Regular paper

Journal of the KIECS. pp. 405-410, vol. 13, no. 2, Apr. 30 2018, t. 88, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2018.13.2.405

정보보안 정책의 다변화 과정에 따른 일원화 절차의 제안과 적용에 따른 안전성 확보에 대한 연구

서우석*

A Study on Securing Stability following the proposal and Application of Integration Procedure following the Diversification Process of Information Security Policies

Woo-Seok Seo*

요 약

공공기관의 정보보안에 관한 다양한 지침이 제정 및 개정되는 등의 일련의 절차와 배급 및 지침 준수에 따른 성과 제도 등 다양하고 다변화된 과정을 하나의 일원화된 절차에 적용하여, 한 번의 개정 또는 변화는 전체 정보보안을 위한 일원화된 절차에서 모든 단계적 환경 조건을 기준으로 적용되어지는 연구와 활용이 이루어져 왔다. 다만, 각 기관들의 업무 영역과 보유하고 유지 및 보안성을 확보해야 하는 대상의 차이가 너무 이질적인 형태의 정보로써 이를 하나의 안전성 확보를 위한 절차에 일련의 과정으로 연계하는 데는 아직도 문제점을 나타내고 있는 것이 사실이다. 또한 공공기관이 예산 반영을 기반으로 구성하고 연구한 결과를 지침으로써 고지하고 이를 민간기관에 재배포 및 구성하는 데에도 시간과 추가적인 경비는 연구목적을 달성하는 부분에 또 다른 문제이기도 하다. 따라서 본 논문에서는 유사기관의 정보보안 대상을 선별 및 통계학적으로 분류하고 이를 정보보안 안전성 확보를 위한 일련의 다양성과 다변화 과정을 거친 일원화 절차를 제안하고 제안된 절차에 적용함으로써 최적의 안전성을 확보하는 연구를 하고자 한다.

ABSTRACT

Distribution of a series of procedure for establishment and revision for various instructions on information security for public institutions and diversified process of performance system following the compliance with the instruction are applied to the integrated procedure that any revision or change has led to the studies that are applied on the basis of all environment requirements and the facilitation of such studies in the integrated procedure for the entire information security. However, as the difference of possessing the work territory for each institution, maintaining and securing the security with the heterogeneous type for subject, the information still displays the issues to link to a series of process to the procedure to secure the foregoing as stability, In addition, the notice should be made by the public institutions for the result structured and notified on the basis of budget and the additional time and expenses for re-distributing to the private institutions would be another issue for the part to accomplish the purpose of such study. Therefore, under this study, the subject of information security of similar institutions should be sorted out and statistically classified, and it proposes the integration procedure through a series of diversity and multi-change process and summarize the same in the proposed procedure to engage in studies to secure the optimal stability.

키워드

Information Security, Policy, Diversification Process, Unification Process, Safety Secure
정보 보안, 정책, 다변화 과정, 일원화 과정, 안전성 확보

* 교신저자 : Security Consulting(Freelancer)
• 접 수 일 : 2018. 01. 06
• 수정완료일 : 2018. 02. 24
• 게재확정일 : 2018. 04. 15
• Received : Jan. 06, 2018, Revised : Feb. 24, 2018, Accepted : Apr. 15, 2018
• Corresponding Author : Woo-Seok Seo
Dept. Security Consulting, Gyeonggi-do R&D laboratory
Email :

Ⅰ. 서 론

공공기관을 시작으로 정보보안에 대한 정책적 보안 지침과 운영 그리고 활용에 따른 적용은 법적인 준수 여부에 대한 준거성으로 다소 더딘 진보를 했다.

다만, 일반기업 대비 수년간의 정보보안에 대한 투자는 소규모 전산 정보 시스템과 주변 환경 관리 부문에 진보된 정보보안의 정책과 실무적인 환경조성이 이루어진 것 또한 사실이다[1].

하지만, 각 기관마다 다양한 그리고 다변화된 정책을 별도로 적용하고 이를 상호 공유하지 않는 등 폐쇄적인 정보보안에 대한 기반 기술로 인해 매번 예산의 중복된 투입과 투입된 예산 대비 반비례하는 기관의 정보보안 완성도의 역효과가 발생하기도 했다.

따라서 본 논문에서는 이러한 주요 다변화 및 다양화 정책을 일원화하고 공통된 기반 전산 장비 및 시스템과 관리 환경을 구축하고 정보보안을 위한 일원화된 안전성 정책의 적용 절차를 표준화함으로써 책정된 예산에 대비하여, 높은 성과와 도출된 객관적인 성과 대비 완벽한 안전성 환경 확보를 도출함으로써 관리상의 효율성까지도 제안하고자 한다[2-3].

이러한 일련의 제안 과정을 통해 본 논문은 1장에서는 연구하고자 하는 목적과 방향성 그리고 현재의 현황 등을 언급하고 2장에서는 정보보안과 같은 전반적인 보안에 대한 정책의 변화와 안전성 확보 기반기술 그리고 각 기관과 기업의 정보보안 기술의 개별화된 현황 등을 세세히 파악하고 3장에서는 정보보안 정책의 다변화 과정에 따른 일원화 절차와 안전성 제안기술을 제시하고자 한다.

마지막으로 4장에서는 정책 이원화의 문제점 해소와 일원화 절차 제안과 적용을 통한 안전성 확보의 실효성의 극대화를 연구결과로 제시하고자 한다[4-5].

Ⅱ. 관련연구

본 관련연구에서 제안하고자 하는 내용은 다양한 기관이 받아들이는 정보보안 정책에 대한 이해와 적용사례를 통해 다양한 문제점에 대한 현황을 파악하고 제시 및 연구함으로써 결론에 대한 기초 자료를 확보코자 한다.

2.1 정보보안 정책의 변화와 현황

정보보안 정책은 최초 각 기관 또는 기업마다 보유한 정보자산에 따른 그리고 자산의 등급에 따른 통계학적 적용 솔루션 등의 분류와 활용과 같은 세부적인 접근이 아닌 네트워크 백본에 일괄적인 보안 네트워크 장비 적용이 흔한 정보보안 사례이다.

따라서 정보보안과 같이 다양하고 다변화된 대상 매체가 발생함에 따라 각 기관과 기업의 정보보안을 위한 안전성 확보 정책인 관리적인 부문과 물리적인 기술 부문에 대해 상호 우월감을 표명하는 수단으로 전락하기도 했다[6].

이는 곧 정보보안의 원래의 목적을 달성하기 위한 결과로써 반영되는 것이 아니라 해당 전산 구축 내역에 대한 대외적인 마케팅 효과와 같은 금전적 이익을 위한 수단으로도 활용되어졌다[7-8].

*** 초기 정보보안 정책적 문제점 :** 정보보안 자산에 대한 정확한 현황 파악도 못한 상태에서 단순 온라인 접근 단일 경로에 대한 접근권한 관리 등과 같은 초기 단순 보안 기술적용 등을 대외적으로 기관과 기업의 정보보안의 안전성을 100% 자신하는 우월감의 표현으로 활용

*** 초기 정보보안 기술적 문제점**

(1) 문제점 1 : 네트워크 접근에 대한 정보보안 물리적 기술적용을 최선으로 판단

(2) 문제점 2 : 인적자원에 대한 정보보안 관리와 접근권한 관리에 대한 부분은 자동화 하지 않고 페이퍼 관리 형태로 수년간 지속 관리

(3) 문제점 3 : 상황발생 시마다 대처했던 방법에 대한 정확한 분석과 결과에 대한 신뢰도를 검증하는 과정을 생략하고 성공한 경우를 물리적 기술지침으로 활용

2.2 정보보안 기반의 안전성 확보 기반 기술현황

국내에서 접하고 적용 가능한 정보보안에 대한 물리적 기반의 기술은 다수의 다양한 그리고 다변화된 기업과 기관의 정책을 상호 규제하는 부분의 역할로 활용함에 따라 많은 제약을 가지고 왔다.

따라서 이는 정보보안에 확대를 통한 기술의 진보보다는 표 1과 같이 네트워크 및 시스템 보안이라는

Category에서 벗어나지 못하는 형태가 되고 말았다[9-10].

표 1. 초기 정보보안을 위한 안전성확보 물리적 기술기반 주용 핵심 적용기술 현황
Table 1. Securing safety for initial information security Status of core applied technology based on physical technology

Technology	Content
Network Security	In the initial stage, it is decided to lease the network communication line or to occupy the network according to the important business rank, and it is determined that the closed network guarantees the technical safety
System Security	In the case of various application software, intensive management is carried out centrally. Therefore, only the basic operating system and system-based firmware ware are applied to the management of security and application of technology.

2.3 기관 및 기업 보유 정보보안 대상의 차이와 분류

정보에 대한 자산분류가 통계학적으로 이루어지지 않고 단순 관리 포인트 차원 또는 업무적 성격에 따른 분류가 발생함에 따라 정보보안의 허점으로 인한 사고가 발생시에도 어떠한 최종 문제점이 발생했는지를 인지하기가 어렵다.

따라서 정보자산의 정확한 분리와 정의 그리고 자산에 대한 각각의 식별자가 존재하게끔 관리정책의 일원화를 진행해야 한다.

*** 환경 및 현황 :** 정보자산 확인 및 구성과 관리 포인트 파악과 목적 구분 불가 상황

III. 정보보안 정책의 다변화 과정에 따른 일원화 절차와 안전성 제안

3.1 정책의 다변화 내역의 통계적 공통변수 제시

정보보안에 대한 사전적 정의를 기준으로 정책을 설립하고 이를 수용하는 단계적 다변화 기관 또는 기업이 있는 경우도 있으나, 실전에서 얻어진 사례를 기반으로 기관 내부 정보보안 정책을 제정한다.

법률과는 상이한 내부 전산환경에 맞춘 상황적 변화에 적응한 정책을 반영하는 경우 등 많은 변화를 보이고 있다.

다만 정책의 기준이 객관적인 통계학적인 방안과 수치에 따라 정보자산을 선정한다.

이어 선정된 자산별 등급을 설정하고 설정된 수치에 따른 정확하고 빠른 대처 프로세스 코드 매핑이 이루어져야 한다,

이러한 과정을 위해서는 다양한 환경 정책상의 일원화를 위한 공통변수 개발에 대한 아이디어와 기획 및 지원이 절실한 상황인 것이다.

3.2 일원화 정보보안 안전성 확보 절차 기준 제시

주요 핵심 정보보안 정책의 다변화와 다양한 변화에 대한 일원화 공통변수가 설정된 이후부터는 절차에 대한 예시와 경우의 수(대처방안)를 구상해야 한다.

구상되어진 대처방안에 대해 등급별로 재설정함으로써 단계별 관리자 또는 자동화 시스템이 인지한 침해에 대한 안전성을 확보한 대처 절차가 실행되는 환경을 구현한다.

다만 법적인 안전성확보조치 기준을 기준으로 최종 절차에 대한 기준을 공통화 함수로 구성하고 함수내의 지표 또한 공통된 정보보안을 위한 점검지표로 선정해야 한다.

따라서 표 2는 일원화된 정보보안의 안전성을 확보하는 절차에 대한 기준 척도로써 공통변수와 점검지표 2가지로 구성 및 구분하여, 각각의 활용과 기준에 대한 정의를 제시하고 있다.

표 2. 안전성 확보 절차 준수를 위한 2가지 기준 제시
Table 2. Two criteria for compliance with safety procedures

division	Contents
Common variable	values that can be grasped by disturbance caused by infringement are proposed as common variables that apply virtual parameters to information security handling procedures and configurations of various environments
Check index	In this paper, we propose an unified security measure for organizations and companies that measure the security standard, and we set common variables for various environmental values of cumulative information security policy

3.3 다변화 정책 변수와 일원화 안전성 확보절차의 연계성 적용

공통변수와 공통변수를 측정하기 위한 점검지표를 세분화 하는 과정을 필요로 한다. 모든 경우의 수를 1,00가지로 예측한다면, 예측한 모든 지료를 측정하고 이를 통계학적으로 안전성을 확보 가능한 최적의 공통변수 값으로 도출하기란 정보보안을 위한 너무나 많은 그리고 다양하고 다변화된 모든 변수와 지표에 대한 정책적 기준 선정의 어려움이 있어 가장 최적의 점검과 가장 최고의 효율성을 확보하기 위한 두 조건의 연계가 필요로 대두되어 진다.

* ***최적화(가상화 논리적 표현)*** : *"공통변수" ∩ "점검지표*

Ⅳ. 안전성 확보 정보보안 정책 표준절차에 대한 확인과 구현

4.1. 정책 구현

안전성확보조치 기준의 다변화와 각기 다른 환경에서 생성된 정보보안 침해에 대한 사례를 본 논문에서 논리적으로 구상하고 제안한 최적화 및 일원화 안전선 황보 조치를 위한 절차에 반영하여, 수향한 결과에 대한 신뢰성과 효율성을 수치로 변환 확인 후 이를 각 해당 테스트 시행을 진행한 기관과 기업에 반영 누적 정보를 그림 1과 같이 재확인한다.

*** 적용 프로세스(절차)**

가. 정보자산(정보시스템, 정보보호시스템 2개 대상 핵심 시스템 분류)
  (1) 자산 파악
  (2) 자산별 위험 등급 지정 및 식별자 배포
  (3) 1차 자산 위험 분류 및 위험 등급에 따른 위험 가중자산 (Risk Weighted Assets) 별도 분류

나. 정보자산 등급 책정
  (1) 위험 등급 가 책정 결과에 대한 공통 자산, 공통 등급 내 유사 자산 Group 구성 및 파악
  (2) 위험 등급 대비 자산 Group 매핑

다. 공통변수 선정
  (1) 매핑 정보에 따른 기초 환경 파악 단계 확정
  (2) 다변화된 침해와 위협에 대한 안정성 Group 등급 조건에 대한 공동변수 책정

라. 점검지표 개발
  (1) 공동 위험 요소에 대한 Group 안정성 확보 조치 기준 준수를 위한 최소한의 준수 지표 개발
  (2) 개발 시 타 안정성 확보 현황 및 인증 준수 조건 ISMS 인증 등과 같은 타 지표와의 비교 검토 사전 요건
  (3) 기업 또는 기관 내 고유 점검 지료 개발

마. 융합 환경과 변수 확정
  => 정보보안 점검 객관성 확보 단계

바. 정보자산 특정

사. 정보보안 최적화 측정 값 도출
  => 수치적 변화 값 도출

아. 실무환경에 적용 : 적용과 현황 수집 단계

자. 누적 환경 변화 수치 DB화

차. 피드백

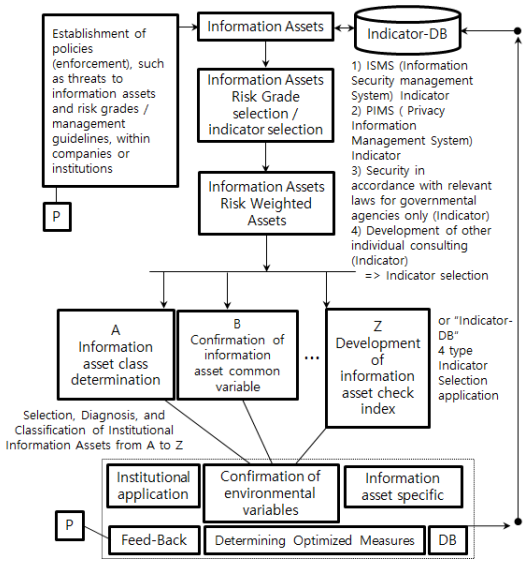

그림 1. 정책 적용 프로세스(절차)
Fig. 1 Policy enforcement process(Procedure)

4.2 정책변화와 최적화 안전성 기준 확보

주요 핵심 정보보안 정책의 다변화를 위한 최적화된 안전성확보조치 기준은 공통변수와 점검지표에 따른 최종 점검 이후 얻어진 결과에 따른 기관과 기업에 맞게끔 보완 및 수정 후 이를 적용함으로써 그림 2는 최종 본 논문에서 제안하는 최적의 안전성 확보를 위한 기준과 정보보안의 실효성 확보 및 실제 침해 차단을 위한 논리적인 정책적 연구의 향후 방향성을 제시하는 흐름을 나타낸다.

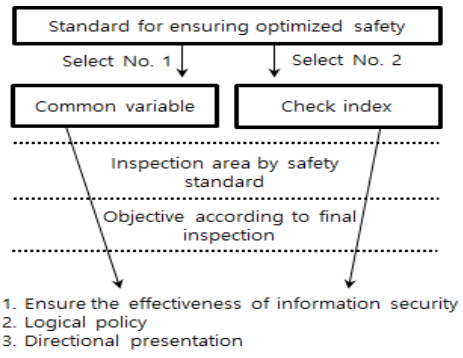

그림 2. 안전성확보조치 기준에 의한 3가지 제안 결과 도출 흐름
Fig. 2 Three suggestions based on safety assurance measure criteria Result flow

4.3 제안 구현 결과에 따른 정책과 안전성 효과 확인

제안된 다변화 및 다양한 기준을 가진 정책 하에 얻어진 결과 수치를 권장하는 적용 프로세스(절차)에 따라 구현함으로써 정보보안의 안전성확보가 결국에는 안정성으로 그 결과를 도출한다.

V. 결 론

본 논문에서는 수많은 300여개 이상의 공공기관과 수요 및 편성 예측까지도 너무 빠른 변화로 인해 예측이 불가능한 기업을 대상으로 정보보안 정책을 교육하고 제안하는 등의 활동을 통해서 다양화 및 다변화된 각각의 정보보안 Infra를 일원화하고 정책의 정용과 반영이 기계화 또한 소프트웨어 관리 수준의 간략하고 단편적인 적용을 통한 효율성을 확보하는데, 목적을 두고 연구를 진행했다.

물론 동일한 정보보안 안전성 확보를 위한 관리적, 물리적, 논리적 3단계 지침 준수를 일률적으로 적용하는 단순 절차 제안에 따른 한 번의 공격으로 전체 기관과 기업의 정보가 노출되고 보안의 실효성과 안전성을 보장 못하는 수준의 기술기반을 일원화 하는 부분을 제안하는 것이 아니라 각각의 특성과 정보보안의 대상을 통계학적으로 분류하고 자산관리 및 자산 분류 등의 기초현황에 따른 객체화 보안 모듈을 큐브와 같은 형태로 제안하고 구성 및 운영하고자 하는 것이다.

따라서 향후 논문 주제에 대한 연구방향은 이러한 정책과 대상조직과 대상 정보에 대한 다각적인 큐브 형태의 안전성 확보를 위한 기술 다변화 과정을 연구하는 과정이 필요하다.

References

[1] Y. Joung, “Legal Concept :Based on Analysis of Cases about Information Security,” *Public law journal*, vol 14, no. 4, 2013, pp. 209-243.

[2] J. Jeong and M. Choi, “A Study on Awareness of Information Security Influencing Trustness,” *Journal of the Korean Institute of Information*

Security and Cryptology, vol. 25, no. 5, 2015, pp. 1225-1233.

[3] M. Lee, "A Development of Curriculum for Information Security Professional Manpower Training," *Journal of the Institute of Electronics and Information Engineers*, vol 54, no. 1, 2017, pp. 46-52.

[4] K. Son, "Status and Prospects of IT Security Industry in Korea," *Communications of the Korean Institute of Information Scientists and Engineers*, vol 28, no. 11, 2010, pp. 72-78.

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

[6] S. Son, J. Park, and S. Moon, "A Study on Improvement Measures of Information Security Relevant Laws for IoT Service Providers," *Institute of Law Studies College of Law and Political Science*, Pusan National University, vol 57, no. 1, 2016, pp. 181-215.

[7] S. Kim and Y. Song, "An Empirical Study on Motivational Factors Influencing Information Security Policy Compliance and Security Behavior of End-Users(Employees) in Organizations," *Global e-Business Association*, vol 12, no. 3, 2011, pp. 327-349.

[8] 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.

[9] J. Jang, C. Choi ,and D. Kim, "Design of Smart Tourism in Big Data," *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," *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