Regular paper

Journal of the KIECS. pp. 111-118, vol. 14, no. 1, Feb. 28. 2019, t. 93, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2019.14.1.111

정보자산 보호를 위한 표준 보안정책 모듈화 기법 적용과 기밀성 및 무결성 확보를 위한 연구

서우석*

A Study on the Application of Modularization Technique to Standard Security Policy to Protect Information Assets and the Securement of Confidentiality and Integrity

Woo-Seok Seo*

요 약

다수의 정보보안을 위한 자산을 보유한 기업으로부터 보유 정보에 대한 운영과 관리차원의 현장 진단과 실태 점검 지표 및 각종 보안성 확보 기준들을 구성하고 이를 기반으로 정보자산의 분류를 시작하게 되었고 정보자산의 운영 및 관리 정책과, 서비스, 보유 디바이스의 물리적 자산관리, 응용소프트웨어 및 플랫폼에 대한 논리적 자산관리에 이르기까지 많은 영역으로 확대되고 있다. 이러한 정보자산 중 일부는 사물인터넷과 같은 새로운 분야의 신기술로써 이미 현실에서 운영되고 있다. 물론 일반 가정에서도 스마트홈과 같은 다양한 전자기기들을 사용하고 이러한 기기들이 과거와는 다르게 정보를 축적하고 가공하는 등의 일련의 정보 라이프 사이클이 존재하게 되었다. 뿐만 아니라 유통까지도 실현되는 지금 무엇보다도 해당 정보자산과 자산이 보유한 정보의 안정성을 확보해야 하는 과제가 도출되었다. 따라서 본 논문에서는 기업으로부터 가정에 이르기까지 보유한 정보자산에 대한 표준 보안정책 모듈화 기법을 제안하고 이를 적용함으로써 기밀성과 무결성 증대를 확보하는 연구를 하고자 한다.

ABSTRACT

For the security of a vast amount of information, it has been started to diagnose the site as a way of operating and managing the information owned by a company holding assets, to establish indexes to check the actual status and all kinds of standards to obtain security, and also to classify the information assets based on that. This has been extended to many different areas including policies to operate and manage information assets, services, the management of owned devices as physical assets, and also the management of logical assets for application software and platforms. Some of these information assets are already being operated in reality as new technology in new areas, for example, Internet of Things. Of course, a variety of electronic devices like Smart Home are being used in ordinary families, and unlike in the past, these devices generate a series of information life cycles such as accumulating and processing information. Moreover, as even distribution is now being realized, we are facing a task to secure the stability of information assets and also information that assets are holding. The purpose of this study is to suggest and apply standard security policy by moduling methods for information assets owned by companies and even families and obtain the enhancement of confidentiality as well as integrity.

키워드

Confidentiality, Information Assets, Integrity, Modularization Techniques, Security Policy
기밀성, 정보 자산, 무결성, 모듈화 기법, 보안 정책

* 교신저자 : Security Consulting(Freelancer)
• 접 수 일 : 2018. 10. 05
• 수정완료일 : 2018. 12. 10
• 게재확정일 : 2019. 02. 15
• Received : Oct. 05, 2018, Revised : Dec. 10, 2018, Accepted : Feb. 15, 2019
• Corresponding Author : Woo-Seok Seo
Dept. Security Consulting, Gyeonggi-do R&D laboratory
Email : ssws2000@nate.com

Ⅰ. 서 론

대규모 전산 및 통신분야 기반시설과 서비스 인프라를 보유한 기업들이 운영하는 정보자산 형태의 디바이스가 내장 보유되어 제공되는 서비스의 특정한 또는 중요한 정보로써 분류되어져 제공하고 있는 콘텐츠들을 새로운 신기술의 형태로 첫 번째 사물인터넷과 같은 기술을 기반으로 주요 정보자산을 기존 기업 내에서 전사적 자원관리를 이용한 관리 및 서비스 제공을 위한 운영기반 등과 같은 다양한 형태로 구성하기도 한다. 또한 일반적인 가정에서 정보자산으로 활용하고 있는 컴퓨터, TV, 자동차, 세탁기, 시계, 유무선 셋톱박스, 냉장고 등을 활용해서 사물인터넷 서비스 또는 단순 원격관리 등을 운영 제공하기도 한다. 따라서 본 논문에서는 큰 범주로는 기업과 가정에 존재하고 관리되는 정보자산에 대한 보안정책과 운영 서비스 내에 존재하는 정보를 대상으로 하는 보안을 기준으로 한다. 또한 이에 대한 보안과 단순 물리적 디바이스 및 논리적 서비스 품랫폼에 대한 보안성을 확보하기 위한 보안 3대 요소의 하나인 정보의 접근에 대한 합법적인 권한의 사용자에게 공개되는 기밀성과 정보의 신뢰도에 대한 척도를 확인하다. 이로써 무결성에 대한 확보 및 확대를 위한 표준 보안정책 모듈화 기법을 최종 제안하고자 한다[1-3].

이러한 모듈화 기법에 대한 제안을 위해 본 논문의 1장에서는 연구하고자 하는 분야에 대한 목적을 언급하고 2장에서는 정보자산을 활용한 신기술과 보안시장 현황, 정보보안의 기술 진화에 대한 관련 현황 등을 파악하고 3장에서는 접근 대상별 보안정책 모듈화 종류와 네트워크 기반의 정보자산 접근에 따른 기밀성 증대 방안을 제시하고자 한다. 마지막으로 4장에서는 네트워크 기반의 공개 정보자산과 접근 권한에 따른 보안성 검증을 시행하고 연구방향을 제시하고자 한다.

Ⅱ. 관련연구

본 관련연구 과정에서 제안하는 연구목적에 대한 다수의 기업과 가정을 대상으로 하는 정보자산의 구분 및 분류와 탑재되어진 정보의 중요성을 감안한 이해성을 높여 사례와 같은 부분을 언급하고 다양한 접근 취약점 등과 같은 보안정책에 대한 문제점인 취약점에 대한 현황들을 연구함으로써 최종 결론에 대한 기초자료를 확보하고자 한다.

2.1 네트워크 기반의 연계 신기술과 보안시장

네트워크 통신 분야는 크게 일반 통신 인프라를 이용한 기술 분야와 컴퓨터 네트워크로 구분 가능하며, 이 중 본 논문에서 언급하고 연구하고자 하는 분야는 컴퓨터 네트워크를 활용하는 부분에 중점을 두고 이를 기반으로 서비스와 플랫폼을 운영하는 정보자산에 대한 시장과 현 상황을 확인하고 연구에 반영하고자 한다[4-5]. 따라서 정보보안의 범주가 현재 많은 발전과 확대가 이루어졌으나 사물인터넷과 같은 신기술로 연구 분야를 집약하여 정보보안에 대한 현황을 제시하고자 한다. 다양한 정보보안을 목적으로 하는 정보자산의 경우 보안에 대한 기준점을 기밀성과 무결성으로 확정하고 2가지 보안기준을 준수하거나 척도를 활용하는 형태로 시장에서 운영되고 구축되어진 상황과 취약점들을 확인한다[6].

*** 정보자산 활용 기반의 사물인터넷에 대한 구성**

1) 유선기기 : PC, 전화기, 팩스, CCTV, 인터폰, 변압기 등,
2) 무선기기 : 스마트폰, 자동차, 냉장고, 세탁기, 시계 등

*** 정보자산 침해 가능 취약점 현황**

1) 정보보안 안정성 확보 지침과 정책의 관리적 취약점,
2) 정보자산 디바이스 자체 물리적 취약점,
3) 유 • 무선 네트워크 구성의 논리적, 물리적 취약점,
4) 정보자산 운영을 위한 서비스 플랫폼 및 어플리케이션 논리적 취약점

2.2 정보보안의 진화와 변화

각종 정보자산이 제공하는 서비스를 기준으로 이에 대한 침해와 취약점 공격에 대한 방어기능으로 다양한 정보보안을 위한 물리적이고 논리적인 방어기술들이 제시되고 구현되어 졌다[7-8]. 하지만 정보보안의 핵심적인 인프라와 탑재 정보에 대한 보안에 있어서 문제점으로 인한 사고사례가 지속적으로 발생하고 있으며, 이에 대한 방어기술 또한 집중적으로 진화하고 있는 상황이다[9], 따라서 표 1과 같은 정보보안의 기초적인 기준점과 해당 구성요소들을 반영한 방어사례 및 형태

를 확인한다.

표 1. 정보보안을 위한 보안 구성요소와 정의 및 쓰임
Table 1. Definition and use of security components for information security

Division	Definition	Uses and Cases
Confidentiality	It means the infringement protection function such as the rule such as the setting of specific constraints on information generated in real time according to the main information on the information asset or the running of the service platform or restriction of access	- Access rights management - Information encryption - Information asset physical control
Integrity	Means the function of protecting the infringement such as the reliability of the information held by the original information asset and the alteration and utilization of the information of the users of the authenticated service	- Hash function - Authentication - Source infringement measure
Availability	Means a defensive function that enables the services provided by information assets to be used normally	- Service utilization - Platform driven

2.3 다양한 네트워크 접근과 권한에 대한 보안정책 실현과 구현

네트워크 기반 인프라를 구성하는 공중망으로부터 유선 또는 무선으로 연결되어 정보자산의 서비스를 제공하도록 하는 다양한 네트워크 접근 경로와 같은 형태에 대한 서비스를 사용하고자 하는 사용자의 접근권한과 관리에 대한 보안정책 설정과 서비스를 제공하기 위한 플랫폼 설정 및 관리권한을 보유한 책임자에 대한 보안정책은 각기 이원화되어 설정하고 적용되어진다[10]. 따라서 표 2와 같이 접근하는 접근자에 따른 접근권한 분리와 정보자산에 제한 접근 이후 활용 가능한 기능과 수행업무에 대한 제한을 관리하는 인증범위 구성을 확인한다.

표 2. 접근권한과 권한별 인증범위 구성현황
Table 2. Status of access authority and authentication scope by authority

Division	Access rights	Authentication
User	read, limited modify, limited execution	password (* Allows password authentication with encrypted password for simple read and execute)
Admin	read, write, execution, modify, delete, verify	Certificate, Smart Card (* Take advantage of multi-dimensional authentication levels such as individual certificates or smart cards with all administrator privileges)

III. 접근 대상별 보안정책 모듈화 종류와 네트워크 기반의 정보자산 접근에 따른 기밀성 증대 제안

다양하고 많은 정보자산이 보유한 정보들의 안정성을 확대하고 기밀성과 무결성 확보를 위한 제안하는 보안정책 모듈화에 대한 외부 또는 네트워크 기반의

접근 대상별 보안정책 모듈화에 대한 종류를 파악하고 이를 기반으로 정보자산 접근에 대한 최종 기밀성 증대 방안을 모색하고자 한다.

3.1 접근 대상별 정보자산의 보유와 구성환경

정보자산에 접근하는 다양한 접근권한을 가진 관리자와 이용자들의 정보자산에 대한 조건별 검증 또는 읽기, 쓰기, 실행 등과 같은 직접적인 정보에 대한 생성으로부터 파기까지의 일련의 라이프사이클에 대한 흐름과 구성환경을 그림 1과 같이 구성한다. 이는 정보자산을 4가지 주요 핵심 기능과 형태를 본 논문에서는 1차적인 연구과정으로 제시하고 있다. 1단계는 정책 설정, 2단계는 정보자산 디바이스의 물리적 정보 탑재 가능 정보 설정, 3단계는 정보자산에 접근하는 유선과 무선 네트워크 보안환경에 대한 설정, 마지막으로는 정보자산이 관리자 또는 사용자들에게 제공하는 서비스 인프라와 최고 관리자의 환경설정을 위한 플랫폼 접근과 감사를 내포하고 있는 전체 권한을 설정하는 단계로 구성된다. 이로써 보안정책의 모듈화를 위한 첫 번째 조건인 기밀성 확보를 위한 모듈조건을 구성한다.

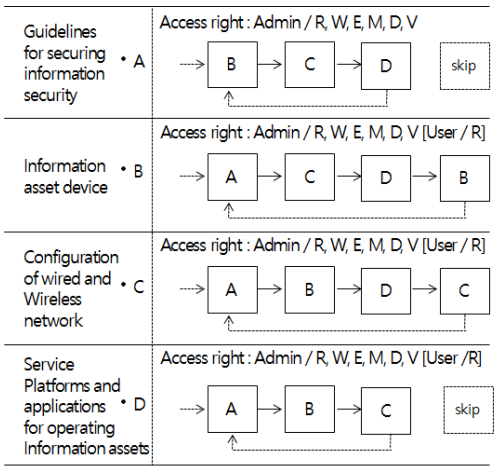

그림 1. 정보자산 구분과 탑재 정보현황 및 접근권한과 권한별 인증구성

Fig. 1 Information asset classification and loading information status and access authority and authentication configuration by authority

물론 무결성을 위한 부분으로는 기밀성의 권한도 일부 포함하는 기능인 직접적인 접근자들에 대한 권한 관리를 구성한다. 해당 구성으로는 읽기, 쓰기, 제한적 쓰기, 수정, 제한적 수정, 실행, 제한적 실행, 삭제, 검증으로 기밀성 준수를 위한 구성조건인 4가지 정보자산의 설정과 연계한다.

3.2 보안정책 모듈 적용에 따른 정보자산과 모듈과의 권한 연계기준

정보자산의 구성 예로써 그림 2와 같이 스마트 시계를 선정하고 정보자산에 대한 보안정책 선정 연계 모듈을 구성하는 표준방식으로 최초 정보자산 운영과 관리를 위한 보안정책을 논리적으로 구성하고 실제 기기인 디바이스에 해당 정책을 탑재 후 운영하는 과정에서 네트워크 연결을 위한 환경설정과 사용자가 지속적으로 서비스 받고자 하는 플랫폼 기반의 정보가 최종 지원되는 서비스 제공 순으로 진행된다.

따라서 최종 정책 적용, 정보자산 디바이스에 정책 탑재, 보안정책 기반의 네트워크 연계 환경 설정, 최종 정보자산의 고유 서비스 제공과 같이 간략하게 표현 가능하다.

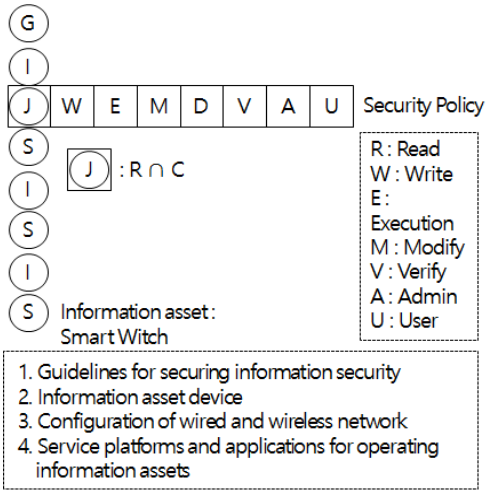

그림 2. 정보자산 접근 보안정책 모듈과 연계 구성

Fig. 2 Information asset access security policy module and linkage configuration

최종 연계되는 정보자산에 대한 접근 보안정책 모듈에 대한 표준화를 위한 연계구성은 정보자산의 기능 구성과 다양한 접근권한에 따른 수행 가능 조건의 일원화 조건을 기준으로 도출한다.

Ⅳ. 네트워크 기반의 공개 정보자산과 접근권한에 따른 보안성 검증

제안하는 정보자산에 대한 표준 보안정책 모듈화 기법 적용에 따른 기밀성과 무결성 증대 방안에 대한 기초자료가 될 수 있는 모듈들의 설계와 설계에 따른 권한분리와 같은 보안성을 검증하고자 한다.

4.1 보안정책 모듈 설계와 구현

정해진 결과를 도출하기 위한 기준척도를 나타내는 것이 아니라 정보자산과 보안정책의 x, y축 지표를 구성하고 이를 상호 교차하는 형태로 정보자산 별 최적의 보안정책을 찾는 과정을 시행하고 최종 결과로 제안하는 보안정책의 모듈인 정보자산 ∩ 보안정책에 따른 최종 형태를 도출하는데 있다. 다만, 두 가지 교차척도를 구하는 방법에 대해서는 정보자산 별 보안정책과의 관련성을 갖는 부분을 각각의 범주로 사전에 표준 보안정책 구성 기초 테이블을 구성하고 이를 시행해야 한다. 이러한 제안하는 연구 결과를 도출하기 위한 가장 기본적인 보안정책 모듈의 설계는 그림 3과 같이 제안하고 있다. 따라서 각 보유한 정보자산의 종류와 권한조건의 조건에 따라서 해당 연계를 구성하고 각 중복 조건에 해당되는 최종 보안정책 조건을 중복되어 일원화된 조건공간에 적용한다.

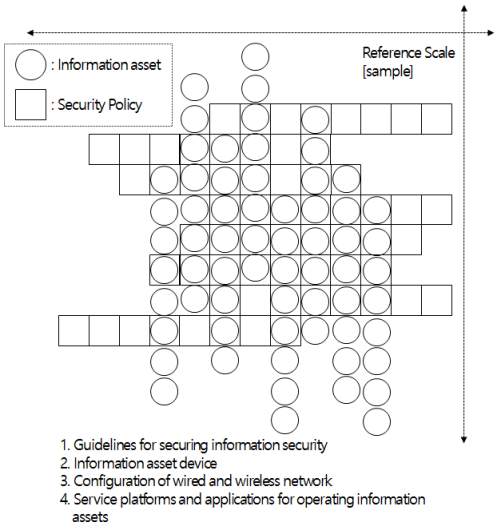

그림 3. 보안정책 모듈 설계 기준
Fig. 3 Security policy module design criteria

제안된 설계 기준에 따른 형태에 대한 중복 조건형태는 그림 4와 같이 축출하고 각 정보자산과 접근권한을 교차 적용함으로써 보안정책을 모듈화 할 수 있다. 물론 해당 최종 중복된 일원화 조건을 최적화하기 위해서는 다수의 정보자산에 대한 지속적인 기본 설계 기준에 적용함으로써 결과를 누적하고 분석해야 한다.

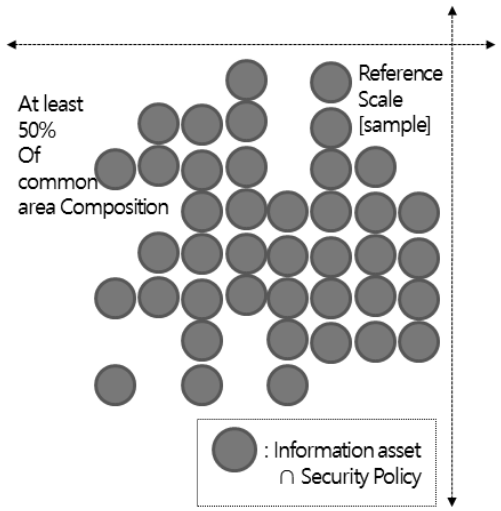

그림 4. 제안된 설계 기준 적용형태에 대한 중복조건 구성
Fig. 4 Construction of redundant conditions for the proposed design criteria application form

4.2 최적화 표준 정보자산 분류와 보안정책 모듈과의 매핑을 통한 보안 기준지표 구성

기업과 가정 또는 그 외의 다양한 환경에서 활용하고 보유하고 있는 정보자산에 대한 최적화 표준 정보자산 분류와 보안정책 모듈에 대한 기준지표는 정보자산에 대한 접근권한의 중복된 일원화 조건을 제시하고 이를 활용한 다수의 중복조건 설정에 따른 결과값을 누적함으로써 최적화된 정보자산을 확인한다.

*** 최적화 표준 정보자산의 환경적 분류**

1) 정책 설정,
2) 정보자산 디바이스 설정,
3) 유무선 네트워크 보안환경 설정,
4. 서비스 인프라 및 플랫폼 접근권한 설정

정보자산을 물리적인 형태의 스마트 시계처럼 단위적으로 지칭하는 것이 아니라 최적화 표준 정보자산 설정을 위한 4단계 설정을 각 정보자산에 일괄적인 조건으로 구성한다. 따라서 최적화 표준 정보자산 분류 기준에 따른 실제 물리적인 디바이스를 역으로 도출하는 방법이다. 이는 기밀성 기반의 보안조건을 제시하는 부분이며, 최종 설계된 기준에 따라 조건식이 중복되고 즉 교차되어 적용되고 일원화됨으로써 가능하다.

4.3 정보자산의 운영과 보안에 대한 안전성 검증 기준안 도출

도출되어진 최적화 표준 정보자산을 기반으로 기업과 가정에서 원하는 정보자산의 서비스를 활용하고 운영하는 단계의 접근권한을 2차적인 조건으로 제시한다. 이는 설계 기준 상에 이미 제시한 중복 및 교차 조건을 도출하기 위한 방안이다. 따라서 최종 제안된 정보자산에 대한 보안정책 모듈화를 기반으로 하는 기밀성과 무결성 확보를 위한 방안은 기본적으로 제시되었다. 다만 정보자산의 물리적인 형태가 하나 이상의 경우에는 다차원의 모듈을 구성하기 위해 그림 5와 같이 최종 제안하는 중복 및 교차 보안 조건과 다차원 정보자산 디바이스의 구성을 타나낸다.

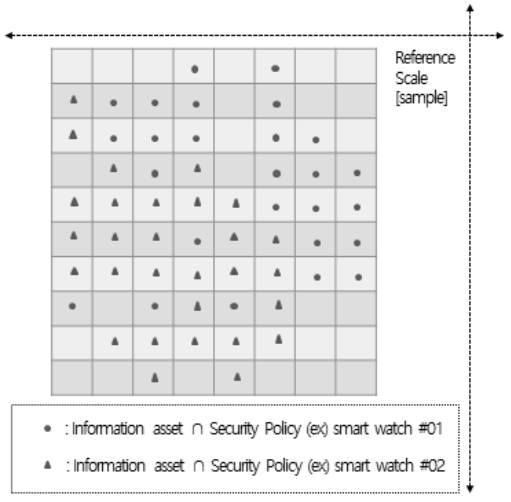

그림 5. 안전성 확보를 기반으로 하는 최종 제안되는 보안정책 검증 기준

Fig. 5 The final proposed security policy verification standard based on security assurance

즉, 기업과 가정에서 보유한 정보자산이 각각 다른 구성으로 보유하고 있으며, 해당 정보자산이 제공하는 서비스의 종류 또한 다른 환경에서 구성되므로 최종 제안된 안전성 확보를 기반으로 하는 보안정책 검증 기준은 적용하는 환경마다 전부 다를 수 있으므로 본 논문에서는 정보자산에 대한 분류를 위한 4가지 기준 조건과 정보자산이 보유한 정보에 대한 서비스 접근 권한에 대한 다양성을 제시하는 다수의 조건을 제안하는데, 연구의 최종 목적을 두고 있다.

V. 결 론

본 논문에서는 대규모 산업기반의 기업으로부터 가장 작은 네트워크 구성 단위인 가정에 이르기까지 정보자산의 분류와 실태를 점검한 결과를 바탕으로 다양한 정보를 보유한 자산들에 대한 보안성을 확보하는 부분에 기밀성과 무결성 확대 방안을 제안하고 이를 연구하는 과정을 진행했다.

물론 기업으로부터 가정에 이르기까지의 모든 정보자산을 분류하고 각 정보자산별 보유한 정보를 구분하고 이를 다시 체계적으로 모듈화 하는 과정이 이루어져야 하나, 본 논문에서는 전체 정보자산을 대상으로 어떠한 환경에서는 정보를 보호하기 위한 표준 보안정책 모듈를 구성하는 기초를 세우고 이를 제안하는 과정을 연구의 방향으로 설정 및 구성하였다.

이후 연구결과에 따른 보안정책 모듈에 대한 방법을 연구과정을 위해 제시한 기업이나 가정의 정보자산이 아닌 새로운 조직과 새로운 정보자상에 적용하고 기밀성과 무결성이 보존되고 안전성까지 감안 가능한지를 확인하는 추가적인 연구과정이 필요하다.

따라서 향후 논문의 주제에 대한 연구방향은 정보보안 3요소 중 기밀성과 무결성을 제시한 금번 연구에 대한 결과와 제시방안에 대해서 추가적으로 정보자산이 보유한 정보에 대한 서비스 제공을 기반으로 하는 서비스 부분에서의 가용성까지 확보하는 연구가 이어져야 한다.

References

[1] Y. Lee, "A Design and Analysis of Multiple Intrusion Detection Model," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 11, no. 6, 2016, pp. 619-626.

[2] K. Kim, D. Wang, and S. Han, "Home Security System Based on IoT," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 12, no. 1, 2017, pp. 147-154.

[3] K. Kim, Y. Park, S. Ro, and B. Kim, "Design of Infringement Accidents Preventing System Using DNS Information Retrieval Integration Method," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 16 no. 9, 2012, pp. 1955-1962.

[4] C. Choi, Y. Lee, and Tae. 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.

[5] S. Paik, S. Kim, and H. Park, "Design and Implementation of Network Access Control for Security of Company Network," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 47, no. 12, 2010, pp. 90-96.

[6] J. Yun, "A Study on the Short Term Curriculum for Strengthening Information Security Capability in Public Sector," *Journal of the Korean Institute of Information Security and Cryptology*, vol. 226 no. 3, 2016, pp. 769-776.

[7] 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.

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

[9] 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.

[10] 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.

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