ISSN 2234-4438
중소기업융합학회 논문지 제6권 제2호 pp. 11-17, 2016 DOI : http://dx.doi.org/10.22156/CS4SMB.2016.6.2.011

기업 정보화 역기능에 따른 피해를 최소화하기 위한 기업 정보 처리 모델 설계

정윤수*
목원대학교 정보통신공학과

Design of Prevention Model according to a Dysfunctional of Corporate Information

Yoon-Su Jeong*
Department of Information Communication Engineering, Mokwon University

요 약 최근 IT 기술이 발달함에 따라 기업에서 생성되는 다양한 종류의 데이터(또는 정보)가 외부의 기관이나 개인에게 유출되는 상황이 잦아지고 있다. 그러나 기업 차원에서 기업 정보의 역기능을 줄이기 위한 대응방안이 미흡한 상황이다. 본 논문에서는 기업 정보화의 역기능을 최소화하기 위한 역할기반의 기업 정보 처리 모델을 제안한다. 제안 모델은 기업 정보를 관리 및 감독하기 위한 관련 부서를 통해 기업 정보를 보호하고, 신속하고 체계적인 복구 및 운영 전략을 수립할 수 있도록 하여 기업 정보화 서비스의 효율성을 향상시켰다. 제안 모델은 정보에 접근하는 사용자의 권한과 역할을 관리자가 중앙 관리하여 정보에 접근하는 사용자가 이상 징후가 포착되면 정보 접근을 차단한 후 신속하고 체계적인 복구 및 운영 연속성 전략을 수립하고 있다. 실험 결과, 제안 모델은 기존 모델에 비해 바이러스 피해가 48.8% 낮았다. 또한, 기업내 발생되는 정보 역기능에 대한 유통 건수는 기존 모델에 비해 17.9% 낮은 결과를 얻었다.

키워드 : 기업, 정보화, 역기능, 유통 피해

Abstract Recently, As the IT skills development, the different kinds of data (or information) generated by the company are becoming more frequent leaked to outside organizations and individuals. However, it is insufficient situation to reduce the dysfunctional corporate information at the enterprise level. In this paper, we propose a role-based enterprise information processing model to minimize the dysfunctions of corporate information. The proposed model is to allow you to set protect corporate information through the relevant departments for the management and supervision of enterprise information, and rapid and systematic recovery and operating strategy was to improve the efficiency of enterprise information services. The proposed model is caught blocking access to information access to information to establish a rapid and systematic recovery and operational continuity strategy after the administrator user permissions and roles that access to information is centrally managed by the user when the abnormality. In experimental results, virus damage was lower 48.8% than the previous model. In addition, information on the number of dysfunction distribution occurring within the company gained 17.9% lower results than the previous model.

Key Words : corporate, IT, Dysfunction, Damage Distribution

Received 2016-06-03 Revised 2016-06-13 Accepted 2016-06-16 Published 2016-06-30
*Corresponding author : Yoon-Su Jeong (bukmunro@mokwon.ac.kr)

1. 서론

최근 중소기업을 중심으로 정보화가 기업 운영과 관련된 가장 큰 보안 이슈 중 하나이다. 이 같은 현상은 기업 정보화가 기업을 중심으로 정보화 역기능(Negative Effect of Informatization)이 확산되고 있기 때문이다[1-6]. 여기서, 정보화 역기능이란 기업에서 사용되는 다양한 전자기기를 통하여 생성되고 활용되는 정보화 활용에 따른 부작용을 의미한다.

정보화 역기능을 통해 사용되는 정보는 기업 내·외의 다양한 경로를 통해 유출되거나 활용되어 기업 경쟁력을 약화시킬 수 있다. 기업 정보화 역기능의 대표적인 예는 불법 정보 유통, 지적 재산권 침해, 소득 계층 간 정보격차 확대 등이 있다[7-11].

기업에서 정보화 역기능을 예방하기 위해서는 기업 내 정보를 다루는 주체들이 독립적으로 정보를 다루지 못하도록 해야 한다. 특히, 기업의 정보화 서비스를 효율적으로 관리하기 위해서는 기업 활동에서 발생되는 정보를 전문적으로 처리할 수 있는 정보화 관련 부서가 필요하다[12,13]. 국내 많은 기업 CEO들은 기업 내 정보화 관련 부서의 필요성을 공감하고 있다. 일부 기업에서는 기업 정보화의 역기능을 막기 위해서 개인 전자기기에 설치된 프로그램이나 문서의 접근제어를 수행하고 있다. 그러나 기업 정보화는 기업이 보유하고 있는 기술이나 기업 간 연계된 전자적인 정보, 정부의 제도적 지원 및 각종 규제 등에 따라 기업 정보 서비스 구조가 서로 다르기 때문에 기업 정보화 역기능에 대한 취약점이 존재한다[3]. 기업은 기업 정보화 역기능을 최소화하기 위해서 기업 정보화 서비스를 처리하는 서버를 레벨에 따라 가상화, 자원공유 및 집중화, 정보위탁, 단말의 다양성 등으로 서비스하고 있다[14,15].

본 논문에서는 기업 정보화의 역기능을 최소화하기 위해서 기업에서 생성 및 발생되는 정보의 레벨에 따라 서비스 접근을 계층화 할 수 있는 기업 정보화 서비스 모델을 제안한다. 제안 모델은 기업 정보를 생성하는 주체를 기업이 보유하고 있는 기술이나 기업 간 연계된 전자적인 정보, 정부의 제도적 지원 및 각종 규제에 따라서 다양한 기업 정보 접근 보안 정책을 적용할 수 있도록 역할기반의 접근권한 관리를 수행한다. 또한, 기업 정보에 접근하는 주체를 관리 및 감독하기 위한 기업 정보화 관련 부서를 통해 기업 정보를 보호하고, 신속하고 체계적인 복구 및 운영 전략을 수립하고, 기업의 정보화 서비스의 효율성을 향상시킨다.

이 논문의 구성은 다음과 같다. 2장에서는 기업정보화 역기능에 대한 개념에 대해서 설명한다. 3장에서는 기업 정보화 역기능을 최소화하기 위한 기업 정보 서비스 모델을 제시하고, 4장에서는 제안 모델에 대한 평가를 분석한다. 마지막으로 5장에서는 이 논문의 결과를 요약하고 향후 연구에 대한 방향을 제시한다.

2. 관련연구

2.1 기업 정보화의 역기능

기업 정보화의 역기능은 기업에서 발생하고 있는 정보화의 여러 가지 특성에 따라 다양하게 나타나고 있다. 특히, 기업 정보화의 역기능은 기업 내 정보화 체계가 원활하게 운영되지 못하기 때문에 나타나는 경우가 대부분이다[1,4,8].

기업의 정보화 역기능 현상은 개인적 성향(해킹, 바이러스, 음란물 유통, 개인정보 유출 등)이 많았으나 최근에는 인터넷과 스마트폰이 발달함에 따라 그 유형과 방식이 다양해지고 있다[3,11,15].

2.2 기업 정보화에 영향을 미치는 요소

기업에서 사용되고 있는 기업 정보는 기업의 특성 및 환경을 고려하여 생성 및 관리되어야 한다. 기업 정보가 정상적으로 기업 활동에 사용되기 위해서 기업에서는 Table 1처럼 기업 정보화에 영향을 미치는 요소를 분류하고 있다[3].

Table 1. Factors affecting the Company informatization

Influencing element
Information introducer
System development approach
The type of operating system, application services, local (city or province)

기업 정보화 서비스가 안정적으로 이루어지기 위해서 기업에서는 Table 2처럼 기업 정보화의 평가 요소를 독립변수와 종속변수로 구분하여 평가 내용을 분류하고 있다[1].

Table 2. Factors of Company information

Evaluation factors	Contents
Independent variable	· ICT experience · S / W development methods · How the system operates · Number of application tasks · Computer processing method · Location of the MIS department within an organization
Dependent variable	· Participation of the CEO · Relationship between the computational department staff · Communication and computing departments step · The attitude of the staff and computing department · And technical capabilities of the computing department staff · Processing of change requests · Support Provider (Vendor) · Response time of the system · Ease of access · Accuracy of the printouts · Temporality, of prints · Accuracy of the output · Reliability of the printouts · The adequacy of the printout · Understanding of the system · Users participate in consciousness · Education system · Degree of system availability · Regular use much system

2.3 정보화 역기능 실태

2.3.1 해킹

해킹은 정보 생성 및 활용을 방해하고 정보유통을 원활하지 못하도록 막고 있다[5]. 기업에서 생성되는 중요 정보 중 해킹으로 인한 기업의 피해는 점점 증가하고 있는 추세이다. 기업을 해킹하는 해커는 기업의 주요 업무를 마비시키고 사회혼란을 초래하는 주요 원인 중 하나이다.

주요 기반시설을 해킹하는 사례를 보면 초기에는 단순 호기심에서 시작하였지만 점차 사이버절도 및 유료사이트 이용과 같은 사이버범죄로 이어지고 있다[2]. 또한 특히, DDOS(분산서비스거부공격)에 의한 해킹은 기업의 기밀 유출 및 전산망 마비 등을 야기할 수 있다.

2.3.2 컴퓨터 바이러스

컴퓨터 바이러스는 일반 PC 사용자들뿐만 아니라 기업에서도 가장 큰 보안위험 중 하나이다. 특히, 컴퓨터 바이러스는 기업의 중요 정보 및 기밀문서 등을 불법적으로 유출시키는 해킹 기술 등과 접목하여 데이터의 유실, 기업 기밀의 유출, 네트워크 시스템의 마비 등 기업에 상당한 피해를 발생시키고 있다[2,8].

2.3.3 기타 정보화 역기능

기타 기업의 정보화 역기능에는 기업 사이트 불법 도용, 불법 사이트 운영, 인터넷 사기, 스팸메일, 정보 조작 등 유·무선 인터넷과 관련된 다양한 정보화 역기능이 있다[3].

3. 기업 정보화 역기능을 최소화하기 위한 모델 설계

3.1 개요

기업 정보화의 역기능을 최소화할 수 있는 제안 모델은 기업의 중요 정보를 레벨에 따라 권한을 부여하여 기업 정보에 접근하는 것을 제어하여 기업에서 발생할 수 있는 기업 정보화 역기능의 보안 사고를 줄 일 수 있도록 하고 있다.

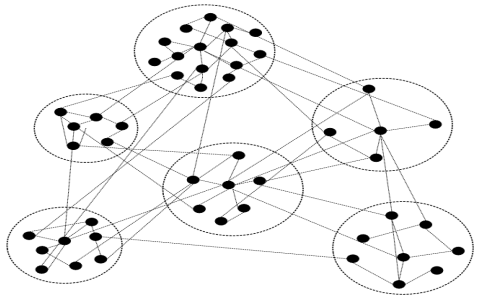

Fig. 1. Overall Information Process Structure of Proposed Model

제안 모델은 Fig. 1처럼 다양한 종류의 기업 정보를 속성(날짜, 시간, 목적 등)에 따라 기업 정보와 속성 정보를 해쉬체인으로 묶어 처리한다.

3.2 기업 정보화 보안 요구사항

제안 모델에서 요구되는 기업 정보화의 보안 요구사항은 Table 3과 같이 11개 항목으로 분류된다.

Table 3. Security Requirement of Company

Item	Contents
IT skills	The degree of IT resources and skills held by the organization to adapt to change and needs
Organizational agility	The extent to which the organization quickly adapt and respond to changes in market / environment / customer requirements
Paticipation of members	The degree of compliance with organizational security policies and membership information security behavior
Security risks experience	The degree of organization within the security-related problems experienced
Competition	The degree of competition within the industry and companies involved
Dependence on partners	Between partners / partner companies technical and strategic dependence degree
IT Strength	The degree of IT utilization and introduction of innovative technologies among enterprises within the industry
IT instability	Rapid development and change in the level of IT skills
Security risk management recognition	Aware of the importance and necessity of security risk management of the organization about
Security risk management development commitment	Decision-making and commitment level of security required for such gaepra designed to enhance an organization's security risk management
Security risk management paractices	Organization and execution of activities related to security risk management degree

Table 3과 같은 보안 요구사항은 기업에서 사용되고 있는 정보의 역기능을 최소화하기 위해 필요한 항목이다.

3.3 기업 정보화 정보 간 상관관계

제안 모델에서는 기업 정보의 역기능을 최소화하기 위해서 기업 정보에서 생성되는 정보 간 상대적 중요도를 쌍대비교 행렬을 바탕으로 식 (1)과 식 (2)처럼 행렬에 사용되는 모든 i, j, k에 대해서 기업 정보의 상대적 중요도를 나타내도록 한다.

$$a_{ij} = w_i / w_j \quad \text{i, j = 1,2,..., } n \qquad \text{식 (1)}$$

$$a_{ij}a_{jk} = (w_i/w_j)\cdot(w_j/w_k) = w_j/w_k = a_{ik} \qquad \text{식 (2)}$$

식 (1) ~ 식 (2)을 통해 기업 정보의 일관성에 사용되는 방정식의 근 $\lambda_i(i$=1, 2, ... ,$n)$은 기업 정보의 상대적 중요도의 합이 $\sum w_j$=1이 되도록 하여 기업 정보의 가중치(종류, 위험도, 개수 등)를 구한다.

3.4 기업 정보간 연계 처리

제안 모델은 기업 정보를 속성 정보와 함께 기업 정보간 상관관계가 높은 정보를 중심으로 서브넷을 구성할 수 있도록 계층화 한다. 기업 정보를 서브넷으로 구성하는 이유는 기업 정보의 상관관계에 따른 확률 값이 높은 기업 정보를 중심으로 기업 정보의 신뢰도를 계층화하기 위해서이다. 제안 모델은 데이터 간 연결 정보를 처리할 때 Table 4와 같은 알고리즘을 사용한다. 제안 모델은 Table 4와 같은 알고리즘을 통해 계층적으로 구성된 기업 정보의 상관관계에 대한 확률 값을 식 (3)과 같이 구한다. 식 (3)은 계층적으로 구성된 기업정보를 해쉬 체인하여 기업 정보의 연결 정보를 확률 P로 표현하기 위해서 사용된다.

$$P = \begin{cases} \dfrac{n}{L} - \dfrac{n((L-1)!)^2}{L^2(L-21)!(L-1)!} & (L \geq 21) \\ \dfrac{n_a}{L} & (1 \leq L \leq 21) \end{cases} \qquad \text{식 (4)}$$

여기서, L은 해쉬 체인의 길이를 의미하고 n은 계층적 기업정보의 수를 의미한다.

Table 4. Hierarchical Information Process Algorithm of Proposed Model

```
Hierarchical_Information(H, p)
input : Company information
output : Company information with correlated a high probability
1.    m = p.num_children_information
2.    k = m-1
3.    while k ≥ 0
4.        p.children[k].I = h(2^k × p.I)
5.        Hierarchical_Information(H, p.children[k])
6.        k=k-1
```

3.5 기업 정보화 서비스 구조

제안 모델의 기업 정보화 서비스 구조는 크게 정보보호 솔루션의 도입, 정보보호 전담 전문 인력 운용, 백업 시스템 및 재난복구 시스템 구축, 정보 역기능에 대한 의식 교육 등 4가지 내용이 포함되어야 한다.

3.5.1 정보보호 솔루션의 도입

기업 정보를 보호하기 위해서 기업이 구매한 솔루션들은 대부분 바이러스 및 해킹으로부터 기업의 정보 및 자산을 지켜내기 위한 경우가 대부분이다. 그러나 기업에서 구매한 솔루션을 사용하는 기업 구성원의 정보보호도 고려하여 정보시스템을 구축하여야만 바이러스 및 해킹으로부터 안전할 수 있다.

3.5.2 정보보호 전담 전문 인력 운용

기업 정보는 대부분은 정보를 생성하는 사용자가 책임을 지고 있는 경우가 대부분이다. 기업 정보의 안전을 보다 더 제 3자로부터 지켜내기 위해서는 정보 생성에서부터 소멸까지 기업 정보를 전문적으로 관리할 수 있는 전문 인력이 필요하다. 최근 기업에서는 기업 정보의 안전성을 보장받기 위해서 기업 정보를 전담하는 전문 인력을 채용 및 운영하고 있는 상황이다. 기업에서는 정보시스템과 관련된 문제가 발생할 경우 기업 피해를 최소화하면서 신속하게 기업 피해에 대응하기 위해서도 전담 인력의 운용은 필요 요구사항이 되고 있다.

3.5.3 백업 시스템 및 재난복구 시스템 구축

기업 정보는 자연재앙 및 기업 실수로 인해 발생되는 기업 피해를 최소화하기 위해서 백업 시스템 및 재난 복구 시스템 구축이 필요하다. 현재 많은 기업이 백업 시스템 및 재난복구 시스템이 구축되어 있지 않은 상태이다. 대기업을 중심으로 백업 시스템 및 재난복구 시스템이 구축되어 있지만 중소기업은 예산 부족으로 인하여 구축되어 있지 못한 게 현실이다.

3.5.4 정보역기능에 대한 의식 교육

기업의 정보 유출 및 손실을 예방하기 위해서는 기업을 구성하고 있는 구성원들에게 주기적인 기업 정보 역기능에 대한 의식 교육을 실시해야 한다. 기업 정보 유출의 대부분을 차지하는 사례가 개인의 부주의한 정보 이용 습관이다. 기업에서는 개인이 활용할 수 있는 정보보호 수칙을 만들어 기업 정보 역기능에 대한 피해를 최소화 하도록 노력해야 한다.

4. 평가

4.1 환경설정

이 절에서는 기업의 정보 역기능과 관련하여 경중사용자별 컴퓨터 바이러스 피해유형, 불건전 정보 접촉 경험, 경중 사용자별 음란물 유통 등에 대해서 평가한다[6].

Table 5. Experimental Environment

Environment Variable	Value
Number of User	100
Experiment Time	24 Hour
버퍼 크기	50 packet/s
Packet Drop Probability	0.01
Data Packet Size	100 bytes

4.2 실험결과

Fig. 2는 기업 내에서 컴퓨터 바이러스 피해 유형을 경중 사용자 별로 구분하여 시스템 전체 파괴, 시스템 점진적 마비, 시스템 일부 파괴, 별 지장 없음 등을 기존 모델과 제안 모델을 비교평가하고 있다.

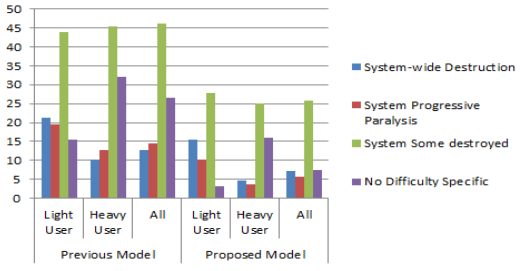

Fig. 2. Type of computer virus damage by Light/Heavy User

실험 결과, 제안 모델은 기존 모델에 비해 경중사용자별 컴퓨터 바이러스 피해가 시스템 전체 파괴, 시스템 점진적 마비, 시스템 일부 파괴, 별 지장 없음 등에 대한 피해가 48.8% 낮은 결과를 나타내고 있다. 이 같은 결과는 제안 모델이 기업 내 역정보화를 예방하기 위해서 기업 정보에 레벨에 따른 접근 권한 부여 및 확률 기반 유해 정보 차단 기능을 적용하였기 때문에 나타난 결과이다.

Table 6. Measures against illegal distribution of corporate information

	Previous Model			Proposed Model		
	Light User	Heavy User	All	Light User	Heavy User	All
Fundamentally blockade	21.3	10.1	12.8	23.8	14.6	18.3
User self-regulation	19.4	12.6	14.4	20.2	19.4	19.7
Information content rating system	43.8	45.3	46.2	49.3	54.5	54
Etc	15.5	32	26.6	4	5.3	3.4
not needed	14.7	25.8	19.7	2.6	6.2	4.7

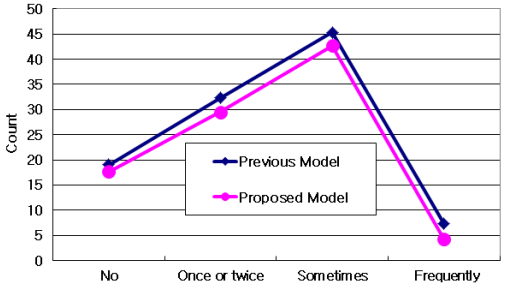

Fig. 3. The number of distribution for Dysfunctional of corporate Information

Fig. 3은 기업 내 발생되는 정보의 역기능에 대한 유통 건수를 기존 모델과 제안 모델을 비교평가하고 있다. 실험 결과, 제안 모델은 기존 모델에 비해 기업에서 사용하는 중요 정보를 불법적으로 유통하는 횟수가 17.9% 낮게 나타났다. 이 같은 결과는 제안 모델이 기업 정보의 불법 유통에 대한 관리·감독에 대한 역할을 기존 모델에 비해 강화한 구조를 만들었기 때문이다. 특히, 기업 정보를 불법적으로 유통할 수 있는 사용자의 직위 및 부서에 따라 추가 관리·감독할 수 있는 감사 역할을 추가하였기 때문에 나타난 결과이다.

Table 6은 기업에서 수행하고 있는 기업 정보 불법 유통에 대한 기업 측면에 수행하고 있는 대책을 크게 원천적 봉쇄, 이용자 자율규제, 정보내용 등급제, 기타, 필요 없음 등 5가지 항목으로 분류하여 제안 모델과 기존 모델을 비교하고 있다. Table 6의 수치 데이터는 53개의 기업을 대상으로 4주 동안 제안 모델을 적용한 결과를 설문을 통해 수집한 결과이다. Table 6의 결과, 제안 모델은 기존 모델에 비해 기업 정보의 불법 유통을 최소화하기 위한 방안으로 원천적 봉쇄, 이용자 자율규제, 정보내용 등급제 등을 엄격하게 적용하여 수행하였지만 기타, 필요 없음에 대한 항목은 기존 모델에 비해 낮은 결과를 얻었다. 기타, 필요 없음에 대한 항목에 대한 수치가 낮은 이유는 제안 모델을 통해 기업 외부로 기업 정보를 유통시킬 수 없는 환경이 만들어졌기 때문이다.

5. 결론

본 논문에서는 기업 내 정보의 역기능을 최소화하기 위해서 기업에서 생성되는 정보의 레벨에 따라 서비스 접근 레벨을 계층적으로 관리·감독 할 수 있는 기업 정보화 서비스 모델을 제안하였다. 제안 모델은 기업 정보를 생성하는 주체를 기업이 보유하고 있는 기술이나 기업 간 연계된 전자적인 정보, 정부의 제도적 지원 및 각종 규제에 따라서 다양한 기업 정보 접근 보안 정책을 적용할 수 있도록 역할을 세분화하였다. 실험 결과, 바이러스로 인한 기업 내 발생할 수 있는 시스템 전체 파괴, 시스템 점진적 마비, 시스템 일부 파괴, 별 지장 없음 등을 기존 모델과 비교 평가한 결과, 기존 모델에 비해 제안 모델이 48.8% 낮은 바이러스 피해를 받았다. 또한, 기업 내 발생되는 정보의 역기능에 대한 유통 건수는 기존 모델에 비해 제안 모델이 17.9% 낮은 결과를 얻었다. 향후 연구에서는 제안된 모델을 실제 환경에 적용할 수 있도록 구현하여 성능평가를 수행할 계획이다.

REFERENCES

[1] R. F. Powers and G. W. Dickson, “MIS Project Management : Myths, Opinions and Reality,” California Management Review, Vol. 15, No. 3, Spring, 1973.

[2] Y. S. Jeong, “Tracking Analysis of User Privacy Damage using Smartphone,” Journal of Convergence Society for SMB, Vol. 4, No. 4, Dec. 2014.

[3] K. I. Kim, “A Design of Managerial Accounting Information Characteristics considered the Organizational

Culture," Journal of Convergence Society for SMB, Vol. 4, No. 4, Dec. 2014.

[4] L. Raymond and N. Magnenat-Talmann, "Information Systems in Small Business : Are They Used in Managerial Decision?," American Journal of Small Business, Vol. 6, No. 4, pp. 20-26, Apr. 1982.

[5] F. Marc, M. Trevor, M. Devvie, E. Gerry, A. Teo, M. David, H. Kevin, B. Joseph, W. Paul, J. Eric and K. L. Mo, Symantec Internet Security Threat Report Trends for 2010, Symantec Corp., Vol. 16, 2011.

[6] L. Nataraj, S. Karthikeyan, G. Jacob and B. Manjunath, "Malware images: Visualization and automatic classification," VizSec '11 Proceedings of the 8th International Symposium on Visualization for Cyber Security, No. 4, pp. 1-15, 2011.

[7] D. A. Quist and L. M. Liebrock, "Visualizing compiled executables for malware analysis," 6th International Workshop on Visualization for Cyber Security, 2009 (VizSec 2009). pp. 27-32, 2009.

[8] S. H. Hong, "Research on Wireless Sensor Networks Security Attack and Countermeasures: Survey," Journal of Convergence Society for SMB, Vol. 4, No. 4, pp. 1-6, Dec. 2014.

[9] H. S. Jung, "Efficient and Secure Group Key Generation Protocol for Small and Medium Business", Journal of Convergence Society for SMB, Vol. 4, No. 4, pp. 19-23, Dec. 2014.

[10] X. Jiang, X. Wang and D. Xu, "Stealthy malware detection through vmm-based "out-of-the-box" semantic view reconstruction," 14th ACM conference on Computer and communications security (CCS '07). 2007. New York, NY, USA: ACM, pp. 128-138, 2007.

[11] V. P. Nair and H. Jain, Y. K. Golecha, M. S. Gaur and V. Laxmi, "MEDUSA: MEtamorphic malware dynamic analysis using signature from API," Proceedings of the 3rd international conference on Security of information and networks (SIN '10). 2010. New York, NY, USA: ACM., pp.263-269, 2010.

[12] P. Trinius, T. Holz, J. Gobel and F. C. Freiling, "Visual analysis of malware behavior using treemaps and thread graphs," 6th International Workshop on Visualization for Cyber Security, 2009 (VizSec 2009). pp. 33-38, 2009.

[13] F. Y. Zhang, D. Y. Qi and J. L. Hu, "Using IRP for Malware Detection," Recent Advances in Intrusion Detection in Lecture Notes in Computer Science. Springer Berlin/Heidelberg, Vol. 6307, pp. 514-515, Sep. 2010.

[14] I. Ahmed and K. S. Lhee, "Classification of packet contents for malware detection," Journal in Computer Virology, Vol. 7, Issue 4, pp. 279-295, Nov. 2011.

[15] M. Skrzewski, "Flow Based Algorithm for Malware Traffic Detection," Computer Networks in Communications in Computer and Information Science. Springer Berlin Heidelberg, Vol. 160, pp. .271-280, Jul. 2011.

저 자 소 개

정 윤 수(Yoon-Su Jeong) [정회원]

- 1998년 2월 : 대학교 전자계산학과 학사
- 2000년 2월 : 충북대학교 전자계산학과 석사
- 2008년 2월 : 충북대학교 전자계산학과 박사
- 2012년 3월 ~ 현재 : 목원대학교 정보통신공학과 조교수

<관심분야> : 유·무선 통신 보안, 정보보호, 헬스케어, 빅 데이터