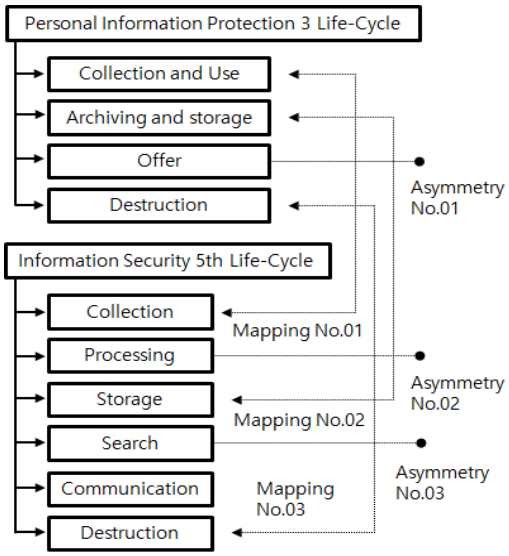

그림 3. 정보보안 5단계 흐름과 개인정보보호 3단계 흐름 비교현황

Fig 3. Information security 5th phase flow and personal information protection 3 phase flow comparison

4.3 정보보안과 개인정보보안의 융합 정책 제시에 따른 표준 정보정책 확인

제안된 정보보안과 개인정보보호의 공통 지표로써 수집, 저장, 관리 3가지를 정책에 반영하고 일원화된 표준화 적용 프로세스를 구현함으로써 최종 결과인 안전성과 위험과 위협으로부터의 물리적, 관리적, 정책적 척도에 따른 객관적 수치를 도출하고 이를 활용 가능한 지표 점검 표준 정책임을 그림 4와 같이 확인한다.

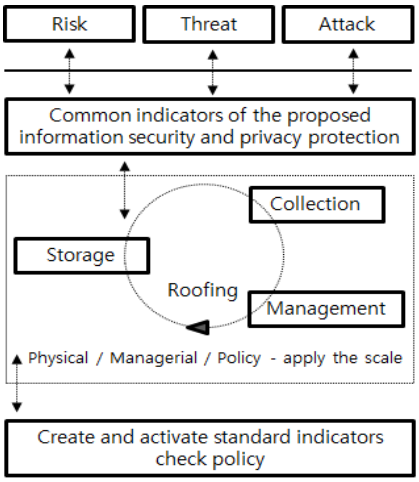

그림 4. 융합정책 연계 흐름과 3가지 정책적 단계

Fig. 4 Convergence policy linkage and three policy steps

V. 결 론

본 논문에서는 정보보안의 대상인 정보자산에 대한 등급과 기준을 개인정보보호와의 상이한 이질적인 정책을 제외하고 공통된 정책을 세우고 이를 활용함으로써 정책기반의 효율성을 극대화하기 위한 연구를 진행하고 정책간의 변화와 차이점 그리고 공통정책 기준 생성에 대해서 확인하는 과정을 확인했다.

물론 결론적으로는 정보보안의 대상이 되는 정보자산의 범주가 개인정보라는 단일 정보자산 대비 많은 분야에 걸쳐서 그 효과와 대상이 존재하는 부분은 확실하지만 그렇다고 개인정보를 정보보안의 정보자산의 하나로 인지하고 관리하는 부분은 엄청나게 많은 주요 개인정보에 대한 손실과 대내외적인 개인과 사회에 미치는 중요 파급적인 문제점의 충격이 크다는 사실을 확실히 확인 가능했다. 따라서 공통자산으로 분류하기 위한 부분이 아닌 별개의 정보자상으로 분류하되 보안을 위한 지침을 하나의 공통 지침으로 일원화하는 과정을 제안했다. 이후 향후 논문 주제에 대한 연구방향은 지속적으로 변경되는 정보보안 지침과 정책 및 법률, 개인정보보호법의 개정 등을 지속적으로 반영하고 공통된 정책을 찾아 일원화하고 유지함으로써 정책의 일원화가 이원화된 관리의 문제점을 최소화할 수 있음을 연구의 결과로 도출해내야 한다.

References

[1] C. Choi, Y. Lee, and T. Lee, "Improvement Method of ELIS Local Laws and Regulations Format for Personal Information Protection," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 11, 2016, pp. 1017-1024.

[2] S. Park and N. Kim, "A Verification Case Study about the Authentication of a Network using AAA," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 12, no. 2, 2017, pp. 295-300.

[3] J. Jeong and M. Choi, "A Study on Awareness of Information Security Influencing Trustness," *J. of the Korean Institute of Information Security and Cryptology*, vol. 25, no. 5, 2015, pp. 1225-1233.

[4] M. Yim, "Why Security Awareness Education is not Effective?," *J. of Digital Convergence*, vol. 12, no. 2, 2014, pp. 27-37.

[5] J. Jang, C. Choi, and D. Kim, "Design of Smart Tourism in Big Data," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 12, no. 4, 2017, pp. 637-644.

[6] J. Kim, "A Mobile-Sink based Energy-efficient Clustering Scheme in Mobile Wireless Sensor Networks," *J. of Korea Academia-Industrial Cooperation Society*, vol. 18, no. 5, 2017, pp. 1-9.

[7] B. Cha, J. Kim, and S. Park, "Prototype Design of Hornet Cloud using Virtual Honeypot Technique," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 10, no. 8, 2015, pp. 891-900.

[8] J. Bae and O. Park, "A case analysis on the effects of HRM on innovative performance," *J. of Korea Academy of Organization and Management*, vol. 30, no. 1, 2006, pp. 177-209.

[9] J. Kim, S. Kim, and S. Ryu, "The Impact of HR Involvement on HR Effectiveness," *J. of Korea Academy of Management*, vol. 12, no. 3, 2004, pp. 127-161.

[10] J. Jang, D. Kim, and C. Choi, "Study on Hybrid Type Cloud System," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 6, 2016, pp. 611-618.

저자 소개

서우석(Woo-Seok Seo)

2006년 숭실대학교 정보과학대학원 정보통신융합학과 (공학석사)
2013년 숭실대학교 일반대학원 컴퓨터학과 (공학박사)
2006년 ~ 2012년 서울특별시용산구시설관리공단 전산총괄
2012년 ~ 2017년 주식회사 이지서티 보안사업본부 본부장(이사), 개인정보보호센터 센터장(이사)
2017년 ~ 현재 시큐리티 컨설팅(Freelancer)
※ 관심분야 : 4차 산업, ICT, IOT, 정보경영, 정보보안, 개인정보, 비식별화, 정보화 전략기획(ISP), 정보화 관리체계, 실태점검, 빅데이터, 인공지능(AI), PIMS, ISMS 인증