석사학위논문

지방자치단체의 정보보호서비스 대가 산정 모델 적용 성과 분석 및 개선 방안

Performance Analysis and Improvement for the Cost Model of Information Protection Services

제주대학교 대학원

융합정보보안학협동과정

오 상 익

2020년 2월

지방자치단체의 정보보호서비스 대가 산정 모델 적용 성과 분석 및 개선 방안

지도교수 조 정 원
지도교수 박 남 제

오 상 익

이 논문을 융합정보보안학협동과정 석사학위 논문으로 제출함

2019년 12월

오상익의 융합정보보안학협동과정 석사학위 논문을 인준함

심사위원장 변 영 철 ㊞

위 원 박 남 제 ㊞

위 원 조 정 원 ㊞

제주대학교 대학원

2019년 12월

목 차

표 목 차

그 림 목 차

요 약

초연결 ICT융합기술과 서비스가 발전하면서 보안위협의 양상이 기존 개인을 대상으로 한 개인정보 유출이나 단순한 금전 탈취 수준을 넘어 국가나 지방자치단체, 공공기관 등을 대상으로 한 사이버 공격이 늘어나고 있다. 국내외적으로 많은 기관에서는 각종 침해사고를 능동적이고 선제적으로 예방하기 위해 다양한 정보보호 관리체계 제도를 도입하여 운영하고 있다. 하지만, 시군구 단위의 지방자치단체인 경우 정보보호를 위한 자발적인 관심과 노력이 낮고 침해사고가 발생할 당시에만 정보보호에 관심을 갖고 그에 따른 예산을 편성하기에 급급하여 속출하는 사이버 공격의 위협에 효과적으로 대응하지 못하고 있는 실정이다. 이러한 산업 전반에 뿌리박힌 정보보호에 대한 낮은 인식과 적용, 전문 인력 부족 등의 고질적인 정보보호 생태계에 대한 체질을 개선하고 선순환 구조를 조성하고자 과학기술정보통신부가 2015년에 정보보호 산업 진흥에 관한 법률을 제정하였다. 이 법률에는 정보보호업체가 공공기관이 도입한 정보보호제품 및 정보보호서비스에 대한 품질 향상을 위하여 정보보호서비스 대가 산정체계를 도입하였고, 이들 기관에서는 제공받고 있는 정보보호서비스에 대해 적정한 대가를 지불할 수 있도록 하였지만, 이 제도를 도입한 기관은 그리 많지 않다.

본 논문은 정보보호서비스 대가 산정체계를 도입하여 운영 중인 기관의 사례분석 및 이용자 대상으로 정보보호서비스 제공과 관련하여 적정한 정보보호서비스 대가 산정 모델 적용에 대해 세밀하게 분석하여 조직의 정보보호성과에 어떠한 영향을 미치는지 실증을 위해 기존 문헌을 중심으로 선행연구 조사와 도입기관의 사례분석을 통해 연구모형과 연구가설을 도출하였고, 가설검증을 위한 자료를 수집하기 위하여 설문조사를 실시하였다. 설문조사는 정보보호서비스 대가 산정 모델 도입 기관의 정보보호 및 정보화담당자를 비롯한 정보화담당부서 공무원들과 이 기관을 대상으로 한 정보화 및 정보보호 관련 프로젝트를 수행하거나 수행한 경험이 있는 제주지역 ICT업체를 대상으로 실시하였으며, 수집된 자료를 바탕으로 다중회귀분석방법을 이용하여 가설검증을 하였다. 정보보호서비스 대가 산정 모델과 정보보호성과에 미치는 영향에 대한 실증 분석결과를 살펴보면, 정보보호서비스 품질은 정보보호성과에 긍정적인 영향을 부분적으로 미치고 있음이 확인되었으며, 정보보호서비스에 대한 적정한 비용 산정을 위한 정보보호서

비스 대가 산정 모델 적용은 정보보호서비스 품질 향상에 긍정적인 영향을 부분적으로 미치고 있음이 확인되었다. 또한, 정보보호서비스 대가 산정 모델을 기관에 도입하여 이에 따른 적용이 정보보호성과에 긍정적인 영향을 부분적으로 미치고 있음이 확인되었다. 정보보호서비스 대가 산정 모델이 국가 및 공공기관에 정착되려면, 현재 정보보호 산업 진흥에 관한 법률에 정보보호서비스 대가 산정 체계를 도입할 수 있다고 권고수준에서 명시한 조항을 '국가 및 공공기관에서는 반드시 반영하여야 한다.'고 강제성을 부여하도록 개정할 필요가 있으며, 국가 및 공공기관이 정보보호서비스 대가 산정 모델 도입을 자발적으로 유도하기 위한 '정보보호 적용 인센티브'를 마련할 필요가 있다.

본 논문은 지방자치단체의 정보보호서비스 대가 산정 모델 도입이 정보보호성과에 미치는 영향에 관해서 실증연구와 현행 정보보호서비스 대가 산정 모델의 문제점과 개선방안을 도출했다는 점에서 기존 연구와 다른 관점에서의 연구이며, 향후 정보보호서비스 대가 산정 모델 도입을 검토하는 국가 및 공공기관이나 공공과 정보보안 산업과의 상생할 수 있는 건전한 정보보호 산업의 생태계 조성과 관련된 정책 수립 시 유용한 참고자료로서 활용될 수 있는데 의미를 갖게 될 것으로 기대된다.

주제어 : 정보보호서비스, 정보보호서비스 대가 산정 모델, 정보보호성과, S-SLA, SERVQUAL

Ⅰ. 서 론

1. 연구의 필요성

본격적인 지능정보사회로의 도래로 초연결 ICT융합기술과 서비스가 발전하면서 보안위협의 양상이 기존 개인을 대상으로 한 개인정보 유출이나 단순한 금전 탈취 수준을 넘어 국가나 지방자치단체, 공공기관 등을 대상으로 한 기반시설 공격으로 인한 사회적 혼란을 유도하거나, 국가-국가 간 사이버 전쟁수준으로 진화하고 있다.

사이버 위협으로부터 사전 예방과 지속적인 대응을 위해 정보보호서비스의 중요성이 커지고 있으나 국내는 다른 국가들에 비해 제도적인 측면과 현실 측면에서 차이가 큰 것으로 나타났다. 특히, 기초 지방자치단체인 경우 정보보호를 위한 자발적인 관심과 노력이 낮고 침해사고가 발생할 당시에만 정보보호에 관심을 갖고 그에 따른 예산을 편성하기에 급급하여 속출하는 사이버 공격의 위협에 효과적으로 대응하지 못하고 있는 실정이다.

정보보호시스템은 하드웨어와 소프트웨어, 또는 하드웨어와 소프트웨어가 결합한 일체형으로 분류되어 있는데, 그동안은 정보보호시스템에 대해서만 유지관리에 따른 일반 대가를 적용받도록 정책이 되어 있어, 보안위협에 대한 지속적인 보안 서비스에 대한 적정한 대가를 제대로 인정받지 못하는 결과를 얻게 되었다. 이에, 정보보안 산업의 위축으로 인해 글로벌 시장에서의 경쟁력 우위를 점하지 못하는 요인으로 작용하고 있다. 이러한 산업 전반에 뿌리박힌 정보보호에 대한 낮은 인식과 적용, 전문 인력 부족 등의 고질적인 정보보호 생태계에 대한 체질을 개선하고 선순환 구조를 조성하고자 과학기술정보통신부가 2015년에 정보보호 산업 진흥에 관한 법률을 제정하였다.

이 법률에는 정보보호업체가 국가기관이나 지방자치단체, 공공기관이 도입한 정보보호제품 및 정보보호서비스에 대한 품질 향상을 위하여 정보보호서비스 대

가 산정체계를 도입하였고, 이들 기관에서는 제공받고 있는 정보보호서비스에 대해 적정한 대가를 지불할 수 있도록 하였다.

하지만, 수요자인 공공기관 담당자와 공급자인 정보보안업체 간의 인식차이가 크다보니 현실적으로 정착하는데 큰 걸림돌이 되고 있다.

본 연구에서는 현재 이제도를 도입하고 있는 기관의 사례분석 및 이용자 대상으로 정보보호서비스 제공과 관련하여 적정한 정보보호서비스 대가 산정 모델 적용에 대해 세밀하게 분석하여 조직의 정보보호성과에 어떠한 영향을 미치는지 실증검증을 통해 공공기관과 정보보안 산업과의 상생할 수 있는 생태계 조성과 본 제도의 정착을 위한 유용한 기초자료로 활용될 수 있도록 하는데 의미를 두고 있다.

2. 연구의 목적

본 연구는 지방자치단체가 조직의 정보보호 관리체계 수준을 향상시키기 위하여 적절한 수준의 정보보호서비스 품질을 위한 적용를 하고 있는지, 즉 정보보호서비스에 대한 대가 산정 모델을 적용한 적용를 통해 질 높은 정보보호서비스 품질을 만들고, 이를 통해 창출된 정보보호서비스 품질이 정보보호성과에 미치는 영향을 조사하는 것을 목적으로 한다. 또한, 정보보호서비스 제공과 관련하여 적정한 정보보호서비스 대가 산정 모델 적용에 대해 세밀하게 분석하여 조직의 정보보호성과에 어떠한 영향을 미치는지를 알아봄으로써 지방자치단체와 정보보안 산업과의 상생할 수 있는 윈-윈 전략 수립 시 활용될 수 있고, 조직의 정보보호 관리체계 전략 수립에 유용한 기초자료로 활용될 수 있도록 하는데 의미를 두고 있다. 구체적인 연구의 목적은 다음과 같다.

첫 번째, 정보보호서비스 품질 활동이 정보보호성과와 어떠한 관계가 있으며, 정보보호서비스 품질 요소 중 신뢰성, 반응성, 전문성, 대응성, 연속성이 정보보호성과의 개선에 얼마나 효과가 있을 것인지를 살펴보고자 한다.

두 번째, 정보보호서비스 품질이 정보보호서비스 대가 산정 모델 적용와 어떠

한 관계가 있으며, 어느 수준의 정보보호서비스 대가 산정 모델 적용이 정보보호서비스 품질의 개선에 얼마나 효과가 있을 것인지를 살펴보고자 한다.

세 번째, 정보보호서비스 대가 산정 모델에 대한 적절한 적용이 기관의 정보보호성과의 개선에 얼마나 효과가 있을 것인지를 재무적 성과와 비재무적 성과로 구분하여 실증적으로 분석하고자 한다.

본 연구에는 서비스 품질 측정방법 중 가장 많이 이용하고 있는 PZB(1988)의 SERVQUAL 모형을 정보보호서비스 품질에 적합하도록 재구성하여 정보보호서비스 대가 산정 모델 적용에 중점을 두어 정보보호서비스 대가 산정 모델 적용이 정보보호서비스 품질에 어떠한 영향을 미치는 지, 정보보호성과에 어떠한 영향을 미치고 이러한 영향에 의하여 정보보호성과는 어떻게 변하는지에 대한 구조적인 관계를 밝히는 것에 연구목적이 있다.

2. 연구의 범위와 방법

본 연구의 방법은 연구 목적을 달성하기 위해 기존 문헌을 중심으로 이론적 배경을 고찰하였다. 이론적 배경은 본 연구와 관련된 연구논문, 연구보고서, 법령집, 가이드 및 매뉴얼, 웹서핑 등의 국내·외 문헌을 중심으로 정보보호서비스, 정보보호서비스 대가 산정 모델, 서비스 품질, 정보보호성과에 대하여 살펴보았다. 다음은 정보보호서비스 대가 산정 모델을 도입한 기관의 사례를 분석하였다. 사례분석은 분석 프로세스 정립, 기관의 정보보호서비스 현황조사, 기관의 정보보호서비스 대가 산정 모델 설계 및 관련 예산 추이 분석, 도입 효과와 문제점 등에 대하여 살펴보았다. 문헌조사와 사례분석을 통해 설정된 연구목적을 실증적으로 고찰하기 위하여 연구가설을 도출하였고, 가설검증을 위한 자료를 수집하기 위하여 설문조사에 의한 실증적 연구를 하였다.

본 연구의 실증분석을 위한 자료 수집과 회수는 다음과 같이 수행하였다. 설문대상자를 국내 유일하게 정보보호서비스 품질에 대한 대가 모델을 적용 도입하고 있는 서귀포시 정보보호 및 정보화담당자를 비롯한 정보화담당부서 공무원들

과 이 기관을 대상으로 한 정보화 및 정보보호 관련 프로젝트를 수행하거나 수행한 경험이 있는 제주지역 ICT 업체로 설문지를 직접 찾아가 면담을 통한 설문지 작성 방법과 e-메일을 통해 송부하여 이루어졌다.

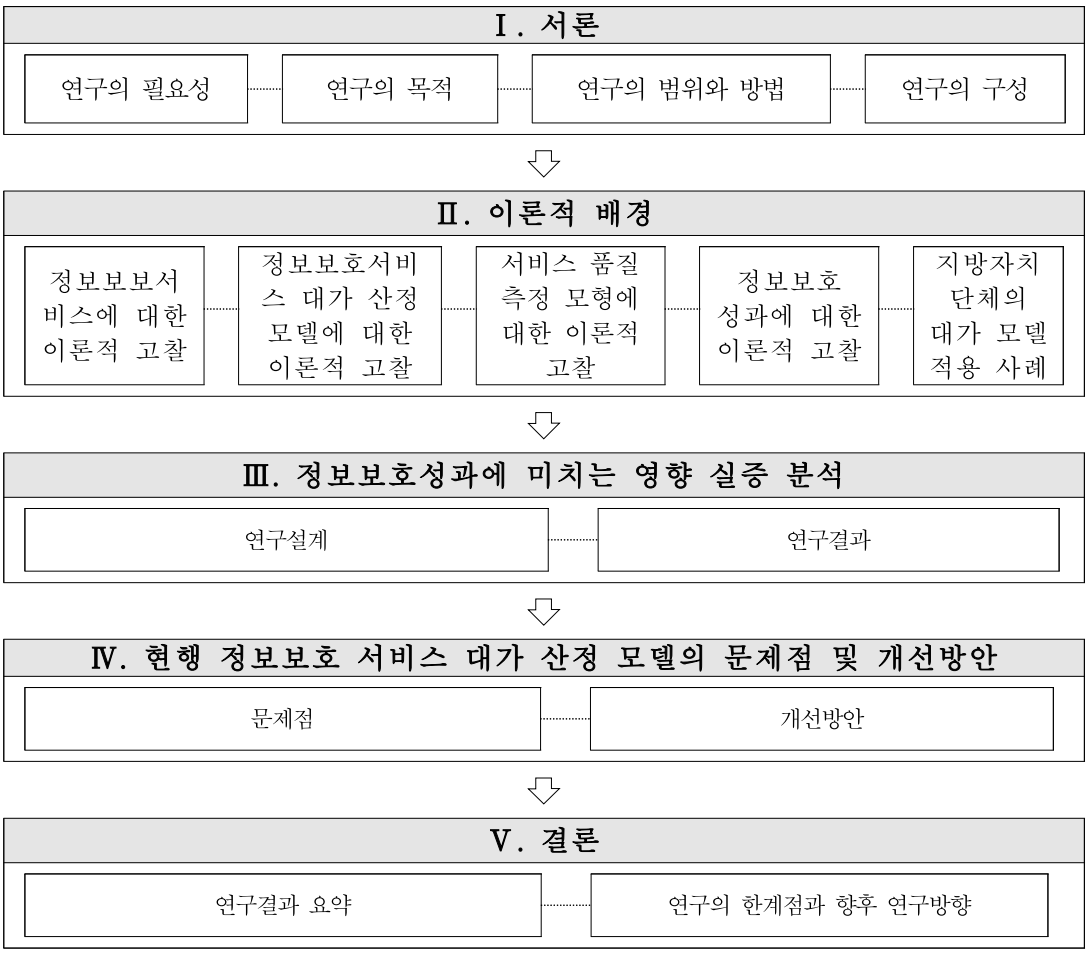
본 조사에 앞서 설문의 신뢰도를 높이기 위해 예비조사를 2019년 9월 16일부터 9월 18일까지 3일간 서귀포시 정보보호업무를 담당하는 공무원 20명을 대상으로 20부의 설문을 실시하였고, 설문 항목 중 이해하기 어렵거나 애매한 내용이 있는 문항들에 대해 자문을 받아서 수정 보완하였다. 본 설문조사는 2019년 9월 23일부터 10월 4일까지 12일간 실시하였다. 조사기간 동안 총 128부의 설문을 송부하여 89부의 설문지가 회수되었으며, 일부 불성실한 답변을 제외한 87부가 최종 분석에 사용되었다.

수집된 자료를 바탕으로 항목들 간의 신뢰성 분석을 위해 Cronbach's α계수를 이용하여 신뢰성 검증을 하였으며, 설문조사 항목들의 판별 타당성 확보를 위해 요인분석을 실시하였다. 최종 잔여변수를 중심으로 변수 간의 상관관계 분석을, 다중회귀분석방법을 이용하여 가설검증을 하였으며, 이 들 분석에는 IBM SPSS Statistics 프로그램을 이용하여 실시되었다.

3. 연구의 구성

본 연구의 구성은 총 5장으로 구성되어 있다. 제Ⅰ장 서론에서는 연구의 필요성, 연구의 목적, 연구의 범위와 방법, 연구의 구성을 밝히고 있다. 제Ⅱ장 이론적 배경에서는 정보보호서비스, 정보보호서비스 대가 산정 모델, 서비스 품질, 정보보호성과에 대한 이론적 검토가 이루어지고, 이에 대한 문헌연구를 정리하고자 한다. 또한, 도입기관의 사례분석은 기관의 정보보호서비스 현황, 기관의 정보보호서비스 대가 산정 모델 설계, 도입효과와 시사점에 대해 분석하고자 한다. 제Ⅲ장 정보보호성과에 미치는 영향 분석에서는 정보보호서비스 품질과 정보보호서비스 대가 산정 모델 적용, 정보보호성과 간의 관계가 설정되어 연구모형을 수립하고자 한다. 이를 통해 가설이 설정되고 설문조사에 대한 내용적 분석이 이루

어질 것이다. 또한, 연구 결과에서는 정보보호서비스 품질과 정보보호성과, 정보보호서비스 품질과 정보보호서비스 대가 산정 모델 적용, 정보보호서비스 대가 산정 모델 적용와 정보보호성과 간의 유의한 차이가 있는지 확인을 위하여 IBM SPSS Statistics 프로그램을 이용하여 분석이 이루어질 것이다. 설문조사를 통해 수집된 자료들을 분석하여 설문항목의 신뢰성과 변수의 개념 타당성을 확보한 후 연구가설 검증을 실시하고, 검증 결과를 분석하고자 한다. 제Ⅳ장 정보보호서비스 대가 산정 모델의 문제점과 개선방안에서는 현행 정보보호서비스 대가 산정 모델 운영상의 문제점을 파악하고 이에 따른 개선방안을 도출하고자 한다. 제Ⅴ장 결론에서는 연구의 시사점과 한계점을 밝히고 향후 연구방향을 제시하고자 한다.



[그림 Ⅰ-1] 연구의 구성

Ⅱ. 이론적 배경

1. 정보보호서비스에 대한 이론적 고찰

1) 정보보호의 정의와 관리

지식정보사회의 핵심 인프라인 정보는 국가나 조직의 전략과 목표를 달성하기 위해 없어서는 안 될 중요한 필수요소라 할 수 있다. 이러한 정보와 이를 저장·관리하고 있는 시스템이 악의적인 해커나 비인가자에게 노출되거나 유출된다면 큰 위험을 초래할 수 있기 때문이다. 특히 국가기관·지방자치단체에서 ICT 기술을 활용하여 쉽게 정보를 수집·가공·저장·검색·송신·수신을 하고 있다. 하지만, 관리적·물리적·기술적 보안 취약점으로 인하여 데이터의 유출, 훼손, 변조 등의 위험이 증가하고 있다. 따라서 정보보호활동은 민간뿐만 아니라 국가기관·지방자치단체에서도 반드시 수행해야 할 중요한 부분이 되었다.

정보보호는 출처에 따라 다양하게 정의되어 있는데, 「정보보호 산업의 진흥에 관한 법률」 제2조에 정의된 정보보호의 정의를 살펴보면, 데이터의 수집·가공·저장·검색·송신·수신 중에 발생할 수 있는 데이터의 유출·변조·훼손 등의 방지 및 복구활동을 수행위한 관리적·물리적·기술적인 수단을 마련하는 것을 말한다. 공급자와 이용자 측면에서의 정보보호를 살펴보면, 내·외부의 보안위협 요소들로부터 시스템, 네트워크 등 시스템의 DB, 정보자산 등을 안전하게 보호하고 운영하기 위한 모든 활동으로, 이용자 측면에서 보면, 개인정보 유출, 남용, 금전적 피해 등을 사전에 방지하기 위한 활동으로 볼 수 있다.

기존의 정보보호가 사이버 침해 대응을 위한 사이버 보안 중심이었다면 최근에는 ICT 기술과 연계 및 융·복합되면서 사이버 공간에서의 위험성이 현실세계로 확장되어 대부분의 디바이스에 보안이 필요한 시대가 본격적으로 도래함에 따라, 정보보호의 범위가 사이버 보안, 물리보안, 융합보안으로 확장되고 있다. 현재의 정보보호의 정의를 살펴보면, 데이터의 흐름과정에서 훼손과 유출 등을

방지하고, 데이터의 훼손, 유출, 변조 등이 발생할 경우 이를 복구하는 것을 규정하고 있으며, 암호・인증・감시・인식 등의 물리보안기술을 활용하여 범죄, 재난・재해 등에 대응하거나 관련 자산을 안전하게 운영하는 것을 규정하고 있다. 또한, 스마트 팩토리, 스마트 그리드, C-ITS, 스마트의료, 스마트 홈 등에 대한 보안도 융합보안 관점으로 이에 속한다고 규정하고 있다.

[표 Ⅱ-1] 정보보호 분류

분류	사이버 보안	물리보안	융합보안
산업 유형	시스템・네트워크 보안, 관제, 디지털 포렌식 등	바이오인식, 무인 전자경비, 영상감시 등	스마트 팩토리, 스마트그리드, C-ITS, 스마트의료, 스마트 홈 등에 대한 보안

정보보호는 무결성(Integrity), 기밀성(Confidentiality), 가용성(Availability) 등 3가지 속성을 정보의 보안성이라고 말하는데, 이를 지키는 것이 정보보호의 목적이다.

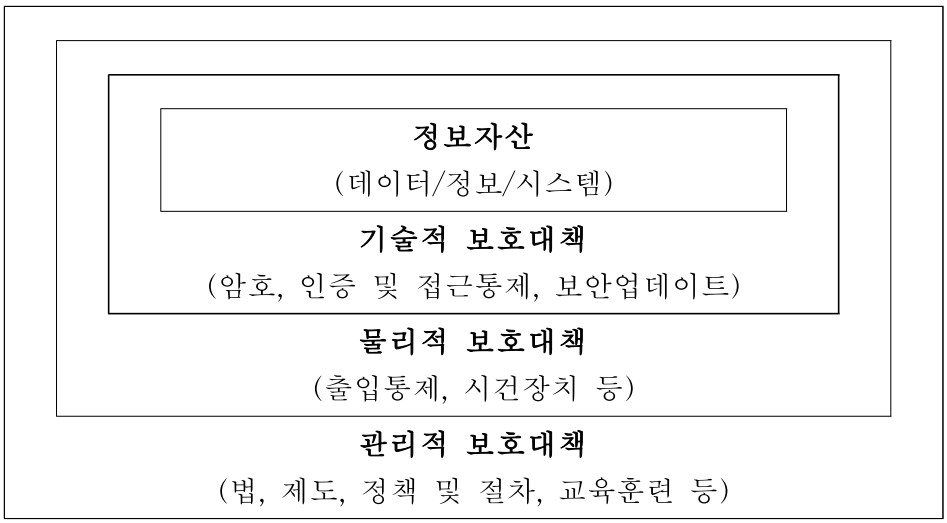
무결성(Integrity)은 정확성을 보증하는 것을 말하는데, 네트워크를 통해 송수신되는 데이터가 위・변조되지 않도록 데이터의 정확성, 유효성, 일관성, 신뢰성을 유지하여 데이터에 부정합과 결손 없이 의도된 목적에 따라 정보가 이용되는 것을 말한다. 무결성의 위협요소는 바이러스(Virus), 프로그램 오류, 백도어(Backdoor) 등이 이에 해당한다.

기밀성(Confidentiality)은 허가된 사용자 및 시스템만 접근할 수 있도록 보호하는 서비스를 말하는데, 기밀성을 유지하기 위해 정보가 유출되더라도 그 데이터를 식별하지 못하도록 암호화하거나 방화벽 등을 이용하여 시스템 또는 데이터의 접근권한을 승인 또는 거부하는데 사용되는 접근통제 기법이 이용된다. 기밀성의 위협요소는 도난, 스니핑(Sniffing), 사회 공학적 사기 등이 이에 해당한다.

가용성(Availability)은 정보나 시스템에 대한 이용과 접근이 적절한 시간에 확실하게 보장되는 상태를 말하는데, 국민의 입장에서 국가나 지방자치단체의 전자정부서비스는 가용성이 가장 중요한 요소 중 하나이다. 가용성의 위협요소는

서비스 거부 공격(DDoS), 자연재해 등이 이에 해당한다.

정보보호의 관리는 관리적, 물리적, 기술적 보호대책으로 규정하고 있는데, 정보보호 관리모형은 [그림 Ⅱ-1]과 같이 제시되어 있다.



[그림 Ⅱ-1] 정보보호 관리 모형

관리적 보호대책은 법, 제도, 교육, 규정 등을 수립하고 수행하여 정보시스템의 신뢰성과 안전성을 확보하기 위한 대책을 말하는데, 정책서 등 자료의 관리, 구성원의 인식 개선을 위한 교육활동 등이 이에 해당한다. 관리적 보호대책은 특히 국가기관이나 지방자치단체에서 정보보호를 효과적으로 보장하기 위하여 다양한 기술적 보호대책과 물리적 보호대책 뿐 아니라 법률, 제도, 정책 및 절차에 대한 관리적 보호대책도 중요하다.

물리적 보호대책은 데이터나 정보시스템이 위치한 정보통신시설을 안전하게 보호하는 활동을 의미하는데, 주요 정보통신시설이나 보호구역에 대해 비인가자의 접근을 차단하기 위한 CCTV, 출입통제를 이용한 관제, 시건장치 등이 이에 속한다.

기술적 보호대책은 정보나 시스템을 보호하기 위한 가장 기본적인 대책으로서 해킹, 악성코드 등을 통한 불법적인 접근을 차단하고 조직 내부 정보자산을 보호하기 위해 이용되는 모든 정보보호 활동을 말한다. 기술 보호대책에는 사용자

인증 및 접근통제, 보안패치 및 업데이트, 시큐어코딩, 보안이 강화된 하드웨어 및 소프트웨어 도입, 암호기술 등의 대책이 이에 속한다.

2) 정보보호서비스의 개요와 특징

정보보호서비스는 정보보호 기술 및 정보보호제품을 활용하여 제공하는 서비스를 칭하며, 정보보호서비스의 특징을 살펴보면 [표 Ⅱ-2]와 같이 네 가지로 제시되어 있다.

[표 Ⅱ-2] 정보보호서비스의 특징

정보보호서비스의 특징
・정보자산에 대한 해킹, 정보유출, 신규 악성코드 감염 등 사이버 위협에 대한 사후 대응중심의 서비스 ・무장애, 성능 Upgrade 등 일반적인 유지관리 서비스 외에 보안 위협에 사전 대비, 대응을 위한 수시 Upgrade 등 보안 조치가 따르는 서비스 ・무결성・기밀성・가용성이 보장되어야 하는 서비스 ・주요정보통신시설 및 사회 기반 시설의 안전과 밀접한 관련이 있는 서비스

3) 정보보호서비스의 종류와 수행내용

정보보호서비스는 보안성 지속서비스, 보안관제, 보안컨설팅, 보안인증(CC 평가인증, 공인인증 등), 보안교육훈련, 물리보안서비스, SI 서비스 등이 이에 포함되어 있다. 이 중 정보보안컨설팅, 보안성 지속서비스, 보안관제서비스의 서비스에 대한 주요 수행내용을 살펴보면 [표 Ⅱ-3]과 같이 규정되어 있다.

[표 Ⅱ-3] 정보보호서비스의 종류별 수행내용(정보보호산업 진흥의 관한 법률)

정보보안컨설팅(제6조)	보안성지속(제7조)	보안관제(제8조)
・주요 정보통신 기반시설 취약점 분석·평가 ・정보보호 관리체계	・보안 업데이트 ・보안정책 관리 ・위험/사고 분석	・보안위협 모니터링 ・사이버 위협 징후 실시간 대응조치 등

정보보안컨설팅(제6조)	보안성지속(제7조)	보안관제(제8조)
(ISMS-P) 인증 · 개인정보 영향평가 · 보안취약점 진단 · 모의해킹 · SW 개발보안 및 보안 강화 컨설팅 등	· 보안성 인증효력 유지 · 보안기술 자문	· 기획·진단·분석·운영서비스 · 기타 수요기관과 수급사업자가 합의한 개별서비스

(1) 정보보안 컨설팅 서비스

정보보안 컨설팅 서비스란 보호해야 할 중요 정보자산을 대상으로 위협요인에 대한 평가, 취약점 분석 및 평가, 보호대책 수립, 정보보호 이행계획 수립, 각종 보안감사, 모의침투 훈련 등 보안 전문가에 의한 보안 전반에 대한 컨설팅 및 지원 서비스를 말한다.

정보보안 컨설팅의 종류는 컨설팅 대상과 목적 등에 따라 주요 정보통신 기반시설 등 정보보호 관련 법률에 의하여 실시하는 컨설팅과 기관 내부의 정보보호 관리체계를 확립하고자 자율적으로 실시하는 컨설팅으로 분류할 수 있다.

한국SW산업협회(2019)가 제시한 정보보호컨설팅의 종류는 [표 Ⅱ-4]와 같다.

[표 Ⅱ-4] 정보보호 컨설팅의 종류

컨설팅 유형	법규	적용대상	목 적
ISO/IEC 27000		기관, 기업, 단체 등	조직의 정보보호관리체계 체계적 확립
ISMS-P	정보통신망법 제47조	정보 통신망 서비스 제공자, 직접 정보통신시설 사업자, 정보통신서비스 부문 일평균 100만명 이상 이용자 또는 100억원 이상 매출액인 사업자	조직의 개인정보 및 정보보호관리체계 체계적 확립

컨설팅 유형	법규	적용대상	목 적
주요 정보통신 기반시설 취약점 분석·평가	정보통신기반 보호법 제9조	주요 정보통신 기반시설	사이버 위협으로부터 주요 정보통신 기반시설을 안정적으로 운용하여 국가의 안전과 국민생활의 안정을 보장
개인정보 영향평가	개인정보보호법 제33조	개인정보처리시스템의 구축 운영 또는 변경하려는 개인정보파일로서 고유식별정보 또는 민감정보 5만명 이상의 처리가 수반되는 개인정보파일, 개인정보파일 연계 시 연계결과 50만명 이상의 개인정보가 포함된 파일, 구축 운영 또는 변경되는 100만명 이상의 개인정보파일	개인정보 처리시스템의 구축·변경하는 경우 개인정보에 미치는 영향을 사전에 조사, 예측, 검토하여 개선방안 도출
취약점 진단 및 모의해킹		국가 및 공공기관, 기업, 단체 등	정보시스템의 보안상 취약점 도출 및 조치
개발보안 컨설팅	전자정부법 제43조제3항	국가 및 공공기관, 기업, 단체 등	SW 개발-설계-구현-운영단계별 보안 약점을 제거 후 사이버 위협 대응
종합정보보호 컨설팅		국가 및 공공기관, 기업, 단체 등	조직의 정보보호관리체계 체계적 확립

정보보안 컨설팅은 다양한 대상과 목적이 존재하여 기관의 정책과 요구사항에 따라 그 세부 유형이 다양하게 존재하기는 하지만, 크게 환경 분석, 현황진단, 위험분석, 대책수립, 구현관리 등 5단계의 방법론을 거치고 있다.

(2) 보안성 지속 서비스

보안성 지속 서비스란 정보보호 솔루션을 이용하여 데이터의 변조·유출·훼손을 예방하기 위한 기술적 서비스이다. 이 중 정보보호 솔루션은 정보보호 제품, 외부 공격 등 위협요인으로부터 보안성 유지를 위한 보안성 지속 서비스, 정보보호 제품의 기능 유지를 위한 일반적 유지관리로 구성된다.

보안성 지속 서비스의 종류는 보안 업데이트, 정보보호정책 관리, 사고 분석 및 위협 분석, 각종 보안성 인증 유지, 보안기술 자문 등이며, 이 들의 주요 서비스 내용을 살펴보면 [표 Ⅱ-5]와 같다.

[표 Ⅱ-5] 보안성 지속서비스의 항목과 주요내용

항목	서비스 내용
보안업데이트	· 룰 패턴 및 시그니처 업데이트 · IT환경 변화에 대한 패치(신규 OS, 표준, 시스템 등)
정보보호정책 관리	· 이용자 환경에 따른 정보보호정책 수립 및 변경
사고분석 및 위협분석	· 사전/사후 침해사고 대응 · 제품군별 위협 분석 보고서 등
각종 보안성 인증 유지	· 보안적합성 검증, CC인증 등 각종 보안성 인증 유지
보안기술자문	· 각종 모의훈련 및 교육훈련 · 보안서비스 Help Desk 운영 · 각종 정보보안감사 지원 등

가. 보안 업데이트

정보보호제품은 지속적이고 지능화되고 있는 공격기법을 시그니처(Signature) 기반으로 변환하여 공격 패턴을 비교하는 방식의 메커니즘을 사용하기 때문에

보안 시그니처(Signature) 업데이트를 지속적으로 관리함으로써 보안성을 향상시킬 수 있다. 새로운 운영체제나 시스템, 프로토콜이나 표준 반영 등 ICT환경 변화에 대한 패치도 보안업데이트에 포함되는 사항이며, 제품의 특성과 공급업체의 관리 정책에 따라 수시 또는 정기로 보안업데이트 시기를 결정할 수 있다.

나. 정보보호정책 관리

정보보호정책 관리는 일반적으로 보안을 강화하거나 완화하는 등의 접근통제를 위한 보안 룰 셋의 변경관리와 납품된 정보보호시스템에 대한 정책 변경관리가 있다. 정보보호정책 변경은 기관이나 기업의 정책이 변경되거나 웹 어플리케이션의 구조나 소스가 변경되었을 경우, 보호 대상 정보시스템의 변화가 발생할 경우 보안정책의 변경이 필요하게 된다.

다. 사고분석 및 위협분석

사고 및 위협분석은 최신 보안위협이나 해킹, 악성코드 등 위협 정보 및 최신 정보보안 기술 동향 정보, 침해사고 분석정보 등을 제공하는 것으로, 제공 시기는 정기 또는 수시 정보 제공 형태로 나눠진다. 수시로 정보 제공하는 경우는 사이버 침해 사고가 발생할 때 발생원인과 대응방안 정보를 제공하는 것이 일반적이며, 침해사고 대응·분석 보고서가 이에 해당된다. 사고 및 위협분석 서비스를 통해 대내·외 서비스의 위협요인과 요소들에 대한 잠재적 취약점 분석과 침투경로 점검, 이용자의 정보시스템에 대한 안전한 보호를 위한 최적의 대응 방안을 제안할 수 있다.

라. 각종 보안성 인증 유지

보안성 인증 유지 서비스는 정보보호제품의 보안성을 보장할 수 있도록 보안성 인증이 필수요건으로 적용되는데, 공통 평가기준(CC : Common Criteria) 인증, 암호검증, 보안적합성 검증 등이 이에 해당된다. 이는 정보보호제품의 최초 개발단계부터 폐기 시까지 모든 주기에 걸쳐 지속적으로 관리되어야 하는 부분이다.

마. 보안기술 자문

보안기술 자문서비스는 수요기관의 침해사고 대응 모의훈련, 조직 구성원 대상

정보보호 교육 지원, 원격 서비스데스크 운영을 통한 문의 대응, 각종 보안감사 지원 등 수요기관이 보안 관련 문제해결을 위해 요청한 경우, 전문 인력의 방문 지원, 전화 또는 온라인 지원 등을 통해 문제를 해결하는 서비스를 말한다.

(3) 보안관제 서비스

보안관제서비스는 사이버 침해를 탐지·분석·대응하는 활동을 말하는데, 기본서비스, 부가서비스 등이 이에 속한다. 한국SW산업협회(2019)가 제시한 보안관제 서비스 유형과 주요 활동을 살펴보면 [표 Ⅱ-6]과 같다.

[표 Ⅱ-6] 보안관제 서비스 유형과 주요 활동

유형		주요활동	비고
기본서비스		· 365일 24시간 실시간 사이버 침해 징후 모니터링·탐지·대응 · 정보시스템 인프라 가용성 모니터링 · 정보보호시스템 Pattern 생성·변경관리	
부가서비스	비상대응서비스	· 사이버위기 경보단계 발령에 따른 CERT 팀 운영 관련 추가 지원 서비스	
	분석서비스	· 초동 분석 결과 기반 정보보호시스템별 보안로그 수집·분석 · 공격자의 정보, 침투시간, 공격기법, 피해여부, 취약점 정보 등 정보자산의 피해규모 파악 · 유형별 대응방안 전략 수립·복구 지원 · 최신 정보보호동향 수집·전파 · 각종 모의훈련 지원	
	진단서비스	· 인프라 취약점 진단 · 웹 취약점 진단	
	운영서비스	· 보안장비 운영·이벤트 및 로그 백업 · 정보통신실 물리적 시설 인프라 관리 · 정보자산의 보안 업데이트·패치 · 정기/예방점검, 정보자산관리, 장애관리	
	기획서비스	· 정보보호시스템 신규 도입·구축 계획 수립	

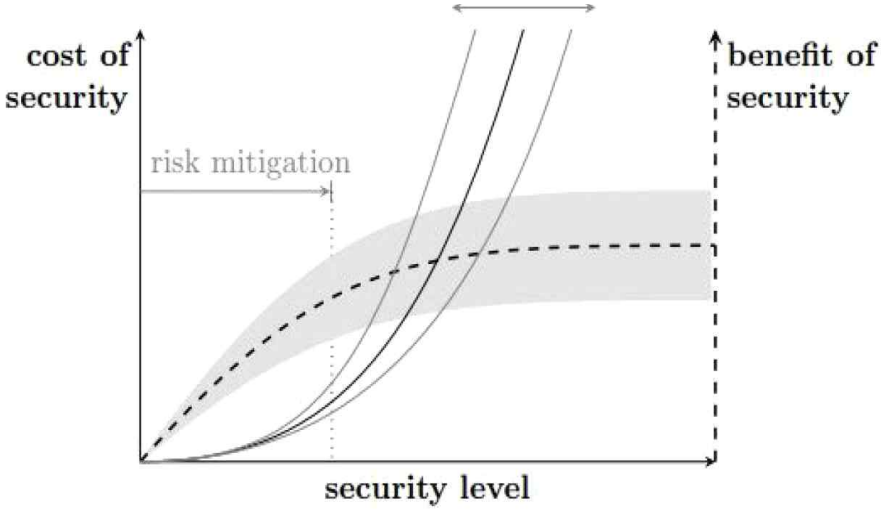
유형		주요활동	비고
		· 관제 영역별 업무의 품질 관리·개선점 도출 · 조직 내부 직원 대상 정보보호교육계획 수립 · 타 부서 정보보호정책 및 서비스 응대	
	개별서비스	· 신규 장비 도입 시 Benchmarking Test · 내부업무 및 고객의 요청에 필요한 시스템 개발 · 시큐어코딩 진단, 악성코드 분석 및 유포 경유지 차단 · 해킹/악성메일 대응 모의훈련·DDoS 모의훈련 등 각종 모의훈련 · 인프라 및 웹해킹 예방 서비스 · 포렌식 분석, 개인정보 노출 및 유출 예방	

2. 정보보호서비스 대가 산정 모델에 대한 이론적 고찰

정보보호서비스 대가에 대한 연구는 비용-편익분석에 따른 대가 산정 연구, SW 중심의 대가 산정에 대한 연구, 보안성 지속서비스 대가 산정, 서비스 수준 성숙도 관점에서의 정보보호서비스 대가 산정에 대한 연구로 구분할 수 있다.

1) 비용-편익분석에 따른 대가 산정

비용-편익분석에 따른 대가 산정에 대한 문헌 연구를 살펴보면, 정보보호 적용로 실현되는 정보보안의 비용과 편익 사이의 관계를 연구하였는데, 위험요인을 완화하기 위한 예방적 노력으로 제공되는 기준 수준의 보안과 그러한 요소들의 연관성을 실증하였다. 때로는 외부의 공격이나 침해를 강력하게 완화하기 위해 다수 조직이 적용하려는 것보다 많은 비용이 들 수 있다. 비용-편익분석을 통해 보안 수익율(ROSI)을 이용해 [그림 Ⅱ-2]와 같이 편익을 비용보다 적게 하고 비용으로 나누어서 백분율로 환산하는 형태를 제안하였다.



[그림 Ⅱ-2] 정보보안에서의 비용/편익 관계(Böhme)

2) 소프트웨어 중심의 대가 산정

소프트웨어 중심의 대가에 대한 문헌 연구을 살펴보면, 정보보호제품과 유지관리 활동별로 적용하는 유지관리 대가 기준 방식으로 활동별 유지관리 소요횟수, 해결 소요 시간, 소요인력 등을 학습곡선을 적용하여 제품·활동별 유지관리 대가 비용을 산정하고, 보정계수를 적용하여 유지관리 대가를 산정하는 방식을 도출하는 연구가 이루어졌다. 또 다른 연구는 일반 소프트웨어와 정보보호 소프트웨어와의 차별성을 두면서, 보안 소프트웨어에는 보안정책 지원, 시그니처 및 패턴업데이트, 공통평가기준(CC) 인증 등에 비용이 수반되는 특성을 제시하였다. 특히, 보안제품군별 보안 업데이트의 비용 산정기준을 소프트웨어사업 대가 기준에 반영하였다. 또한, 2010년 “정보보안 SW 유지보수 대가 기준 연구”를 통해 국내·외 보안 소프트웨어산업 및 유지관리체계 현황을 조사 비교하여 국내의 요율체계의 문제점을 도출하였고, 이를 근거로 정보보호서비스의 범위 확대, 정보보호제품과 정보보호서비스 활동단위별 유지관리 대가 기준 방식으로 개선하였다. 특히, 소프트웨어 개발 보안서비스와 같은 경우 보정계수를 적용하여 유지관리 대가를 산정하는 방식으로 제안하였다.

3) 보안성 지속서비스 대가 산정

보안성 지속서비스 대가 산정에 관한 문헌연구를 살펴보면, 정보보호제품에 대한 보안성 지속을 위해 수행되는 서비스 현황을 분석하고, 그 제품별 특성을 고려하여 서비스를 다시 보안업데이트, 보안정책, 위협분석, 인증유지, 기술자문 등 보안성 지속 서비스를 분류하고 [표 Ⅱ-7]과 같이 서비스 대가를 요율방식과 정액제를 산정하는 형태를 제안하였다.

[표 Ⅱ-7] 보안성 지속 서비스 대가 산정방식

구 분	산정방식
요율	장비도입가액 × 요율
정액제	라이선스 비용(보안 지속성 서비스 비용 포함)

한국정보보호산업협회 등(2018)은 매년 개정되고 있는 “소프트웨어 사업 대가 산정 가이드”를 통해 보안성 지속 서비스 대상 제품에 대한 보안성 지속 서비스 요율 책정 기준을 서비스 활동주기를 기준으로 하여 보안 서비스별 포인트(SSP : Security Services Point) 측정 방식을 [표 Ⅱ-8]과 같이 제안하였다.

[표 Ⅱ-8] 보안 서비스별 포인트(SSP : Security Services Point) 측정 방식

구 분	산정방식	
보안업데이트	월 1회 이상 또는 년 12회 이상	30
	분기별 1회 이상 또는 년 4회 이상	25
	반기별 1회 이상 또는 년 2회 이상	20
보안정책관리	월 1회 이상 또는 년 12회 이상	20
	분기별 1회 이상 또는 년 4회 이상	15
	반기별 1회 이상 또는 년 2회 이상	10
위험/사고분석	월 1회 이상 또는 년 12회 이상 사고대응보고 및 위협분석 보고	20
	분기별 1회 이상 또는 년 4회 이상 사고대응보고 및 위협분석 보고	15

구 분	산정방식	
	반기별 1회 이상 또는 년 2회 이상 사고대응보고 및 위협분석 보고	10
보안성 인증효력 유지	공통 평가기준(CC) 인증 등 보안성 인증 효력 유지	20
	기타 보안성 인증 유지	10
보안기술자문	년 2회 이상 모의훈련 또는 기술 자문 20시간 이상	10
	년 1회 이상 모의훈련 또는 기술 자문 10시간 이상	5
계		SSP*

[표 Ⅱ-8]의 보안성 지속 서비스 대가의 산정방식을 근거로 제품별로 보안성 지속 서비스의 항목별 배점을 합산한 보안 서비스별 포인트(SSP)를 [표 Ⅱ-9]와 같이 적용한 요율을 적용할 수 있도록 제시하였다.

[표 Ⅱ-9] 보안성 지속 서비스 대가 산정방식(SSP 방식)

산정방식
보안성 지속 서비스 요율(%) = 10 × (SSP / 100)

4) SCS성과평가체계 모델의 대가 산정

보안서비스 수준 성숙도 기반의 서비스 대가 산정에 대한 문헌 연구를 살펴보면, 보안성 지속서비스 대가 산정방식 중 요율방식과 정보보호 서비스 수준 협약(S-SLA : Security Service Level Agreement)을 보안성 지속서비스 대가 산정방식 중 요율방식을 보안장비 유지관리비에 적용한 국내 기관의 사례를 분석하여 보안성 지속서비스 비용 지출에 대한 편익분석 측면에서 편익성이 높은 것으로 나타났다.

정보보호서비스 활동에 대한 평가를 보다 객관적으로 하기 위해 국가표준기술원(NIST)의 사이버 보안 프레임워크(CSF : Cyber security Framework)와 보안 서비스 수준 협약지표를 결합하여 보안 연속성 서비스(SCS : Security Continuity Service) 성과평가체계 모델을 [표 Ⅱ-10]과 같이 제안하였다. NIST

의 CSF는 2014년 미국 사이버보안 강화법 제정 시행에 따라 미국의 NIST가 개발한 사이버보안 프레임워크이다. NIST 사이버 보안 프레임워크(CSF)는 기업이나 조직에서 사이버 보안 운영을 계획, 관리 및 지속적으로 개선하기 위해 제작한 프레임워크이다. 보안 연속성 서비스(SCS) 성과평가체계 모델은 정보보호 활동 및 위험 관리와 관련된 회계요소를 품질 비용모델에 연결하는 데 여전히 유용할 수 있다.

[표 Ⅱ-10] 보안 연속성 서비스(SCS) 성과평가체계 모델

서비스 항목		기준요율 (%)	S-SLA		가중치	SCS Rate (%)
			목표	최소		
Identify	자산 식별 및 중요도 평가	0.3	95	93	0.4~1.0	기준요율 × 가중치
	보안 취약점 확인 및 조치	0.2	95	93	0.4~1.0	
	보안 절차 준수	0.2	95	93	0.4~1.0	
	중요인원 유지	0.1	95	93	0.4~1.0	
	보안 업데이트, 보안 패치 업데이트	0.5	95	93	0.4~1.0	
	위험분석평가	0.5	95	93	0.4~1.0	
Protect	정보보호 대책 및 이행계획 수립	0.4	95	93	0.4~1.0	
	주요 IT 인프라 모니터링 및 가용성 확인	0.3	95	93	0.4~1.0	
	해킹 시뮬레이션 교육	0.4	95	93	0.4~1.0	
	보안감사지원	0.3	95	93	0.4~1.0	
	기술 조언	0.1	95	93	0.4~1.0	
	예방점검, 정기점검	0.3	95	93	0.4~1.0	
	장애 및 오류, 페일오버 시간 및 복구 시간	0.3	95	93	0.4~1.0	
Respond	실시간 보안 위협 모니터링 및 탐지 및 초기 분석	0.4	95	93	0.4~1.0	
	예방점검, 정기점검	0.4	95	93	0.4~1.0	
	데이터 유출, 관리자 권한 침해 분석 등	0.5	95	93	0.4~1.0	
Detect	사이버 위협 증상의 실시간 대응 및 보고	0.5	95	93	0.4~1.0	
	초기 분석 결과를 토대로 보	0.5	95	93	0.4~1.0	

서비스 항목		기준요율 (%)	S-SLA		가중치	SCS Rate (%)
			목표	최소		
	안 장비 상세 데이터 수집 및 분석					
	악성코드분석 및 유통예방서비스	0.5	95	93	0.4~1.0	
Recover	다양한 유형에 대한 복구 지원 및 대응책 및 전략	0.5	95	93	0.4~1.0	
	백업 장치 이벤트 및 로그 분석	0.5	95	93	0.4~1.0	
	재해복구테스트	0.3	95	93	0.4~1.0	
SCS Rate(%)		8			0.4~1.0	

[표 Ⅱ-11]은 SCS 성과평가체계 모델을 적용한 요율방식의 정보보호서비스 대가 산정방식은 제품별로 세부항목별 기준요율과 가중치를 곱한 후 도출된 최종 요율을 모두 합산하면 정보보호서비스 대가 요율(SCS Rate)이 결정된다. 제품별 정보보호서비스 대가 산정방식은 제품공급가격에 SCS Rate를 곱하여 산정하는 방식이다.

[표 Ⅱ-11] 항목별 가중치 산출식 및 적용기준

구분	산식			
산출방식	$PR = \sum\left(\frac{N}{T}\right) \times 100\%$	N : 수행률 T : 목표치, PR : 기준요율		
지표별 가중치	SLA별 가중치 값			
	100~95%	~93%	~90%	85%~
	1.0	0.8	0.6	0.4
서비스 대가	산출식(요율제)			
	Purchase price × SCS Rate(%)			

3. 서비스 품질 측정 모형에 대한 이론적 고찰

1) 서비스의 정의와 특징

서비스(Service)는 통상적으로 생산된 재화를 운반하거나 생산과 소비에 필요한 인력을 제공하는 일라고 정의할 수 있는데, 서비스는 다양성으로 인해 연구자들마다 명확한 개념의 일치와 합의를 끌어내지 못하고 있다. 미국마케팅협회는 서비스를 “재화를 판매하기 위해 제공 또는 준비와 관련된 모든 활동, 만족, 편익”이라고 정의하였고, Gronroos(1978)은 “서비스를 일반적으로 제공하는 기관과 기업에 의해 제공받는 자와 재화 간의 상호작용에서 발생하는 일련의 활동”으로 정의하였다.

서비스의 특성은 크게 무형성, 동시성, 이질성, 소멸성으로 구분되어 질 수 있다. 첫 번째 특성인 무형성은 직접 만지거나 볼 수 없다는 객관적 의미와 이러한 의미 때문에 서비스가 어떠한지를 알기 어렵다는 주관적 의미를 지니고 있다. 무형성은 저장할 수도, 특허를 낼 수도, 가격을 책정할 수도 없는 모호성을 지니고 있으며, 법률, 의료, 강의 등이 이에 해당된다.

두 번째 특성인 동시성은 비분리성이라고도 하며, 생산과 소비의 분리가 되지 않고 생산과 소비가 동시에 일어나는 특성을 지닌다. 동시성은 서비스제공-고객 간 서로 영향을 미치고, 서비스 제공자가 서비스 결과에 커다란 영향을 미치며, 대량으로 생산이 어렵다.

세 번째 특성인 이질성은 서비스가 고객에게 전달하는 과정에서 상황에 따라 변수가 발생하기 때문에 서비스 제공자의 전문성과 숙련도, 고객의 성향과 환경에 따라 서비스가 다를 수 있다. 이질성은 직원의 행위에 따라 서비스 제공과 고객 만족에 영향을 미치고, 서비스 제공과정에서 예측 불가능한 변수가 서비스 품질에 영향을 미친다.

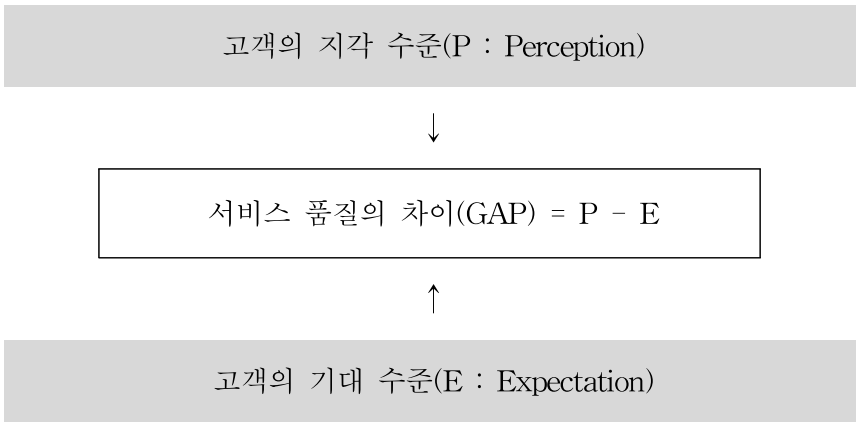
네 번째 특성인 소멸성은 제공하지 않은 서비스는 소멸된다. 즉, 재화는 존재하나 서비스는 무형이기 때문에 사라진다는 의미이다. 소멸성은 제공한 서비스는 1회성이기 때문에 그에 따른 편익도 동시에 사라진다는 것이며, 수요와 공급을

맞출 수 없고, 서비스의 반품도 불가능하다.

2) 서비스 품질의 GAP 측정 모형

서비스 품질은 서비스의 질에 대한 고객의 판단을 의미하는데, 서비스 품질 차이(GAP)는 서비스 제공자가 제공하고자 하는 서비스와 고객이 받고자 하는 서비스의 정도의 차이에서 발생한다.

서비스 품질 갭 모형은 [그림 Ⅱ-3]과 같이 서비스를 제공받는 고객이 원하는 서비스 기대와 서비스 지각 간의 갭(Gap) 차이를 의미한다.



[그림 Ⅱ-3] 서비스 품질의 차이(GAP)

서비스 품질 측정방법은 SERVQUAL, SERVPERF, E-S-QUAL 등이 있다. 이 중 Parasuraman 등(1988)이 제안한 SERVQUAL 연구모형을 가장 많이 사용되고 있다.

Parasuraman 등(1988)에 의하면 서비스 품질은 물리적 재화의 품질보다 평가하기 어렵기 때문에, 서비스 품질의 차이뿐만 아니라 서비스 전달과정에 대한 평가도 포함되어야 한다고 주장하였다.

SERVQUAL 연구모형은 1988년에 처음 개발되었는데, 초기 측정 모형의 척도인 서비스 품질 차원을[표 Ⅱ-12]와 같이 총 10개로 구분하여 제시하였다.

[표 Ⅱ-12] 서비스 품질 차원의 구분

차원	내용
신뢰성	약속한 서비스를 정확하고 일관되게 제공
접근성	서비스 접근의 용이성, 편리성
의사소통	고객의 이해도 높은 언어 사용
숙련성	제공 서비스에 대한 기술과 지식 습득
친절	서비스 직원들의 공손함, 존중, 배려, 친근함
신용	신용, 명성과 이미지
반응성	언제든지 서비스를 제공할 준비가 되어 있음
안전	비밀 유지, 물리적 안전
유형성	서비스와 관련된 직원의 품위, 장비, 시설 등 물리적인 측면
고객의 이해 및 인지	고객의 요구 습득 및 인식

이후 초기 SERVQUAL 연구모형의 척도인 서비스 품질 차원 10개의 항목에 대해 신뢰성 분석과 요인 분석을 통해 부적절한 측정항목을 통합 및 제거하여 신뢰성, 유형성, 확신성, 반응성, 공감성 등 5개 차원으로 [표 Ⅱ-13]과 같이 재구성하여 발전시켰다. 수정된 SERVQUAL 연구모형은 서비스 품질 측정 도루로 현재까지도 일반적으로 이용되고 있다.

[표 Ⅱ-13] 수정된 서비스 품질 차원의 구분

차원	내용
신뢰성	약속한 서비스를 믿음직스럽고 정확하게 제공하는 능력
유형성	물리적인 시설 및 장비 능력, 종업원의 외모, 통신 장비의 이해와 활용의 용이성
확신성	신용과 자신감 고취

차원	내용
반응성	신속한 서비스를 제공하여 고객들을 도와 줌
공감성	고객들에게 개별적인 관심을 갖고 서비스를 제공

SERVQUAL 연구모형을 이용한 서비스 품질 측정에 관한 문헌 연구를 살펴보면, 첫 번째 연구는 SERVQUAL 연구 모형과 SERVPERF 연구 모형을 이용하여 ISMS 인증제도 성과측정 모형을 개발하여 성과측정을 실증하였다.

또 다른 연구는 SERVQUAL 연구모형을 이용하여 공공서비스의 관점에서 국가 개인정보보호 정책을 접근하여 공공서비스의 품질을 정책의 성과로서 분석하였다.

[표 Ⅱ-14] SERVQUAL 연구모형을 이용한 선행연구

연구자	연구내용
우정훈(2015)	SERVQUAL을 활용한 ISMS 성과측정 모형 개발에 대한 실증연구
경지훈(2016)	IT 보안 서비스 품질의 측정 방법에 관한 연구

4. 정보보호성과에 대한 이론적 고찰

정보보호성과란 조직이 정보보호 활동을 통해 보안사고의 예방, 정보자산의 훼손 및 손실 방지와 같은 목적으로부터 대외 이미지 및 신뢰도 증대, 고객 만족 등과 같은 능동적인 목적이 있다. 정보보호 활동을 통해 조직 구성원들의 보안 역량을 강화시켜 업무 효율성과 서비스 품질의 향상을 유도하는 효과도 있을 수 있다. 정보보호성과에 관한 문헌 연구를 살펴보면, 정보보호 활동의 질적인 문제를 연구하기 위해 보안수익률(ROSI ; Return On Security Investment) 대 위험의 관점에서 정보보호제품 및 정보보호서비스의 성과를 측정하려는 연구와 정보자산

보호성과와 경쟁우위 확보, 이미지 개선 등의 조직의 본질적인 성과를 입증하고자 하는 경우, 정보보호성과에 미치는 영향에 대한 실증검증으로 살펴볼 수 있다.

1) 보안수익률(ROSI) 관점에 관한 문헌 연구

보안수익률(ROSI) 관점에서의 정보보호성과에 관한 선행연구를 살펴보면, 첫 번째 선행연구에서는 재무성과 도출을 고려하여 보안사고 방지를 위한 관리적 통제와 기술적 통제를 이위한 보안솔루션의 이용 효과를 실증 검증함으로써 보안수익률(ROSI) 대 위험의 관점에서의 성과로 정의하였다.

두 번째 선행연구에서는 위험 분석활동의 효과를 평가하기 위하여, 공급자와 수요자, 기업, 고객, 기타 관련자에 대한 사회, 경제, 기술, 환경, 경제, 심리적 측면의 성과를 확률 척도를 이용하여 측정하도록 함으로써 다양한 계층의 이해 당사자와 분야측면에서의 정보보호 성과를 정의하였다.

세 번째 선행연구에서는 정보보호사고의 영향을 감쇄시키기 위하여 위험분석과 정보보호 사고에 따른 영향 분석을 통해 정보보호의 요구사항을 도출하여야 한다고 제시하여 정보보호 사고로부터 영향 감쇄시키는 활동을 위험 분석활동의 목적으로 정의하였다.

2) 정보보호 성과에 관한 문헌 연구

정보보호성과에 관한 선행연구를 살펴보면, 첫 번째 선행연구에서는 기관이나 조직에서 도입, 운용하고 있는 ISMS의 관리과정을 PDCA 단계로 분류하고, 단계별 관리과정에 대한 정보보호 성과에 미치는 영향에 대하여 분석하였는데, 정보보호 관리과정 중 계획-실행-점검단계에서 조직의 정보보호성과에 영향을 미치는 것으로 밝혀졌다.

두 번째 선행연구는 조직의 정보보호 이행 정도가 정보보호성과에 어떠한 영향을 미치는지를 확인하고자 하였다.

세 번째 선행연구는 대학조직의 정보 유통과정에서 프라이버시 염려가 개인정보보호의 통제활동과 개인정보보호 성과에 미치는 영향을 분석하고자 하였다.

네 번째 선행연구에서는 국내의 개인정보보호 적용의 성과측정에 대해 정성적

및 정량적 성과 측정이 가능한 개인정보보호 적용모델을 개발하여 성과에 미치는 영향을 분석하고자 하였다.

마지막 선행연구에서는 급변하는 경영환경에서 중소기업 조직구성원의 의식전환이 있어야 조직의 정보보호를 원활히 수행할 수 있기 때문에 구성원들의 개인적 차원의 인식과 행동이 조직의 정보보호성과에 미치는 영향을 실증적으로 검증하고자 하였다.

5. 지방자치단체의 정보보호서비스 대가 산정 모델 적용 사례 분석

1) 기관의 정보보호서비스 대가 산정 모델 설계

현재 정보보호 서비스를 도입 적용하고 있는 국내 유일한 기관인 제주지역 S기관의 적용사례를 통해서 정보보호 서비스가 어떠한 효과를 미치는지 검증하고자 한다. 이 기관은 정보보호서비스 수준 관리(S-SLM : Security Service Level Management)를 기반으로 하여 2017년부터 정보보호제품과 일부 정보시스템에 대한 정보보호 서비스 대가를 적용하고 있다.

(1) 기관의 정보보호서비스 유형

기관의 정보보호서비스 유형은 기획, 진단/위험관리, 분석, 운영, 대응, 지원 등 6개 분야의 서비스로 구성되어 있으며, 서비스별 주요활동은 [표 Ⅱ-15]와 같다.

[표 Ⅱ-15] 정보보호서비스 유형

서비스 영역	주요 활동
정보보호 관리체계 서비스	· 정보보호관리체계(ISMS-P) 구축 영역별 기획 · 정보보호서비스 영역별 품질 관리 및 개선 도출 · S-PDCA별 보안관리대책 수립 기획 등
위험분석 관리서비스	· 정보자산 식별 및 중요도 평가 · 서버, 보안장비, DB, 네트워크, IoT 등 인프라 취약점 진단

서비스 영역	주요 활동
	· 웹 취약점 및 시큐어코딩 진단 · 보안취약점 진단결과에 따른 위험분석평가 및 보호대책 수립
위협분석 관리서비스	· 외부로부터 침해 탐지 로그/패킷 수집 · 초동 분석결과를 기초로 한 보안로그 수집·분석 · 공격자의 정보, 침투시간, 공격방법, 취약점정보, 정보자산의 피해여부 등 피해규모 파악, 복구지원 · 유형별 대응 방안 전략 수립
보안운영 서비스	· 정보보호시스템 운영, 장비 이벤트 및 로그 백업 · 서버, 보안장비, DB, 네트워크, IoT 등 IT 인프라의 정기/긴급 보안패치 및 릴리즈 · 정기점검 및 장애처리, 자산 관리 업무 · 주요 IT 인프라 가용성·무결성 체크 · 정보보호시스템 패턴 생성 및 변경관리 · 정보보호 교육 및 기술동향 자문 · 정보보호시스템 운영 및 가용성, 보안동향 등 시스템 분석보고서 작성/관리
보안대응 서비스	· 사이버 침해 및 보안위협 모니터링/탐지·대응조치·분석 · 악성코드 분석, 악성코드 유포지 차단 서비스 · 해킹/악성메일 대응 모의훈련 및 복구테스트 서비스 등
보안지원 서비스	· PC 등 Endpoint 장비에 대한 보안진단 및 조치 지원 · 보안 관련 Help-desk 운영 및 응답지원 등

(2) 정보호서비스 수준 협약

서비스 수준 협약(SLA : Service Level Agreement)은 공급자가 IT 서비스를 제공함에 있어 소비자와 당사자 간에 서비스에 대해 목표와 측정지표 등을 정한 협약서이다. 일반적으로 포함되는 측정지표는 시스템 가동률, 장애 복구율, 서비스 응답률, 서비스 완료시간 등이다.

이 기관은 2017년부터 제품군별 유지보수와 정보보호 지속 서비스를 S-SLA(S-SLA : Security Service Level Agreement) 중심으로 측정하고 이를 바탕으로 적정한 대가를 적용하고 있다. 이 기관의 정보보호제품과 일부 정보시스

템에 대한 정보보호 서비스 대가 측정기준을 [표 Ⅱ-16]과 같이 적용하고 있다.

[표 Ⅱ-16] 정보호서비스 수준 협약(S-SLA) 기준

항목	기준요율 (%)	SLA	
		목표	최소
보안업데이트 실적	0.5	99	95
보안패치업데이트 실적	0.5	99	95
자산식별 및 중요도 평가 실적	0.2	99	95
보안취약점 진단 및 조치실적	0.8	99	95
위험분석평가 실적	0.5	99	95
자산 가용성 모니터링 실적	0.5	99	95
정기점검/예방점검 실적	0.3	99	95
장애처리 실적	0.5	99	95
침해 탐지 로그/패킷 분석 실적	0.2	99	95
침해 및 보안위협 모니터링 실적	0.5	99	95
보안위협 징후 초동 대응 및 보고 실적	0.5	99	95
보안장비 룰셋 정책 변경관리 실적	0.5	99	95
정보보호교육 실적	0.3	99	95
해킹메일 대응 모의훈련 실적	0.5	99	95
데이터 복구테스트 실적	0.5	99	95
Endpoint 보안 진단 지원 실적	0.5	99	95
보안 help-desk 운영 및 응대지원 실적	0.2	97	92
기술자문 실적	0.3	97	92
각종 보안관련 보고서 작성 및 보고 실적	0.2	97	92
계(적용요율)	8		

세부 항목별로 측정기준은 수행주기를 주, 월, 분기, 반기, 연간별로 세분화하였고, S-SLA 기준을 목표와 최소치를 정하였다.

[표 Ⅱ-17] 세부항목별로 측정기준

평가항목	수행주기					
	주	월	분기	반기	년	수시
보안업데이트 실적			○			
보안패치업데이트 실적			○			
자산식별 및 중요도 평가 실적			○			
보안취약점 진단 및 조치실적			○			
위험분석평가 실적			○			
자산 가용성 모니터링 실적		○				
정기점검/예방점검 실적		○				
장애처리 실적						○
침해 탐지 로그/패킷 분석 실적	○					
침해 및 보안위협 모니터링 실적	○					
보안위협 징후 초동 대응 및 보고 실적	○					
보안장비 룰셋 정책 변경관리 실적		○				
정보보호교육 실적				○		
해킹메일 대응 모의훈련 실적					○	
데이터 복구테스트 실적					○	
Endpoint 보안 진단 지원 실적		○				
보안 help-desk 운영 및 응대지원 실적						○
기술자문 실적					○	
각종 보안관련 보고서 작성 및 보고 실적		○				

(3) S-SLA 기반의 대가 산정 방법

기관의 S-SLA 측정 평가를 월단위로 실시하였으며, [표 Ⅲ-4]과 같이 S-SLA의 목표수준(TL) 대비 해당 월의 측정치(M)율을 계산한 후 가중치(R)를 적용하였다. 여기서 나온 S-SLA 측정 평가결과에 목표 달성도에 따른 부여된 가중치(V) 값으로 계산하여 제품별 정보보호 서비스 대가요율을 산정하였다.

<table>
<tr><td rowspan="2">S-SLA evaluation result formula</td><td>Div.</td><td colspan="3">Method</td></tr>
<tr><td>SLA results (SL)</td><td colspan="3">(M / TL × 100) × R</td></tr>
<tr><td colspan="5">↓</td></tr>
<tr><td rowspan="2">S-SLA Objective Attainment Criteria</td><td rowspan="2">Result (V)</td><td>Above the target level</td><td>Minimum level and above</td><td>Minimal criterion attainment failure</td></tr>
<tr><td>1.0</td><td>0.8</td><td>0.5</td></tr>
<tr><td colspan="5">↓</td></tr>
<tr><td rowspan="2">Security Continuity Service Costs</td><td colspan="4">Method</td></tr>
<tr><td colspan="4">SL × V</td></tr>
</table>

[그림 Ⅲ-1] S-SLA 기반의 대가 산정방법

2) 적용 효과와 시사점

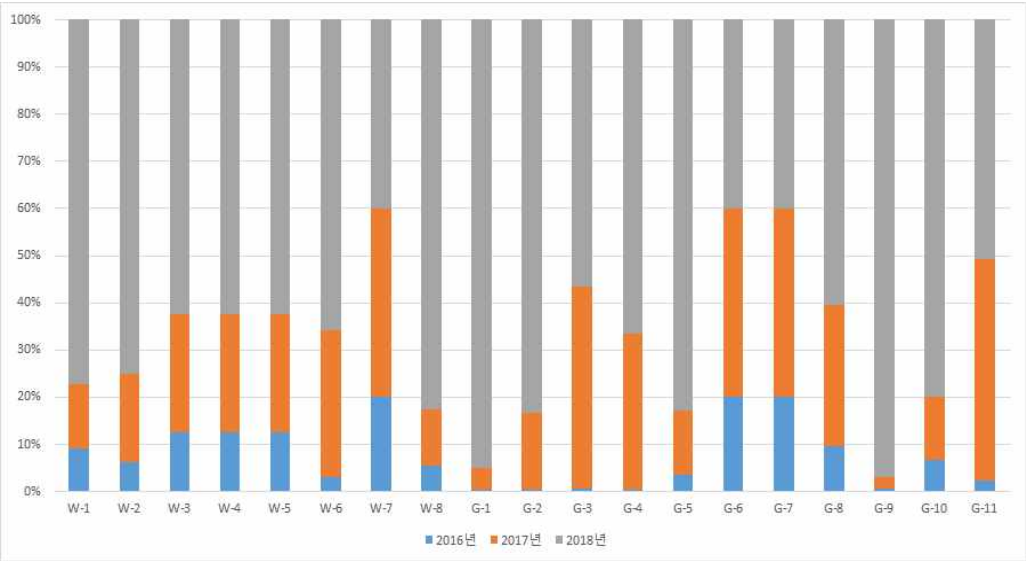
정보보호 서비스 대가 적용의 효과를 전체적으로 평가하는 것은 많은 어려움이 따른다. 특히, 소프트웨어의 일반 유지보수 범위와 소프트웨어 성격이 강한 정보보호 서비스의 범위가 중복되는 부분으로 인해 기관에서는 이를 최대한 구분지어 요율을 적용하고 있다. 도입 효과를 분석하기 위해 정보보호서비스 대가 도입하기 전인 2016년도의 유지관리 완료보고서와 도입을 시작한 2017년, 2018년도의 유지관리 완료보고서를 참고하여 연간 보안업데이트, 보안 리스크 분석, 침해대응 처리, 모의훈련, 기술자문 건수 등을 기준으로 분석한 결과 도입 이전보다 도입 후의 효과가 [표 Ⅱ-18]과 [그림 Ⅲ-2]와 같이 나타났다.

[표 Ⅱ-18] 수행요소별 도입 전·후 비교(단위 : 건수)[1)]

항목	변수	2016년	2017년	2018년
보안업데이트 실적*	W-1	2	3	17
보안패치업데이트 실적*	W-2	1	3	12
자산식별 및 중요도 평가 실적*	W-3	1	2	5
보안취약점 진단 및 조치실적*	W-4	1	2	5
위험분석평가 실적*	W-5	1	2	5

1) 서귀포시 2016~2018년 정보보호시스템 유지관리 완료보고서(통계) 자료 재구성하였음.(* : WAF 1대 예시, ** : 공통)

항목	변수	2016년	2017년	2018년
자산 가용성 모니터링 실적*	W-6	12	118	251
정기점검/예방점검 실적*	W-7	12	24	24
장애처리 실적*	W-8	12	26	181
침해 탐지 로그/패킷 분석 실적**	G-1	1	12	251
보안장비 룰셋 정책 변경관리 실적**	G-2	1	118	237
침해 및 보안위협 모니터링 실적**	G-3	1	49	251
보안위협 징후 초동 대응 및 보고 실적**	G-4	1	66	87
정보보호교육 실적**	G-5	1	4	24
해킹메일 대응 모의훈련 실적**	G-6	1	2	2
데이터 복구테스트 실적**	G-7	1	2	2
Endpoint 보안 진단 지원 실적**	G-8	38	118	238
보안 help-desk 운영 및 응대지원 실적**	G-9	1	5	189
기술자문 실적**	G-10	1	2	12
각종 보안관련 보고서 작성 및 보고 실적**	G-11	12	231	251



[그림 Ⅲ-2] 도입전과 후 효과 비교

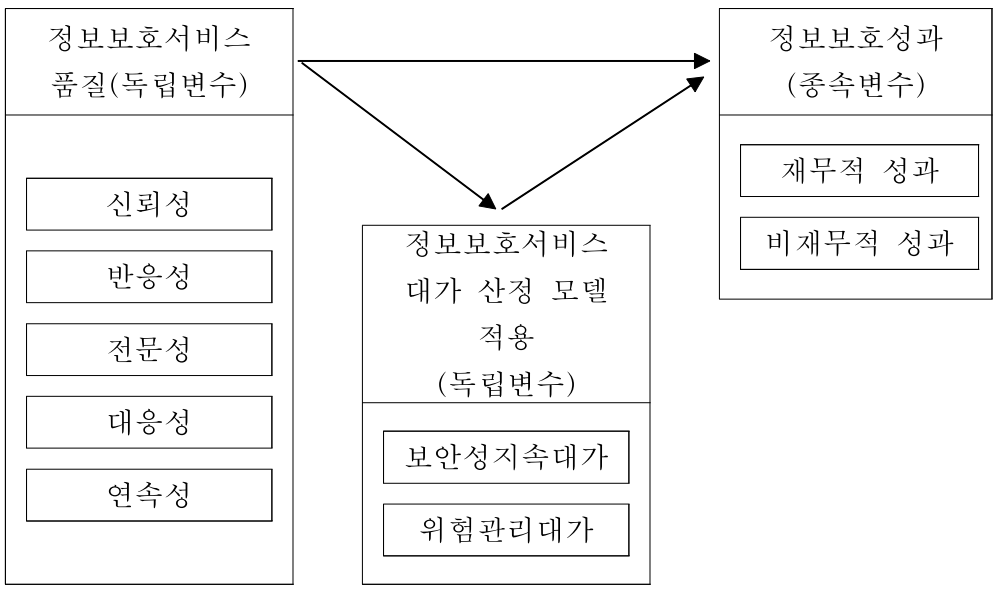
이 기관의 사례 분석을 한 결과, S-SLA 기반의 정보보호서비스 대가 산정의 효과는 비용-효용분석 측면에서 효용성이 높은 것으로 나타났다. 하지만, 기관의 정보보호담당 공무원과 면담방식의 인터뷰를 진행한 결과, 정보보호서비스와 이에 따른 대가 지급이 어떠한 영향을 미치는지 내부 구성원들과 프로젝트를 수행하고 있는 기업들에 대해 의견수렴을 통해 성과를 파악할 필요가 있다고 하였다. 따라서 본 연구에서는 도입기관의 정보보호와 정보화업무 담당 공무원과 이와 관련된 프로젝트를 수행하고 있는 기업을 대상으로 정보보호서비스와 정보보호서비스 대가 산정 모델 적용이 조직의 정보보호성과에 어떠한 영향을 미치는지 실증을 하고자 한다.

Ⅲ. 정보보호성과에 미치는 영향 실증분석

1. 연구 설계

1) 연구 모형

본 연구의 기본적인 틀은 정보보호 수준 향상을 위해 도입된 정보보호서비스 대가 산정 모델과 정보보호성과 간의 관계를 검증하는 모형이다. 정보보호서비스 대가 산정 모델에 대한 적용의 정도에 따라 정보보호성과에 차이가 있는지, 정보보호서비스 대가 산정 모델이 적용된 각각의 정보보호서비스 품질에 대해 신뢰성, 반응성, 전문성, 대응성, 연속성에도 영향을 미치는지와, 정보보호서비스 대가 산정 모델 적용이 정보보호성과에 영향을 미치는지에 대해 알아보기 위하여 [그림 Ⅲ-1]과 같은 연구 모형을 설정하였다.



[그림 Ⅲ-1] 연구모형

정보보호 수준 향상을 위해 도입된 정보보호서비스 품질에 대해 집중적인 적용를 한다는 것은 지방자치단체의 전사적인 정보보호 관리체계 과정에서 서비스 품질 지향성을 추구하는 것으로서, 이러한 노력은 기관의 지향적인 정보보호 수준 향상 문화의 조성을 촉진할 것이다. 정보보호서비스 품질을 향상시키기 위해 제공된 서비스에 대한 적정한 보상에 대한 적용를 효과적으로 하는 지방자치단체에서는 큰 정보보호성과의 개선을 이룰 수 있을 것이다. 따라서 본 연구 모형은 지방자치단체의 정보보호서비스 품질, 정보보호서비스 대가 산정 모델, 그리고 각각의 변수가 종속변수인 정보보호성과에 미치는 인과관계를 고려하였다. 본 연구모형은 체계적이고 안정적인 전자정부 서비스를 제공하고자 하는 지방자치단체에게 중요한 시사점을 제공할 수 있을 것이다.

2) 연구 가설

지방자치단체의 정보보호서비스 품질에 대한 대가 모델이 기관의 정보보호성과에 미치는 영향에 대한 관계를 분석하기 위해 [그림 Ⅲ-1]과 같은 연구 모형에 따라 연구가설을 설정하고 이를 검증하고자 한다.

(1) 정보보호서비스 품질과 정보보호성과 간의 관계

보안 사고를 사전에 막기 위하여 수행하는 정보보안 기획-진단-분석-운영-대응 단계별 정보보호서비스의 품질을 향상하기 위해 적용하거나 관련 프로젝트를 실시하는 기관은 내부 직원과 고객의 신뢰를 얻을 수 있을 것으로 본다.

첫 번째 주요 가설로 정보보호서비스 품질이 정보보호성과에 긍정적인 영향을 미칠 것으로 가정하고 검증해보고자 한다.

가설 1. 정보보호서비스 품질은 정보보호성과에 양(+)의 영향을 미칠 것이다.
1-1. 신뢰성은 정보보호성과에 양(+)의 영향을 미칠 것이다.
1-2. 반응성은 정보보호성과에 양(+)의 영향을 미칠 것이다.
1-3. 전문성은 정보보호성과에 양(+)의 영향을 미칠 것이다.
1-4. 대응성은 정보보호성과에 양(+)의 영향을 미칠 것이다.
1-5. 연속성은 정보보호성과에 양(+)의 영향을 미칠 것이다.

(2) 정보보호서비스 대가 산정 모델 적용와 정보보호서비스 품질 간의 관계

정보보호서비스에 대해 적정한 보상을 위하여 마련된 정보보호서비스 대가 산정 모델 적용이 정보보호서비스 품질에 얼마나 기여하고, 지방자치단체의 정보보호성과에 어떠한 영향을 미치는가를 분석하는 것은 중요하다. 정보보호서비스 대가 산정 모델 적용에 대해 얼마나 적용할 것인지의 문제 접근보다 효율적이고 전략적으로 보상이 가능한 대가 모델을 활용하는 것이 최상의 정보보호서비스 품질을 결정할 수 있을 것이다.

정보보호서비스 대가 산정 모델의 적용를 적절하게 한다면, 이를 통해 직접적으로 보안사고와 장애에 대한 대응시간 단축, 신속한 조치 등 서비스 품질이 향상되고, 안정적인 전자정부 서비스 제공에 대한 고객 만족도 향상을 시킬 수 있으며, 궁극적으로 기관의 신뢰도 향상을 통해 정보보호성과가 증대되는 관계가 형성될 것이다.

두 번째 주요 가설로 정보보호서비스 대가 산정 모델에 대한 적용의 정도에 따라 정보보호서비스 품질, 즉 신뢰성, 반응성, 전문성, 대응성, 연속성에 영향을 미치는지 검증해보고자 다음과 같은 가설을 제시한다.

가설 2. 정보보호서비스 대가 산정 모델 적용은 서비스 품질에 양(+)의 영향을 미칠 것이다.

2-1. 정보보호서비스 대가 산정 모델 적용은 신뢰성에 양(+)의 영향을 미칠 것이다.

2-2. 정보보호서비스 대가 산정 모델 적용은 반응성에 양(+)의 영향을 미칠 것이다.

2-3. 정보보호서비스 대가 산정 모델 적용은 전문성에 양(+)의 영향을 미칠 것이다.

2-4. 정보보호서비스 대가 산정 모델 적용은 대응성에 양(+)의 영향을 미칠 것이다.

2-5. 정보보호서비스 대가 산정 모델 적용은 연속성에 양(+)의 영향을 미칠 것이다.

(3) 정보보호서비스 대가 산정 모델과 정보보호성과 간의 관계

정보보호와 기관의 대외 신뢰도의 가치와의 관계는 시민의 신뢰성을 기반으로 한다. 시민이 안전하다고 느끼지 못하면 지방정부는 존재의 의미가 없는 것이다. 특히 보안 사고는 기관 내부의 보안정책이나 정보보호시스템 관리가 허술하거나 시민의 개인정보가 안전하지 못하다는 신호가 될 수 있으며, 장기적인 관점에서

기관의 정보보호성과와 신뢰성을 의심하게 될 것이다. 대부분의 기관은 이를 사전에 방지하기 위해 보안 관련 솔루션을 구매하거나 보안 프로젝트를 실시하고 있으며, 이를 통해 시민의 신뢰를 얻을 수 있도록 노력하고 있다.

마지막 가설로 정보보호서비스 대가 산정 모델 적용이 정보보호성과에 긍정적인 영향을 미칠 것으로 가정하고 검증해고자 한다. 정보보호서비스 대가 산정 모델에 대한 적용의 정도에 따라 재무적 성과와 비재무적 성과로 구분하여 정보보호성과에 영향을 미치는지를 살펴보고자 다음과 같은 가설을 제시한다.

가설 3. 정보보호서비스 대가 산정 모델 적용은 정보보호성과에 양(+)의 영향을 미칠 것이다.

3-1. 보안성 지속 대가 적용은 정보보호성과에 양(+)의 영향을 미칠 것이다.

3-2. 위험관리 대가 적용은 정보보호성과에 양(+)의 영향을 미칠 것이다.

3) 연구 설계

(1) 변수의 조작적 정의

본 연구는 지방자치단체의 정보보호서비스 품질에 대한 적정한 보상을 위해 마련된 정보보호서비스 대가 산정 모델과 정보보호성과와의 관계를 분석하기 위해 배경변수로 인구 통계학적 특성, 독립변수로 정보보호서비스 품질, 매개변수로 정보보호서비스 대가 산정 모델 적용, 종속변수로 정보보호성과와의 관계로 설정하였다.

본 연구에서 설문항목은 기존 연구의 요인들과 설문항목을 참고하여 연구 목적에 맞게 수정 보완하였으며, 연구의 진행은 설문의 신뢰성을 높이고자 사전 설문조사를 실시한 후 이를 통해 수집된 설문조사 자료를 바탕으로 실증분석을 실시하였다. 모든 설문항목은 리커트(Likert) 7점 척도를 사용하였다.

[표 Ⅲ-1] 연구 변수의 조작적 정의와 출처

구분	연구변수		조작적 정의	출처
독립변	정 보 보	신뢰성	약속한 서비스를 정확하고 신뢰성	PZB(1988),

구분	연구변수		조작적 정의	출처
수	호서비스 품질		있게 수행하는 능력	김홍일(2011) 등
		반응성	고객의 요구와 불만을 신속하게 처리하는 자세	
		전문성	능력을 활용하여 고객에게 확신을 주는 자세	
		대응성	고객의 요구사항을 자발적으로 신속하게 서비스하고자 하는 자세	
		연속성	정보보서비스가 연속적으로 서비스하고자 하는 자세	
	정보보호서비스 대가산정 모델 적용	보안성 지속대가	보안성 지속서비스, 보안관제, 보안컨설팅, 시큐어 코딩 등 보안서비스에 대한 비용 산정	조연호(2015), 한국정보보호산업협회(2017) 등
		위험관리 대가	보안사고 대응, 정보보호서비스 불만에 따른 환불비용 등 위험관리 비용 산정	
종속변수	정보보호성과	재무적성과	보안사고 비용, 침해사고에 따른 손실비용 등	NIST(2007), Hagen(2008)
		비재무적성과	기관 이미지 및 신뢰도, 서비스 품질, 직무 및 인식 개선	

가. 정보보호서비스 품질

정보보호서비스는 정보시스템에 대한 해킹, 정보유출, 신규 악성코드 등 내·외부 보안위협에 대한 사전 예방과 사후 대응을 위한 활동을 말하며, 주요 서비스로는 보안성 지속서비스, 보안컨설팅, 보안관제서비스, 물리보안 등으로 구분된다. 본 연구에서 제시하는 정보보호서비스의 유형은 다음과 같다.

[표 Ⅲ-2] 정보보호서비스 유형

서비스 영역	주요 활동
정보보호 관리체계 서비스	· 정보보호관리체계(ISMS-P) 구축 영역별 기획 · 정보보호서비스 영역별 품질 관리 및 개선 도출 · S-PDCA별 보안관리대책 수립 기획 등
위험분석 관리서비스	· 정보자산 식별 및 중요도 평가 · 서버, 보안장비, DB, 네트워크, IoT 등 인프라 취약점 진단 · 웹 취약점 및 시큐어코딩 진단

서비스 영역	주요 활동
	· 보안취약점 진단결과에 따른 위험분석평가 및 보호대책 수립
위협분석 관리서비스	· 외부로부터 침해 탐지 로그/패킷 수집 · 초동 분석결과를 기초로 한 보안로그 수집 · 분석 · 공격자의 정보, 침투시간, 공격방법, 취약점정보, 정보자산의 피해여부 등 피해규모 파악, 복구지원 · 유형별 대응 방안 전략 수립
보안운영 서비스	· 정보보호시스템 운영, 장비 이벤트 및 로그 백업 · 서버, 보안장비, DB, 네트워크, IoT 등 IT 인프라의 정기/긴급 보안패치 및 릴리즈 · 정기점검 및 장애처리, 자산 관리 업무 · 주요 IT 인프라 가용성 · 무결성 체크 · 정보보호시스템 패턴 생성 및 변경관리 · 정보보호 교육 및 기술동향 자문 · 정보보호시스템 운영 및 가용성, 보안동향 등 시스템 분석보고서 작성/관리
보안대응 서비스	· 사이버 침해 및 보안위협 모니터링/탐지·대응조치 · 분석 · 악성코드 분석 및 유포지 차단 서비스 · 해킹메일 모의훈련 및 복구테스트 서비스 등
보안지원 서비스	· PC 등 Endpoint 장비에 대한 보안진단 및 조치 지원 · 보안 관련 Help-desk 운영 및 응답지원 등

지방자치단체는 국민과 관련된 유 · 무형 자산의 행정업무와 서비스, 데이터를 보유하고 있다. 특히 국민의 개인정보를 주로 이용하고 있기 때문에, 이와 관련된 전자정부서비스 품질의 판단은 국민의 전반적인 판단에 의해 측정되고 있다. 하지만, 정보보호서비스에 대한 서비스 품질은 국민들이 직접적으로 체감할 수 없기 때문에 직접적인 수혜를 받고 있는 기관 내 · 외부의 종사자를 대상으로 할 필요가 있다.

본 연구에서는 정보보호서비스 품질에 대한 적정한 보상 대가를 산정하는 과정도 함께 수행해야 되기 때문에 지방자치단체의 종사자와 정보보호서비스를 제공하는 수행사 직원이 자신들의 기관에서 제공하고 있는 정보보호서비스 품질과 이를 통해 도출된 정보보호서비스 대가 산정 모델 적용에 초점을 맞춰 정보보호

서비스 품질, 즉 신뢰성, 반응성, 전문성, 대응성, 연속성 등 세부 요소를 활용하여 품질의 수준을 판단하고자 한다.

본 연구에서는 정보보호서비스 품질에 대한 적정한 보상 대가를 산정하는 과정도 함께 수행해야 되기 때문에 지방자치단체의 종사자와 정보보호서비스를 제공하는 수행사 직원이 자신들의 기관에서 제공하고 있는 정보보호서비스 품질과 이를 통해 도출된 정보보호서비스 대가 산정 모델 적용에 초점을 맞춰 정보보호서비스 품질 수준을 판단하고자 한다.

나. 정보보호서비스 대가 산정 모델 적용

정보보호서비스 대가 산정 모델이란 기관의 데이터의 훼손·변조·유출 등을 예방하기 위해 보안업데이트, 보안정책관리, 위험분석평가, 사고분석, 보안 기술자문, 모의훈련 등 관리적·물리적·기술적 기반의 보안서비스에 대해 적정한 보상차원에서 서비스별 원가를 산정하는 방식이다.

본 연구에서는 보안성 지속대가와 위험관리대가 등 2가지 관점으로 구분하였다. 보안성 지속대가는 정보보호서비스 품질 향상을 위한 적용비용이며, 위험관리대가는 서비스 불만에 따른 개선, 보안사고 대응 실패에 따른 환불비용, 대외 신뢰도 회복에 따른 비용 등으로 구성하였다.

다. 정보보호성과

본 연구에서는 정보보호성과에 대한 Hagen(2008)이 제시한 리스크 관리 관점, 경제적 관점, 법적 관점, 문화적 관점 등 3가지 관점 중 리스크 관리, 경제적, 문화적 관점 등 3가지 관점을 채택하였으며, 각 관점에 속하는 세부 항목은 문헌연구를 통해 다시 재무적 성과와 비재무적 성과로 재구분하여 8개의 성과 측정치를 채택하여 likert 7점 척도를 이용하여 측정하였다.

[표 Ⅲ-3] 정보보호성과의 관점 유형(재분류)

분류	측정항목
리스크 관리	· 보안사고 손실 감소

⇨

분류	측정항목
재무적 성과	· 보안사고 손실 감소 · 보안사고 처리비용 감소

분류	측정항목
관점	
경제적 관점	· 보안사고 처리비용 감소 · 경영진과 직원의 보안 관심과 인식 증가
문화적 관점	· 기관의 보안수준 향상 · 공급자와 협력자의 신뢰와 관계 향상 · 조직의 정보보호역량증가 · 기관의 대외 이미지와 신뢰도 증대
법적 관점	· 법 준거성

분류	측정항목
비재무적 성과	· 경영진과 직원의 보안관심과 인식 증가 · 기관의 보안수준 향상 · 공급자와 협력자의 신뢰와 관계 향상 · 조직의 정보보호역량 증가 · 기관의 대외 이미지와 신뢰도 증대

(2) 설문지의 구성

본 연구에 이용된 설문지는 1) 정보보호서비스 품질 수준 측정, 2) 정보보호서비스 대가 산정 모델 적용 측정, 3) 정보보호성과 측정, 4) 조사대상자의 일반적 특성(인구 통계학적 특성) 등 4가지 부분으로 구성되어져 있다. 설문지의 구성을 정리하면 [표 Ⅲ-4]와 같다.

[표 Ⅲ-4] 설문지 항목의 구성

구분		문항
정보보호서비스 품질	신뢰성	나는 정보보호서비스를 통해 조직의 정보보호 관리체계에 대한 신뢰가 향상되었다고 생각한다.
		나는 정보보호서비스를 통해 내부 관리적, 기술적, 물리적 보안 규정에 대한 신뢰가 향상되었다고 생각한다.
		나는 정보보호서비스를 통해 기관의 대외 신뢰도가 전반적으로 향상되었다고 생각한다.
	반응성	나는 정보보호서비스 담당 직원이 고객 욕구 변화에 따른 신속한 대응능력을 갖추었다고 생각한다.
		나는 정보보호서비스 담당 직원으로부터 빠른 기술지원을

구분		문항
		받았다고 생각한다.
		나는 정보보호서비스 담당 직원이 고객 불만에 대한 처리 속도가 빠르다고 생각한다.
	전문성	나는 정보보호서비스 담당직원은 고객의 질문에 답변할 충분한 전문지식과 정보를 가지고 있다고 생각한다.
		나는 정보보호서비스 담당직원이 보안 관련 법률 및 제도, 관리적, 물리적, 기술적 보호조치에 대한 전문지식을 보유하고 있다고 생각한다.
		나는 정보보호서비스를 통해 위험분석 및 평가의 적절한 업무 수행이 가능해졌다고 생각한다.
	대응성	나는 정보보호서비스를 통해 보안 사고를 예방하는데 효과적이라고 생각한다.
		나는 정보보호서비스를 통해 보안사고 발생 시 신속한 대응이 가능하다고 생각한다.
		나는 정보보호서비스를 통해 정보유출 등 보안사고가 감소되었다고 생각한다.
	연속성	나는 정보보호서비스를 통해 정보보호교육 및 훈련 활동에 적극적 참여 및 지원이 증가하였다고 생각한다.
		나는 정보보호서비스를 통해 정보보호에 대한 관심과 인식이 증가했다고 생각한다.
		나는 정보보호서비스를 통해 지속적인 정보보호활동이 이루어지고 있다고 생각한다.
정보보호서비스 대가 모델 적용	보안성 지속 대가	나는 조직이 정보보호서비스 품질 향상을 위한 보안성 지속서비스 비용에 적용를 아끼지 않는다고 생각한다.
		나는 조직이 정보보호서비스 품질 향상을 위해 서비스에 대한 적정한 대가를 산정하여 이에 대한 적용를 아끼지 않는다고 생각한다.
		나는 정보보호서비스 품질 대가는 지금 내고 있는 금액 이상으로 거래가치가 있다고 생각한다.
	위험관리 대가	나는 정보보호서비스 불만에 대한 개선비용에 적용를 아끼지 않는다고 생각한다.
		나는 사이버 침해 대응 불만족에 대한 환불비용(손해배상 등)에 적용를 아끼지 않는다고 생각한다.
		나는 하락된 기관의 대외 신뢰도 회복을 위한 관리비용에

구분		문항
		적용를 아끼지 않는다고 생각한다.
정보보호성과	재무적	나는 정보보호서비스를 통해 보안사고 손실이 감소하였다고 생각한다.
		나는 정보보호서비스를 통해 보안사고 처리비용(처리시간 단축 등)을 절감하였다고 생각한다.
		나는 보안적용의 효율성이 증가되었다고 생각한다.
	비재무적	나는 정보보호서비스를 통해 경영진과 직원의 보안에 대한 관심과 인식이 증가되었다고 생각한다.
		나는 정보보호서비스를 통해 기관의 보안 수준(무결성, 기밀성, 가용성)이 향상되었다고 생각한다.
		나는 정보보호서비스를 통해 공급자와 협력자의 신뢰와 관계가 향상되었다고 생각한다.
		나는 정보보호서비스를 통해 조직의 정보보호역량이 증가되었다고 생각한다.
		나는 정보보호서비스를 통해 기관의 대외 이미지와 신뢰도가 증대되었다고 생각한다.

(3) 자료 수집 및 응답자의 일반적 특성

본 조사에 앞서 설문의 신뢰도를 높이기 위해 예비조사를 2019년 9월 16일부터 9월 18일까지 3일간 서귀포시 정보보호담당 공무원을 대상으로 20부의 설문을 실시하였고, 설문 항목 중 이해하기 어렵거나 애매한 내용이 있는 문항들에 대해 자문을 받아서 수정 보완하였다.

본 설문조사는 2019년 9월 23일부터 10월 4일까지 12일간 서귀포시 정보보호 및 정보화담당자를 비롯한 정보화담당부서 공무원들과 이 기관을 대상으로 한 정보화 및 정보보호 관련 프로젝트를 수행하거나 수행한 경험이 있는 제주지역 ICT 업체를 대상으로 직접방문, FAX, 이메일을 통해 실시하였다. 조사기간 동안 총 128부의 설문을 송부하여 89부의 설문지가 회수되었으며, 일부 불성실한 답변을 제외한 87부가 최종 분석에 사용되었다.

실증분석에 사용된 설문에 대한 응답자의 특성은 응답자의 성별, 연령, 학력, 직장유형, 직위(급), 근무년수 등으로 구분하였다.

[표 Ⅲ-5] 표본의 특성

항목	대상	N	유효비율(%)	누적비율(%)	계
성별	남	51	58.6	58.6	87
	여	36	41.4	100.0	
연령	20대	16	18.4	18.4	87
	30대	29	33.3	51.7	
	40대	32	36.8	88.5	
	50대 이상	10	11.5	100.0	
최종학력	고졸	-	-	-	87
	대졸(2년)	5	5.7	5.7	
	대졸(4년)	75	86.2	92.0	
	대학원졸	7	8.0	100.0	
직장유형	공무원	62	71.3	71.3	87
	ICT 업체	25	28.7	100.0	
직위(급)	사원급	12	13.8	13.8	87
	임원급	13	14.9	28.7	
	5급 이상	3	3.4	32.2	
	6급	9	10.3	42.5	
	7급	26	29.9	72.4	
	8급 이하	24	27.6	100.0	
근무년수	3년 미만	25	28.7	28.7	87
	3~5년	11	12.6	41.4	
	5~10년 미만	19	21.8	63.2	
	10년 이상	32	36.8	100.0	

총 87부의 설문에 대한 표본특성을 분석한 결과를 살펴보면, 응답자의 성별 분포는 남성이 51명(58.6%), 여성이 36명(41.4%)으로 나타났고, 연령별 분포는 40대가 32명(36.8%)로 가장 많았으며, 30대 29명(33.3%), 20대 16명(18.4%), 50대 이상 10명(11.5%)의 순으로 나타났다. 직장유형은 공무원 62명(71.3%), ICT업체 25명(28.7%)의 분포를 보였다. 직위(급)별 분포는 공무원인 경우, 7급 26명(29.9)로 가장 많았으며, 8급 이하 24명(27.6%), 6급 9명(10.3%), 5급 이상 3명(3.4%)의 순으로 나타났으며, 일반인인 경우, 임원급 13명(14.9%), 사원급 12명(13.8%)의 분포를 보였다. 근무년수의 분포는 10년 이상 32명(36.8%)로 가장 많았으며, 3년 미만 25명(28.7%), 5~10년 미만 19명(21.8%), 3~5년 미만 11명(12.6%)의 순으로

분포를 보였다. 설문응답자의 학력은 대졸(4년제) 75명(86.2%), 대학원졸 7명(8%), 대졸(2년제) 5명(5.7%)의 분포를 보였다.

(4) 분석방법

수집된 자료를 바탕으로 항목들 간의 유사성과 일관성, 예측가능성과 의존가능성, 안전성, 정확성 등을 알아보는 신뢰성 분석은 크론바흐(Cronbach, 1951)의 알파계수(Cronbach's α)를 이용하여 신뢰성을 검증하였고, 설문조사에 이용된 항목들에 대한 요인분석을 통해 판별 타당성을 확보하고자 하였다. 측정 도구에 대한 타당성 및 신뢰성이 확보된 후 남은 최종 항목에 대해 개념 및 변수 간 상관관계분석을 실시하였고, 가설검증을 위해 다중회귀분석방법을 이용하였다. 분석도구는 IBM SPSS statistics를 이용하였으며, 사용된 통계기법을 정리하면 다음 [표 Ⅲ-6]과 같다.

[표 Ⅲ-6] 자료 분석 방법

구분		분석내용	활용 통계기법
기초분석		표본의 구성	빈도분석
		측정도구의 타당성 및 단일 차원성	신뢰성 및 요인분석
		개념 및 변수 간 상관관계	상관관계분석
가설 검증	가설 1	정보보호서비스 품질이 정보보호성과에 미치는 영향	다중회귀분석
	가설 2	정보보호서비스 대가 산정 모델 적용이 정보보호서비스 품질에 미치는 영향	다중회귀분석
	가설 3	정보보호서비스 대가 산정 모델 적용이 정보보호성과에 미치는 영향	다중회귀분석

2. 연구 결과

1) 측정도구의 신뢰성 및 타당성 검증

(1) 신뢰성 검증

신뢰성은 연구대상에 대해 측정오류가 존재하지 않기 위해 모든 변수에 대해 반복적으로 측정하였을 때 결과에 대한 일관성을 보장하느냐를 판단하는 개념이다. 모든 변수에 대해 얼마나 신뢰성 있게 측정되었는지의 여부에 대한 검증이 필요하며, 본 연구에서도 Cronbach's α계수를 이용하여 동일한 개념에 대해 다수의 복수 항목으로 신뢰도를 측정하였다. Cronbach's α계수는 0~1 사이의 값을 가지고 있으며, 신뢰도 계수의 적정수준을 판정하는 절대적인 기준은 없지만, 일반적으로 Nunally(1979)가 제시한 0.7 이상이면 적정수준으로 판단하고 있다.

본 연구의 각 변수에 대한 신뢰도 분석 결과 [표 Ⅲ-7]과 같이 제시되어 있다.

[표 Ⅲ-7] 신뢰도 분석 결과

구분	측정변수		문항수	Cronbach's α 계수
독립변수	정보보호서비스 품질	신뢰성	3	0.797
		반응성	3	0.732
		전문성	3	0.767
		대응성	3	0.839
		연속성	3	0.802
	정보보호서비스 대가 모델 적용	보안성지속대가	3	0.730
		위험관리대가	3	0.724
종속변수	정보보호성과	재무적 성과	3	0.834
		비재무적 성과	5	0.711
전체			29	0.886

모든 측정변수에 대해 신뢰도 분석결과를 살펴보면, 모든 측정 변수의 Crobach's α 값이 0.7을 넘어 측정도구의 신뢰도를 확보되었다고 볼 수 있으며, 전체 29개 문항에 대한 신뢰도는 .886으로 나타났다. 따라서 이번 연구를 위해 개발된 모든 변수들의 잔여 항목을 요인분석에 이용하였다.

(2) 타당성 검증

요인분석(Factor analysis)은 다 수의 측정항목을 공통요인으로 묶어서 자료의 복잡성을 줄이고, 변수를 구성하는 항목들이 동일한 구성 개념을 측정하는지를 파악하는 분석방법으로, 측정도구의 타당성을 검증하기 위해 많이 사용하고 있다.

본 연구에서는 측정도구의 타당성을 검증하기 위해 주성분분석(PCA : Principal component analysis)을 실시하였다. 주성분분석은 정보의 손실을 최소화하면서 다수의 변수를 가능한 한 최소한의 요인으로 줄이는 데 그 목적이 있다. 요인 수의 결정하는 고유 값의 기준을 1보다 클 경우에만 추출되게 하였고, 요인들 간의 상호 독립성을 유지한 상태로 회전하는 방법인 직교회전방법인 베리멕스(Varimax method)를 이용하여 분석하였다.

일반적으로 요인분석 결과, 공통성(Communality)이 0.4 미만이면 요인분석에서 제거하는 것이 요인분석의 적합도가 가장 좋기 때문에 요인적재 값(Factor loading)이 0.4 이상인 것을 기준으로 하였다.

가. 정보보호서비스 품질에 대한 타당성 검증

정보보호서비스 품질에 대한 요인분석을 실시한 결과가 [표 Ⅲ-8]과 같이 제시되어 있다. 정보보호서비스 품질에 대한 설문 항목의 문항 간 상관성이 높게 나타나며 한 개로 묶여 개념 간의 타당성이 적절한 것으로 나타났다.

[표 Ⅲ-8] 정보보호서비스 품질에 대한 요인 분석 결과

구분	측정변수		문항수	요인
독립변수	정보보호 서비스 품질	신뢰성	REL-3	0.682
			REL-2	0.638

구분	측정변수		문항수	요인
			REL-1	0.504
		반응성	REA-2	0.819
			REA-1	0.685
			REA-3	0.569
		전문성	PRO-2	0.828
			PRO-3	0.754
			PRO-1	0.531
		대응성	RES-1	0.742
			RES-2	0.690
			RES-3	0.616
		연속성	CON-1	0.804
			CON-2	0.780
			CON-3	0.605

나. 정보보호서비스 대가 산정 모델 적용에 대한 타당성 검증

정보보호서비스 대가 산정 모델 적용에 대한 요인분석을 실시한 결과가 [표 Ⅲ-9]와 같이 제시되어 있다. 정보보호서비스 대가 산정 모델에 대한 설문 항목의 항목 간 상관성이 높게 나타나며 하나로 묶여 개념 간의 타당성이 적절한 것으로 나타났다.

[표 Ⅲ-9] 정보보호서비스 대가 산정 모델 적용에 대한 요인 분석 결과

구분	측정변수		문항수	요인
독립변수	정보보호서비스 대가 산정 모델 적용	보안성지속대가	PRE-2	0.751
			PRE-1	0.722
			PRE-3	0.558
		위험관리대가	RIM-3	0.668
			RIM-1	0.641
			RIM-2	0.622

다. 정보보호성과에 대한 타당성 검증

정보보호성과에 대한 요인분석을 실시한 결과가 [표 Ⅲ-10]과 같이 제시되어 있다. 정보보호성과에 대한 설문 항목의 문항 간 상관성이 높게 나타나며 하나로 묶여 개념 간의 타당성이 적절한 것으로 나타났다.

[표 Ⅲ-10] 정보보호 성과에 대한 요인 분석 결과

구분	측정변수		문항수	요인
종속변수	정보보호성과	재무적	FIN-2	0.789
			FIN-1	0.761
			FIN-3	0.693
		비재무적	NFI-3	0.799
			NFI-2	0.750
			NFI-4	0.745
			NFI-5	0.681
			NFI-1	0.549

2) 기술통계량과 상관관계 분석

(1) 기술통계량

기술통계량은 표본에 대한 중요한 기초적인 자료이다. 이 장에서는 본 연구에서 사용될 주요 변수인 정보보호서비스 품질, 정보보호서비스 대가 산정 모델 적용, 정보보호성과의 특성에 대한 기초 통계량을 제시하였다. 각 변수에 대한 기술통계량을 통해서 각 변수 간의 간단한 관계를 판단할 수 있을 것이다.

가. 정보보호서비스 품질에 대한 기초통계량

가설 검증에 이용될 정보보호서비스 품질의 하위 변수인 신뢰성, 반응성, 전문성, 대응성, 연속성에 대한 기초통계량은 [표 Ⅲ-11]과 같이 제시되어 있다.

[표 Ⅲ-11] 정보보호서비스 품질에 대한 기초통계량(총괄)

구분	측정변수		N	최소값	최대값	평균	표준편차
정보보호서비스 품질	신뢰성	REL	87	1	30	16.95	11.083
	반응성	REA	87	1	27	16.06	10.803
	전문성	PRO	87	1	53	35.34	22.337
	대응성	RES	87	1	37	18.61	16.071
	연속성	CON	87	1	37	22.20	14.072

[표 Ⅲ-11]의 정보보호서비스 품질에 대한 기초통계량을 살펴보면 신뢰성의 평균은 16.95, 반응성의 평균은 16.06, 전문성의 평균은 35.34, 대응성의 평균은 18.61, 연속성의 평균은 22.20으로 나타났다. 이러한 결과는 지방자치단체인 서귀포시는 전문성, 대응성, 연속성, 신뢰성, 반응성 순으로 정보보호서비스 품질을 이용자에게 제공하고 있음을 알 수 있다. 세부 문항별 기초통계량은 [표 Ⅲ-12]와 같이 제시되어 있다.

[표 Ⅲ-12] 정보보호서비스 품질에 대한 기초통계량(세부)

구분	측정변수		N	최소값	최대값	평균	표준편차
정보보호서비스 품질	신뢰성	REL-1	87	5	7	6.53	0.567
		REL-2	87	5	7	6.43	0.542
		REL-3	87	5	7	6.47	0.662
	반응성	REA-1	87	5	7	6.43	0.603
		REA-2	87	5	7	6.41	0.657
		REA-3	87	5	7	6.38	0.651
	전문성	PRO-1	87	5	7	6.26	0.493
		PRO-2	87	5	7	6.15	0.418

구분	측정변수		N	최소값	최대값	평균	표준편차
		PRO-3	87	5	7	6.13	0.426
	대응성	RES-1	87	4	7	6.46	0.679
		RES-2	87	4	7	6.47	0.819
		RES-3	87	5	7	6.44	0.677
	연속성	CON-1	87	5	7	6.51	0.547
		CON-2	87	5	7	6.53	0.546
		CON-3	87	5	7	6.59	0.540

나. 정보보호서비스 대가 산정 모델 적용에 대한 기초통계량

정보보호서비스 대가 산정 모델 적용에 검증될 하위 변수인 보안성 지속대가, 위험관리대가에 대한 기초통계량은 [표 Ⅲ-13]과 같이 제시되어 있다.

[표 Ⅲ-13] 정보보호서비스 대가 산정 모델 적용에 대한 기초통계량(총괄)

구분	측정변수		N	최소값	최대값	평균	표준편차
정보보호서비스 대가모델 적용	보안성 지속대가	PRE	87	1	38	19.71	16.385
	위험관리 대가	RIM	87	1	37	20.95	14.214

[표 Ⅲ-13]의 정보보호서비스 대가 산정 모델 적용에 대한 기초통계량을 살펴보면 보안성 지속대가의 평균은 19.71, 위험관리대가의 평균은 20.95로 나타났다. 이러한 결과는 제주지역의 S기관이 정보보호서비스 품질에 대한 적정한 대가에 대해 평균 정도의 적용를 하고 있으며, 공급자와 수혜자 모두 평균정도의 만족감을 느끼고 있음을 알 수 있다. 세부 문항별 기초통계량은 [표 Ⅲ-14]와 같이 제

시되어 있다.

[표 Ⅲ-14] 정보보호서비스 대가 산정 모델 적용에 대한 기초통계량(세부)

구분	측정변수		N	최소값	최대값	평균	표준편차
정보보호서비스 대가모델 적용	보안성 지속대가	PRE-1	87	4	7	6.54	0.625
		PRE-2	87	4	7	6.64	0.628
		PRE-3	87	5	7	6.48	0.645
	위험관리 대가	RIM-1	87	5	7	6.59	0.518
		RIM-2	87	5	7	6.70	0.485
		RIM-3	87	6	7	6.56	0.499

다. 정보보호성과에 대한 기초통계량

정보보호성과에 검증될 하위 변수인 재무적 성과와 비재무적 성과에 대한 기초통계량은 [표 Ⅲ-15]와 같이 제시되어 있다.

[표 Ⅲ-15] 정보보호성과에 대한 기초통계량(총괄)

구분	측정변수		N	최소값	최대값	평균	표준편차
정보보호성과	재무적 성과	FIN	87	1	38	19.41	16.619
	비재무적 성과	NFI	87	1	14	5.23	5.249

[표 Ⅲ-15]의 정보보호성과에 대한 기초통계량을 살펴보면 재무적 성과의 평균은 19.41, 비재무적 성과의 평균은 5.23으로 나타났다. 이러한 결과는 제주지역의 S기관이 정보보호서비스 품질과 정보보호서비스 대가 산정 모델 적용로 평균 이상의 정보보호성과를 얻고 있음을 보여 주는 것이라 할 수 있다. 세부 문항별 기

초통계량은 [표 Ⅲ-16]과 같이 제시되어 있다.

[표 Ⅲ-16] 정보보호성과에 대한 기초통계량(세부)

구분	측정변수		N	최소값	최대값	평균	표준편차
정보보호성과	재무적 성과	FIN-1	87	4	7	6.47	0.679
		FIN-2	87	4	7	6.49	0.805
		FIN-3	87	5	7	6.48	0.645
	비재무적 성과	NFI-1	87	4	7	6.34	0.819
		NFI-2	87	4	7	6.46	0.696
		NFI-3	87	4	7	6.46	0.833
		NFI-4	87	5	7	6.44	0.694
		NFI-5	87	4	7	6.32	0.707

(2) 상관관계 분석

본 연구의 주요 변수인 정보보호서비스 품질, 정보보호서비스 대가 산정 모델 적용, 정보보호성과 간의 상관관계를 분석하기 위해 Pearson의 상관관계 분석을 실시하였다. 상관관계 분석은 하나의 변수가 다른 변수와의 상관성을 가지고 변하는지를 검증하기 위해 이용되며 변수들 간의 상관성 정도를 특정 변수의 분산 중에서 다른 변수가 같이 변하는 공분산이 어느 정도 영향을 미치느냐에 따라 좌우된다. 상관관계의 크기를 나타내는 값은 상관계수라 하는데, 상관계수는 -1 ~ +1 사이의 값을 갖는다. 상관계수가 하나의 독립변수가 높아질수록 종속변수가 높아지는 관계라면 이를 양(+)적 상관관계라고 하며, 독립변수가 높아질수록 종속변수가 낮아지는 관계라면 이를 음(-)적 상관관계라고 한다. 상관계수가 0에 근사하면 상관관계가 거의 없다고 할 수 있다.

본 연구에서의 변수들 간의 상관관계를 분석한 결과는 [표 Ⅲ-17]과 같다.

[표 Ⅲ-17] 관련 변수 간의 상관관계 결과

	신뢰성	반응성	전문성	대응성	연속성	보안성 지속 대가	위험 관리 대가	재무적 성과	비재무적 성과
신뢰성	1								
반응성	.042	1							
전문성	.197	-.019	1						
대응성	.553**	.019	.228*	1					
연속성	-.038	.130	-.056	-.128	1				
보안성 지속대가	.519**	.028	.189	.970**	-.105	1			
위험관리 대가	.014	.030	-.005	-.344**	.189	-.314**	1		
재무적 성과	.551**	.042	.189	.970**	-.127	.940**	-.310**	1	
비재무적 성과	.345**	.239*	.133	.716**	-.024	.694**	-.293**	.695**	1

* $p < .05$, ** $p < .01$

[표 Ⅲ-17]의 상관관계를 살펴보면, 대부분의 변수가 1% 유의수준에서 통계적으로 유의한 것으로 나타났다.

첫 번째, 정보보호서비스 품질의 측정변수를 살펴보면, 신뢰성은 대응성(r=.553), 보안성지속대가(r=.519), 재무적 성과(r=.551), 비재무적 성과(r=.345)로 1% 유의수준(p<.01)에서 유의한 양(+)적 상관관계를 보인 것으로 나타난 반면에, 반응성(r=.042), 전문성(r=.197), 연속성(r=-.038), 위험관리대가(r=.014)로 변수 간의 상관관계가 없는 것으로 나타났다. 반응성은 비재무적 성과(r=.239)로 5% 유의수준에서 유의한 양(+)적 상관관계를 보인 것으로 나타난 반면에, 전문성(r=-.019), 대응성(r=.019), 연속성(r=.130), 보안성 지속대가(.028), 위험관리대가

(r=.030), 재무적 성과(r=.042)로 변수 간의 상관관계가 없는 것으로 나타났다. 전문성은 대응성(r=.228)로 5% 유의수준에서 유의한 양(+)적 상관관계를 보인 것으로 나타난 반면에, 연속성(r=-.056), 보안성 지속대가(r=.189), 위험관리대가(r=-.005), 재무적 성과(r=.189), 비재무적 성과(r=.133)로 변수 간의 상관관계가 없는 것으로 나타났다. 대응성은 보안성 지속대가(r=.970), 재무적 성과(r=.970), 비재무적 성과(r=.716)로 1% 유의수준에서 유의한 양(+)적 상관관계를 보인 것으로 나타난 반면에, 위험관리대가(r=-.344)로 1% 유의수준에서 유의한 음(-)적 상관관계를 보인 것으로 나타났으며, 연속성(r=-.128)로 변수 간의 상관관계가 없는 것으로 나타났다. 연속성은 보안성 지속대가(r=-.105), 위험관리대가(r=.189), 재무적 성과(r=-.127), 비재무적 성과(r=-.024)로 변수 간의 상관관계가 없는 것으로 나타났다.

두 번째, 정보보호서비스 대가 산정 모델 적용의 측정변수를 살펴보면, 재무적 성과(r=.940), 비재무적 적용(r=.694)로 1% 유의수준에서 유의한 양(+)적 상관관계를 보인 것으로 나타난 반면에, 위험관리대가(r=-.314)로 1% 유의수준에서 유의한 음(-)적 상관관계를 보인 것으로 나타났다. 위험관리대가는 재무적 성과(r=-.310), 비재무적 적용(r=-.293)로 1% 유의수준에서 유의한 음(-)적 상관관계를 보인 것으로 나타났다.

마지막으로, 정보보호성과의 측정변수를 살펴보면, 재무적 성과는 비재무적 성과(r=.695)로 1% 유의수준에서 유의한 양(+)적 상관관계를 보인 것으로 나타났다.

3) 가설 검정

정보보호서비스 품질 대가 모델 적용이 정보보호성과에 어떠한 영향을 미치는지 검증하기 위해 다중회귀분석(Multiple linear regression analysis)을 이용했다.

다중회귀분석은 여러 개의 독립변수가 동시 종속변수에 영향을 미치는 경우 검증할 때 많이 이용된다. 다중회귀분석에서 가장 중요한 것은 독립변수들에 대한 유의성 여부를 확인하기 전에 회귀모형에 대한 적합도와 설명력을 확인해야 하는데, 적합도는 SPSS 측정결과표 중 ANOVA 항목을 확인하여 유의확률 결과

가 분산분석의 p<.05보다 작으면 회귀모형이 적합하다고 할 수 있다. 회귀모형에 대한 설명력은 회귀모형에 불필요한 변수여부를 판단하는 것을 의미하는데, 다중회귀분석에서는 수정된 R^2(adjusted R^2) 값으로 확인한다. 수정된 R^2(adjusted R^2)은 불필요한 독립변수가 추가되었을 경우 감소하게 되어있는 특성을 지니고 있으며, SPSS 측정결과표의 모형요약 항목 중 수정된 R^2(adjusted R^2) 값으로 판단한다.

다중회귀분석에서는 잔차의 독립성 여부를 판단하기 위해 Durbin-Watson 통계량으로 판단한다. 잔차는 회귀분석에서 나타나는 오차 값으로 규칙없이 무작위로 나타난다는 의미이며, 관측 값에서 예측 값을 뺀 수치이다. Durbin-Watson 통계량은 SPSS 측정결과표의 모형요약 항목 중 Durbin-Watson값이 일반적으로 많이 이용되는 기준이 1.5~2.5 사이에 근사하면 잔차의 독립성 가정을 위배하지 않은 것으로 평가된다.

다중회귀분석에서는 여러 개의 변수가 있기 때문에, 독립변수 간의 유사성을 판단하는 다중공선성을 살펴봐야 된다. 다중공선성의 문제여부는 분산팽창지수(VIF : Variance Inflation Factor)를 통해 판단되며, 일반적으로 VIF < 10이면 문제없는 것으로 판단된다. 다중공선성에 문제가 없다면, 변수별로 유의성을 판단하기 위해 SPSS 측정결과표의 계수 항목 중 독립변수별로 유의확률(p)의 값을 확인하여 변수의 p<.05보다 작으면 독립변수가 종속변수에 유의한 영향을 미치는 것으로 평가되며, 변수의 p값이 .000으로 나온 경우에는 p<.001로 영향을 미치는 것으로 판단된다.

마지막으로 독립변수가 종속변수에 유의한 영향이 양(+)인지, 음(-)인지 판단하기 위해 회귀계수를 확인하는데, SPSS 측정결과표의 계수 항목 중 독립 변수별로 표준화 계수값(β)이 양수(+)이면 '독립변수가 종속변수에 긍정적인 영향을 미친다.'로 판단할 수 있으며, 이는 독립변수가 높아질수록 종속변수도 높아진다는 의미이다. 반면에, 표준화 계수값(β)이 음수(-)이면 '독립변수가 종속변수에 부정적인 영향을 미친다.'로 판단할 수 있으며, 이는 독립변수가 높아질수록 종속변수는 낮아진다는 의미이다.

본 연구에서는 '정보보호서비스 품질이 정보호성과에 미치는 영향', '정보보호서비스 대가 산정 모델 적용이 정보보호서비스에 미치는 영향', '정보보호서비스 대

가 산정 모델 적용이 정보보호성과에 미치는 영향' 등 3가지 가설에 다음과 같이 가설 검증을 하였다.

(1) 정보보호서비스 품질이 정보보호성과에 미치는 영향

정보보호서비스 품질이 정보보호성과에 미치는 영향에 대한 검증은 독립변수인 정보보호서비스 품질의 세부 변수인 신뢰성, 반응성, 전문성, 대응성, 연속성이 종속변수인 정보보호성과의 세부변수인 재무적 성과, 비재무적 성과에 어떠한 영향을 미치는지 검증하기 위해 다중회귀분석을 한 결과 다음과 같이 보여 졌다.

가. 정보보호서비스 품질이 재무적 성과에 미치는 영향

정보보호서비스 품질의 세부 변수인 신뢰성, 반응성, 전문성, 대응성, 연속성이 재무적 성과에 미치는 영향에 대해 다중회귀분석을 통해 검증한 결과는 [표 Ⅲ-18]과 같다.

[표 Ⅲ-18] 정보보호서비스 품질-재무적 성과 간의 관계 분석결과

종속변수	독립변수	비표준화 계수		표준화 계수	*t*	*p*	*VIF*
		B	표준오차	*β*			
재무적 성과	(상수)	0.814	1.375		0.592	.555	
	신뢰성	0.038	0.048	.025	0.786	.434	1.455
	반응성	0.036	0.041	.024	0.877	.383	1.020
	전문성	-0.027	0.020	-.036	-1.296	.199	1.065
	대응성	0.995	0.034	.962	29.542***	<.001	1.494
	연속성	-0.009	0.032	-.008	-0.292	.771	1.037
	F=265.321(p<.001), R^2=.942, $_{adj}R^2$=.939, $D-W$=2.072						

*p<.05, **p<.01, ***p<.001

[표 Ⅲ-18]과 같이 회귀분석 결과, 정보보호서비스 품질의 회귀모형의 적합도는 F=265.321, p<.001로 유의한 것으로 나타났으며, 회귀모형의 설명력은 약 93.9%(수정된 R제곱은 93.9%)로 나타났다(R^2=.942, $adjR^2$=.939).

한편 잔차의 독립성 여부를 판단하기 위해 측정한 결과, Durbin-Watson 통계량은 2.072로 2에 근사하므로 잔차의 독립성 가정을 위배하지 않는 것으로 평가되었고, 다중공선성 문제여부를 판단하기 위한 분산팽창지수(VIF)도 모든 변수에서 10미만으로 나타나 다중공선성 문제가 없는 것으로 평가되었다.

회귀계수의 유의성을 검증한 결과, 대응성(β=.962, p<.001)은 재무적 성과에 긍정적인 영향을 미치는 것으로 보여졌다. 즉, 대응성이 높아질수록 재무적 성과도 높아지는 것으로 평가되었다. 반면, 신뢰성(β=.025, p=.434), 반응성((β=.024, p=.383), 전문성(β=-.036, p=.199), 연속성(β=-.008, p=.771)은 유의하지 않은 것으로 나타났다. 즉, 신뢰성, 반응성, 전문성, 연속성은 재무적 성과에 직접적인 영향을 미치는 않는다는 것으로 검증되었다.

나. 정보보호서비스 품질이 비재무적 성과에 미치는 영향

정보보호서비스 품질의 세부 변수인 신뢰성, 반응성, 전문성, 대응성, 연속성이 비재무적 성과에 미치는 영향에 대해 다중회귀분석을 통해 검증한 결과는 [표 Ⅲ-19]와 같다.

[표 Ⅲ-19] 정보보호서비스 품질-비재무적 성과 간의 관계 분석결과

종속변수	독립변수	비표준화 계수		표준화 계수	*t*	*p*	*VIF*
		B	표준오차	*β*			
비재무적 성과	(상수)	-0.689	1.186		-0.582	.562	
	신뢰성	-0.039	0.042	-.083	-0.944	.348	1.455
	반응성	0.108	0.036	.223	3.033**	.003	1.020
	전문성	-0.004	0.018	-.019	-0.253	.801	1.065

종속변수	독립변수	비표준화 계수		표준화 계수	t	p	VIF
		B	표준오차	β			
	대응성	0.251	0.029	.768	8.632***	<.000	1.494
	연속성	0.015	0.028	.041	0.551	.583	1.037
	F=21.582(p<.001), R^2=.571, $_{adj}R^2$=.545, $D-W$=1.502						

*p<.05, **p<.01, ***p<.001

[표 Ⅲ-19]와 같이 회귀분석 결과, 정보보호서비스 품질의 회귀모형의 적합도는 F=21.582, p<.001로 유의한 것으로 나타났으며, 회귀모형의 설명력은 약 54.5%(수정된 R제곱은 54.5%)로 나타났다(R^2=.571, $adjR^2$=.545).

한편 잔차의 독립성 여부를 판단하기 위해 측정한 결과, Durbin-Watson 통계량은 1.502로 2에 근사하므로 잔차의 독립성 가정을 위배하지 않는 것으로 평가되었고, 다중공선성 문제여부를 판단하기 위한 분산팽창지수(VIF)도 모든 변수에서 10미만으로 나타나 다중공선성 문제가 없는 것으로 평가되었다.

회귀계수의 유의성을 검증한 결과, 반응성(β=.223, p<.01)과 대응성(β=.768, p<.001)은 비재무적 성과에 긍정적인 영향을 미치는 것으로 보여 졌다. 즉, 반응성과 대응성이 높아질수록 재무적 성과도 높아지는 것으로 평가되었다. 반면, 신뢰성(β=-.083, p=.348), 전문성(β=-.019, p=.801), 연속성(β=.041, p=.583)은 유의하지 않은 것으로 나타났다. 즉, 신뢰성, 전문성, 연속성은 재무적 성과에 직접적인 영향을 미치는 않는다는 것으로 검증되었다.

다. 정보보호서비스 품질이 정보보호 성과에 미치는 영향

정보보호서비스 품질이 정보보호 성과에 미치는 영향에 대해 [표 Ⅲ-18]과 [표 Ⅲ-19]와 같이 검증한 결과를 정리하면, 정보보호서비스 품질의 변수 중 대응성은 재무적 성과와 비재무적 성과 모두에 긍정적인 영향을 미치는 것으로 나타났고, 반응성은 비재무적 성과에 긍정적인 영향을 미치는 것으로 나타났다. 이는 대응성이 높을수록 정보보호성과가 높아지며, 반응성이 높을수록 비재무적 성과

가 높아지는 것으로 판단된다. 즉, 정보보호서비스 품질이 정보보호성과에 부분적으로 긍정적인 영향을 미치는 것으로 검증되었으며, 정보보호서비스의 품질이 높아질수록 정보보호성과도 부분적으로 높아진다는 의미이다.

[표 Ⅲ-20] 가설 1 검증 결과

가설	내용		결과
가설 1	**정보보호서비스 품질이 정보보호성과에 미치는 영향**		**부분 채택**
		신뢰성이 재무적 성과에 미치는 영향	기각
		반응성이 재무적 성과에 미치는 영향	기각
		전문성이 재무적 성과에 미치는 영향	기각
		대응성이 재무적 성과에 미치는 영향	**채택**
		연속성이 재무적 성과에 미치는 영향	기각
		신뢰성이 비재무적 성과에 미치는 영향	기각
		반응성이 비재무적 성과에 미치는 영향	**채택**
		전문성이 비재무적 성과에 미치는 영향	기각
		대응성이 비재무적 성과에 미치는 영향	**채택**
		연속성이 비재무적 성과에 미치는 영향	기각

(2) 정보보호서비스 대가 산정 모델 적용이 정보보호서비스 품질에 미치는 영향

정보보호서비스 대가 산정 모델 적용이 정보보호서비스 품질에 미치는 영향에 대한 검증은 독립변수인 정보보호서비스 대가 산정 모델의 세부 변수인 보안성 지속 대가, 위험관리 대가가 종속변수인 정보보호서비스 품질의 세부변수인 신뢰성, 반응성, 전문성, 대응성, 연속성에 어떠한 영향을 미치는지 검증하기 위해 다중회귀분석을 한 결과 다음과 같이 보여 졌다.

가. 정보보호서비스 대가 산정 모델 적용이 신뢰성에 미치는 영향

정보보호서비스 대가 산정 모델의 세부 변수인 보안성 지속 대가 적용, 위험관리 대가 적용이 신뢰성에 미치는 영향에 대해 다중회귀분석을 통해 검증한 결과는 [표 Ⅲ-21]과 같다.

[표 Ⅲ-21] 정보보호서비스 대가 산정 모델-신뢰성 간의 관계 분석결과

종속변수	독립변수	비표준화 계수		표준화 계수	t	p	VIF
		B	표준오차	β			
신뢰성	(상수)	6.007	2.520		2.384	0.019	
	보안성지속대가	0.393	0.065	.581	6.057***	<.001	1.109
	위험관리대가	0.153	0.075	.196	2.046*	.044	1.109
	F=18.358(p<.001), R^2=.301, $_{adj}R^2$=.288, $D-W$=2.046						

*p<.05, **p<.01, ***p<.001

[표 Ⅲ-21]과 같이 회귀분석 결과, 정보보호대가 모델 적용의 회귀모형의 적합도는 F=18.358, p<.001로 유의한 것으로 나타났으며, 회귀모형의 설명력은 약 28.8%(수정된 R제곱은 28.8%)로 나타났다(R^2=.301, $adjR^2$=.288).

한편 잔차의 독립성 여부를 판단하기 위해 측정한 결과, Durbin-Watson 통계량은 2.046으로 2에 근사하므로 잔차의 독립성 가정을 위배하지 않는 것으로 평가되었고, 다중공선성 문제여부를 판단하기 위한 분산팽창지수(VIF)도 보안성 지속 대가 적용(VIF=1.109), 위험관리 대가 적용(VIF=1.109) 모두에서 10미만으로 나타나 다중공선성 문제가 없는 것으로 평가되었다.

회귀계수의 유의성을 검증한 결과, 정보보호서비스 대가 산정 모델의 세부 변수인 보안성지속대가(β=.581 , p<.001), 위험관리대가(β=.196, p<.05)는 신뢰성에 긍정적인 영향을 미치는 것으로 보여 졌다. 즉, 정보보호서비스 대가 산정 모델 적용이 증가할수록 신뢰성이 높아지는 것으로 평가되었다.

나. 정보보호서비스 대가 산정 모델 적용이 반응성에 미치는 영향

정보보호서비스 대가 산정 모델의 세부 변수인 보안성 지속 대가 적용, 위험관리 대가 적용이 반응성에 미치는 영향에 대해 다중회귀분석을 통해 검증한 결과는 [표 Ⅲ-22]와 같다.

[표 Ⅲ-22] 정보보호서비스 대가 산정 모델-반응성 간의 관계 분석결과

종속변수	독립변수	비표준화 계수		표준화 계수	t	p	VIF
		B	표준오차	β			
반응성	(상수)	14.826	2.941		5.042	0.000	
	보안성지속대가	0.027	0.076	.042	0.363	.717	1.109
	위험관리대가	0.033	0.087	.043	0.377	.707	1.109
	F=.104(p=.901), R^2=.002, $_{adj}R^2$=-.021, $D-W$=1.964						

*p<.05, **p<.01, ***p<.001

[표 Ⅲ-22]와 같이 회귀분석 결과, 정보보호대가 모델 적용의 회귀모형의 적합도는 F=.104, p=.901로 유의수준 5%보다 높아서 유의하지 않은 것으로 나타났으며, 회귀모형의 설명력은 약 -2.1%(수정된 R제곱은 -2.1%)로 나타났다(R^2=.002, $adjR^2$=-.021). 한편, 잔차의 독립성 여부를 판단하기 위해 측정한 결과, Durbin-Watson 통계량은 1.964으로 2에 근사하므로 잔차의 독립성 가정을 위배하지 않는 것으로 평가되었고, 다중공선성 문제여부를 판단하기 위한 분산팽창지수(VIF)도 보안성 지속 대가 적용(VIF=1.109), 위험관리 대가 적용(VIF=1.109) 모두에서 10미만으로 나타나 다중공선성 문제가 없는 것으로 평가되었다.

회귀계수의 유의성을 검증한 결과, 정보보호서비스 대가 산정 모델의 세부 변수인 보안성지속대가(β=.042, p=.717), 위험관리대가(β=.043, p=.707) 모두 변수의 유의수준 5%을 넘어서서 반응성에 유의하지 않은 것으로 보여 졌다. 즉, 정보

보호서비스 대가 산정 모델 적용이 반응성에 직접적인 영향을 미치지 않는다는 것으로 평가되었다.

다. 정보보호서비스 대가 산정 모델 적용이 전문성에 미치는 영향

정보보호서비스 대가 산정 모델의 세부 변수인 보안성 지속 대가 적용, 위험관리 대가 적용이 전문성에 미치는 영향에 대해 다중회귀분석을 통해 검증한 결과는 [표 Ⅲ-23]과 같다.

[표 Ⅲ-23] 정보보호서비스 대가 산정 모델-전문성 간의 관계 분석결과

종속변수	독립변수	비표준화 계수		표준화 계수	*t*	*p*	*VIF*
		B	표준오차	*β*			
전문성	(상수)	27.787	5.968		4.656	0.000	
	보안성지속대가	0.283	0.154	.207	1.841	.069	1.109
	위험관리대가	0.095	0.177	.060	0.535	.594	1.109
	F=1.696(p=.190), R^2=.039, $_{adj}R^2$=.016, $D-W$=1.725						

*p<.05, **p<.01, ***p<.001

[표 Ⅲ-23]과 같이 회귀분석 결과, 정보보호대가 모델 적용의 회귀모형의 적합도는 F=1.696, p=.190으로 유의수준 5%보다 높아서 유의하지 않은 것으로 나타났으며, 회귀모형의 설명력은 약 1.6%(수정된 R제곱은 1.6%)로 나타났다(R^2=.039, $adjR^2$=.016). 한편, 잔차의 독립성 여부를 판단하기 위해 측정한 결과, Durbin-Watson 통계량은 1.725로 2에 근사하므로 잔차의 독립성 가정을 위배하지 않는 것으로 평가되었고, 다중공선성 문제여부를 판단하기 위한 분산팽창지수(VIF)도 보안성 지속 대가 적용(VIF=1.109), 위험관리 대가 적용(VIF=1.109) 모두에서 10미만으로 나타나 다중공선성 문제가 없는 것으로 평가되었다.

회귀계수의 유의성을 검증한 결과, 정보보호서비스 대가 산정 모델의 세부 변

수인 보안성지속대가(β=.207, p=.069), 위험관리대가(β=.060, p=.594) 모두 변수의 유의수준 5%를 넘어서서 전문성에 유의하지 않은 것으로 보여 졌다. 즉, 정보보호서비스 대가 산정 모델 적용이 전문성에 직접적인 영향을 미치지 않는다는 것으로 평가되었다.

라. 정보보호서비스 대가 산정 모델 적용이 대응성에 미치는 영향

정보보호서비스 대가 산정 모델의 세부 변수인 보안성 지속 대가 적용, 위험관리 대가 적용이 대응성에 미치는 영향에 대해 다중회귀분석을 통해 검증한 결과는 [표 Ⅲ-24]와 같다.

[표 Ⅲ-24] 정보보호서비스 대가 산정 모델-대응성 간의 관계 분석결과

종속변수	독립변수	비표준화 계수		표준화 계수	*t*	*p*	*VIF*
		B	표준오차	*β*			
대응성	(상수)	1.159	1.051		1.102	0.273	
	보안성지속대가	0.938	0.027	.956	34.675***	<.001	1.109
	위험관리대가	-0.049	0.031	-.044	-1.587	.116	1.109
	F=687.414(p<.001), R^2=.942, $_{adj}R^2$=.941, $D-W$=1.900						

*p<.05, **p<.01, ***p<.001

[표 Ⅲ-24]와 같이 회귀분석 결과, 정보보호대가 모델 적용의 회귀모형의 적합도는 F=687.414, p<.001로 유의한 것으로 나타났으며, 회귀모형의 설명력은 약 94.1%(수정된 R제곱은 94.1%)로 나타났다(R^2=.942, $adjR^2$=.941).

한편 잔차의 독립성 여부를 판단하기 위해 측정한 결과, Durbin-Watson 통계량은 1.900으로 2에 근사하므로 잔차의 독립성 가정을 위배하지 않는 것으로 평가되었고, 다중공선성 문제여부를 판단하기 위한 분산팽창지수(VIF)도 보안성 지속 대가 적용(VIF=1.109), 위험관리 대가 적용(VIF=1.109) 모두에서 10미만으로

나타나 다중공선성 문제가 없는 것으로 평가되었다.

회귀계수의 유의성을 검증한 결과, 정보보호서비스 대가 산정 모델의 세부 변수인 보안성지속대가(β=.956 , p<.001)는 대응성에 긍정적인 영향을 미치는 것으로 보여 졌다. 즉, 보안성 지속 대가 적용이 증가할수록 대응성이 높아지는 것으로 평가되었다. 반면, 위험관리 대가(β=-.044, p=.116)는 유의하지 않은 것으로 나타났다. 즉, 위험관리대가 적용은 대응성에 직접적인 영향을 미치는 않는다는 것으로 검증되었다.

마. 정보보호서비스 대가 산정 모델 적용이 연속성에 미치는 영향

정보보호서비스 대가 산정 모델의 세부 변수인 보안성 지속 대가 적용, 위험관리 대가 적용이 연속성에 미치는 영향에 대해 다중회귀분석을 통해 검증한 결과는 [표 Ⅲ-25]와 같다.

[표 Ⅲ-25] 정보보호서비스 대가 산정 모델-연속성 간의 관계 분석결과

종속변수	독립변수	비표준화 계수		표준화 계수	*t*	*p*	*VIF*
		B	표준오차	*β*			
연속성	(상수)	19.464	3.761		5.175	0.000	
	보안성지속대가	-0.044	0.097	-.051	-0.451	.653	1.109
	위험관리대가	0.171	0.112	.173	1.536	.128	1.109
	F=1.662(p=.196), R^2=.038, $_{adj}R^2$=.015, $D-W$=2.309						

*p<.05, **p<.01, ***p<.001

[표 Ⅲ-25]와 같이 회귀분석 결과, 정보보호대가 모델 적용의 회귀모형의 적합도는 F=1.662, p=.196으로 유의수준 5%보다 높아서 유의하지 않은 것으로 나타났으며, 회귀모형의 설명력은 약 1.5%(수정된 R제곱은 1.5%)로 나타났다(R^2=.038, $adjR^2$=.015). 한편, 잔차의 독립성 여부를 판단하기 위해 측정한 결과,

Durbin-Watson 통계량은 2.309로 2에 근사하므로 잔차의 독립성 가정을 위배하지 않는 것으로 평가되었고, 다중공선성 문제여부를 판단하기 위한 분산팽창지수(VIF)도 보안성 지속 대가 적용(VIF=1.109), 위험관리 대가 적용(VIF=1.109) 모두에서 10미만으로 나타나 다중공선성 문제가 없는 것으로 평가되었다.

회귀계수의 유의성을 검증한 결과, 정보보호서비스 대가 산정 모델의 세부 변수인 보안성지속대가(β=-.051, p=.653), 위험관리대가(β=.173, p=.128) 모두 변수의 유의수준 5%을 넘어서서 연속성에 유의하지 않은 것으로 보여 졌다. 즉, 정보보호서비스 대가 산정 모델 적용이 연속성에 직접적인 영향을 미치지 않는다는 것으로 평가되었다.

바. 정보보호서비스 대가 산정 모델 적용이 정보보호서비스 품질에 미치는 영향

정보보호서비스 대가 산정 모델 적용이 정보보호서비스 품질에 미치는 영향에 대해 검증한 결과를 정리하면, 정보보호서비스 대가 산정 모델의 변수 중 보안성 지속 대가 적용은 신뢰성과 대응성에 긍정적인 영향을 미치는 것으로 나타났고, 위험관리 대가 적용은 대응성에 긍정적인 영향을 미치는 것으로 나타났다. 이는 정보보호서비스 대가 산정 모델 적용이 증가될수록 신뢰성이 높아지며, 보안성 지속 대가 적용이 증가될수록 대응성이 높아지는 것으로 판단된다. 즉, 정보보호서비스 대가 산정 모델 적용이 정보보호서비스 품질에 부분적으로 긍정적인 영향을 미치는 것으로 검증되었으며, 정보보호서비스 대가 산정 모델 적용이 증가될수록 정보보호서비스 품질도 부분적으로 높아진다는 의미이다.

[표 Ⅲ-26] 가설 2 검증 결과

가설	내용		결과
가설 2	**정보보호서비스 대가 산정 모델 적용이 정보보호서비스에 미치는 영향**		**부분 채택**
		보안성 지속 대가가 신뢰성에 미치는 영향	**채택**
		보안성 지속 대가가 반응성에 미치는 영향	기각
		보안성 지속 대가가 전문성에 미치는 영향	기각

가설	내용		결과
		보안성 지속 대가가 대응성에 미치는 영향	**채택**
		보안성 지속 대가가 연속성에 미치는 영향	기각
		위험관리 대가가 신뢰성에 미치는 영향	기각
		위험관리 대가가 반응성에 미치는 영향	기각
		위험관리 대가가 전문성에 미치는 영향	기각
		위험관리 대가가 대응성에 미치는 영향	**채택**
		위험관리 대가가 연속성에 미치는 영향	기각

(3) 정보보호서비스 대가 산정 모델 적용이 정보보호 성과에 미치는 영향

정보보호서비스 대가 산정 모델 적용이 정보보호 성과에 미치는 영향에 대한 검증은 독립변수인 정보보호서비스 대가 산정 모델의 세부 변수인 보안성 지속 대가, 위험관리 대가가 종속변수인 정보보호 성과의 세부변수인 재무적 성과, 비재무적 성과에 어떠한 영향을 미치는지 검증하기 위해 다중회귀분석을 한 결과 다음과 같이 보여 졌다.

가. 정보보호서비스 대가 산정 모델 적용이 재무적 성과에 미치는 영향

정보보호서비스 대가 산정 모델의 세부 변수인 보안성 지속 대가 적용, 위험관리 대가 적용이 재무적 성과에 미치는 영향에 대해 다중회귀분석을 통해 검증한 결과는 [표 Ⅲ-27]과 같다.

[표 Ⅲ-27] 정보보호서비스 대가 산정 모델-재무적 성과 간의 관계 분석결과

종속변수	독립변수	비표준화 계수		표준화 계수	*t*	*p*	*VIF*
		B	표준오차	*β*			
재무적	(상수)	1.154	1.548		0.745	0.458	

종속변수	독립변수	비표준화 계수		표준화 계수	t	p	VIF
		B	표준오차	β			
성과	보안성지속대가	0.948	0.040	.934	23.785***	<.000	1.109
	위험관리대가	-0.020	0.046	-.017	-0.436	0.664	1.109
	F=317.474(p<.001), R^2=.883, $_{adj}R^2$=.880, $D-W$=1.963						

*p<.05, **p<.01, ***p<.001

[표 Ⅲ-27]과 같이 회귀분석 결과, 정보보호대가 모델 적용의 회귀모형의 적합도는 F=317.474, p<.001로 유의한 것으로 나타났으며, 회귀모형의 설명력은 약 88.0%(수정된 R제곱은 88.0%)로 나타났다(R^2=.883, $adjR^2$=.880).

한편 잔차의 독립성 여부를 판단하기 위해 측정한 결과, Durbin-Watson 통계량은 1.963으로 2에 근사하므로 잔차의 독립성 가정을 위배하지 않는 것으로 평가되었고, 다중공선성 문제여부를 판단하기 위한 분산팽창지수(VIF)도 보안성 지속 대가 적용(VIF=1.109), 위험관리 대가 적용(VIF=1.109) 모두에서 10미만으로 나타나 다중공선성 문제가 없는 것으로 평가되었다.

회귀계수의 유의성을 검증한 결과, 정보보호서비스 대가 산정 모델의 세부 변수인 보안성지속대가(β=.934 , p<.001)는 재무적 성과에 긍정적인 영향을 미치는 것으로 보여 졌다. 즉, 보안성 지속 대가 적용이 증가할수록 재무적 성과가 높아지는 것으로 평가되었다.

나. 정보보호서비스 대가 산정 모델 적용이 비재무적 성과에 미치는 영향

정보보호서비스 대가 산정 모델의 세부 변수인 보안성 지속 대가 적용, 위험관리 대가 적용이 비재무적 성과에 미치는 영향에 대해 다중회귀분석을 통해 검증한 결과는 [표 Ⅲ-28]과 같다.

[표 Ⅲ-28] 정보보호서비스 대가 산정 모델-비재무적 성과 간의 관계 분석결과

종속변수	독립변수	비표준화 계수		표준화 계수	t	p	VIF
		B	표준오차	β			
비재무적 성과	(상수)	1.661	1.023		1.623	.108	
	보안성지속대가	0.214	0.026	.668	8.123***	<.001	1.109
	위험관리대가	-0.031	0.030	-.084	-1.019	.311	1.109
	F=40.048(p<.001), R^2=.488, $_{adj}R^2$=.476, $D-W$=1.577						

*p<.05, **p<.01, ***p<.001

[표 Ⅲ-28]과 같이 회귀분석 결과, 정보보호대가 모델 적용의 회귀모형의 적합도는 F=40.048, p<.001로 유의한 것으로 나타났으며, 회귀모형의 설명력은 약 48.8%(수정된 R제곱은 48.8%)로 나타났다(R^2=.488, $adjR^2$=.476).

한편 잔차의 독립성 여부를 판단하기 위해 측정한 결과, Durbin-Watson 통계량은 1.577로 2에 근사하므로 잔차의 독립성 가정을 위배하지 않는 것으로 평가되었고, 다중공선성 문제여부를 판단하기 위한 분산팽창지수(VIF)도 보안성 지속대가 적용(VIF=1.109), 위험관리 대가 적용(VIF=1.109) 모두에서 10미만으로 나타나 다중공선성 문제가 없는 것으로 평가되었다.

회귀계수의 유의성을 검증한 결과, 정보보호서비스 대가 산정 모델의 세부 변수인 보안성지속대가(β=.668, p<.001)는 비재무적 성과에 긍정적인 영향을 미치는 것으로 보여 졌다. 즉, 보안성 지속 대가 적용이 증가할수록 비재무적 성과가 높아지는 것으로 평가되었다.

다. 정보보호서비스 대가 산정 모델 적용이 정보보호 성과에 미치는 영향

정보보호서비스 대가 산정 모델 적용이 정보보호 성과에 미치는 영향에 대해 검증한 결과를 정리하면, 정보보호서비스 대가 산정 모델의 변수 중 보안성 지속

대가 적용은 정보보호성과의 세부 변수인 재무적 성과와 비재무적 성과에 긍정적인 영향을 미치는 것으로 나타났다. 이는 보안성 지속 대가 적용이 증가될수록 정보보호성과가 높아지는 것으로 판단된다. 즉, 정보보호서비스 대가 산정 모델 적용이 정보보호 성과에 부분적으로 긍정적인 영향을 미치는 것으로 검증되었으며, 정보보호서비스 대가 산정 모델 적용이 증가될수록 정보보호 성과도 부분적으로 높아진다는 의미이다.

[표 Ⅲ-29] 가설 3 검증 결과

가설	내용		결과
가설 3	**정보보호서비스 대가 산정 모델 적용이 정보보호성과에 미치는 영향**		**부분 채택**
		보안성 지속 대가가 재무적 성과에 미치는 영향	**채택**
		보안성 지속 대가가 비재무적 성과에 미치는 영향	**채택**
		위험관리 대가가 재무적 성과에 미치는 영향	기각
		위험관리 대가가 비재무적 성과에 미치는 영향	기각

Ⅳ. 현행 정보보호서비스 대가 산정 모델의 문제점 및 개선방안

1. 문제점

1) 현행 정보보호서비스 대가 산정 모델의 문제점

정보보호서비스 대가 산정 모델은 정보보호 기술 및 정보보호제품을 활용하여 제공하는 서비스에 대해 적정한 대가를 지불하고자 서비스 유형에 따른 비용을 산정하는 방식을 말한다.

현행 정보보호서비스 대가 산정 방식은, 한국SW산업협회에서 매년 발표하는 “SW사업 대가 산정 가이드”를 살펴보면, 정보보호제품에 대한 보안성 지속 서비스 대가는 보안서비스별 수행기준 포인트제(SSP) 기반의 요율제 방식, 보안관제 및 보안컨설팅 서비스 대가는 투입공수(Man Month) 방식으로 산정할 수 있도록 규정하였다. 요율제 방식은 정보보호제품에 대한 도입단가에 일정비율(8%)을 곱하여 산정하는 방식이며, 투입공수는 SW 기술자 등급에 따라 사업에 참여하는 비중을 기준으로 노임단가를 적용하여 직접인건비, 기술료, 제경비 등을 산정하여 적용하는 방식이다. 하지만, 요율제 방식은 보안업데이트, 패턴 업데이트, 보안취약점 진단 및 조치 등 제품에 대한 고유의 보안성을 유지하고자 할 경우 적합하나, 위험분석 관리나 기술자문, 모의훈련, 보안인증 유지 등 부가서비스에 대한 비용 산출에는 적합하지 않으며, 제조사에서 상용 SW의 업데이트와 보안업데이트를 구분하지 않고 통합하여 업데이트를 수행하고 있기 때문에 일반 유지보수 대가와 정보보호서비스 대가가 중복으로 산정되는 문제를 지니고 있다. 투입공수 방식은 서비스별 업무량에 따라 적정한 투입 인력수 산정이 어렵고, 고정비 방식으로 서비스 중요도에 따른 복잡성과 수행규모 등이 대가에 반영되지 않기 때문에 객관적이고 합리적인 대가 산정의 기준이 되지 못한다.

제주지역의 S기관 적용 사례를 살펴보면, 정보보호서비스에 대한 S-SLA 기준을 근거로 요율제 방식과 투입공수방식을 혼합 적용하였다. 이 기관은 정보보호

제품에 대한 보안업데이트, 패턴 및 패치 업데이트, 제품의 장애/자원관리 등 보안성 지속서비스 중 일부 서비스에 대해 요율제 방식을 적용하였고, 정보보호서비스를 기획서비스, 위험분석관리, 운영, 지원서비스로 재분류하여 투입공수방식과 고정가격방식을 혼합 적용하였다. 고정가격방식은 정보보호서비스 유형별로 서비스 수준을 정하고 공급자와 수요기관 간의 S-SLA 계약을 통해 합의된 고정가격을 지급하는 방식이다. 또한, 이 기관에서는 정보보호서비스 목표 및 활동과 관련된 서비스 측정 항목과 기준을 사전에 마련하여 공급자와 서비스 수준 협약 체계를 하여 월별로 S-SLA 측정을 통해 결과를 서비스 품질에 대한 대가에 곱하여 인센티브 또는 패널티를 부여하고 있다. 하지만, 보안서비스와 보안위협도의 특성 상 S-SLA 측정기준을 명확하게 규정하기가 어렵고, 기준이 투입량에 따르다 보니 서비스 품질에 대한 보장이 어렵다.

[표 Ⅳ-1] 현행 정보보호서비스 대가 모델 비교

구분		SW사업대가 산정가이드	국가 및 지자체 사례 (조달청 입찰정보 분석)	제주지역의 S기관 사례
정보보호 서비스 유형별 대가 산정 방식	보안성 지속 서비스	요율제	-	요율제 + SLA
	정보보안 관리체계 서비스	-	-	투입공수 + 고정가격방식
	보안관제서비스	투입공수 (Man Month)	투입공수 (Man Month)	투입공수 (Man Month)
	보안컨설팅서비스	투입공수 (Man Month)	투입공수 (Man Month)	투입공수 (Man Month)

2) 정보보호서비스 대가 산정 모델 적용 관련 법제의 문제점

정보보호서비스 품질에 대해 대가로 산정하기 위한 기준의 GAP이 공급자인 정보보보업계와 수요자인 공공기관 간의 차이가 크다보니 현실적으로 정착하는데 큰 걸림돌이 되고 있다. 이를 개선하기 위해 현재 정보보호 산업 진흥에 관한

법률 제10조에 ‘정보보호서비스 대가를 적정하게 지급하도록 노력해야 한다고’ 규정하고 있지만, 권고수준의 규정이어서 이를 적용하고자 하는 공공기관은 많지 않다.

[표 Ⅳ-2] 정보보호서비스 대가 산정 모델 적용 관련 주요 법제 현황

구분	상세내용
정보보호산업의 진흥에 관한 법률	제10조(정보보호제품 및 정보보호서비스의 대가) ① 공공기관등은 정보보호사업의 계약을 체결하는 경우 정보보호산업의 발전과 정보보호제품 및 정보보호서비스의 품질보장을 위하여 적정한 수준의 대가를 지급하도록 노력하여야 한다.
정보통신기반 보호법	적용 되지 않음

3) 대가 모델 적용 유인책 및 서비스 품질 검증체계 부재의 문제점

공공기관이 자발적으로 정보보호서비스 대가 산정 모델 도입을 유도하기 위한 ‘정보보호 적용 인센티브’를 마련할 필요가 있다. 또한, 공급자가 제공하는 정보보호서비스에 대한 품질 수준이 지급 대가 수준에 적합한지를 국가 공인 평가기관을 통해 보다 객관적이고 공정한 평가하여 인증을 할 필요가 있다.

[표 Ⅳ-3] 현행 지방자치단체 합동평가 주요항목

분야	평가항목
평화와 번영의 한반도	・관리적 정보보안 역량 개선율 ・사이버위기대응 역량 개선율 ・기술적 정보보안 역량 개선율

2. 개선방안

정보보호서비스 대가 산정 모델이 국가 및 공공기관에 적용될 수 있도록 다음과 같이 효율적인 수행방안을 제시한다. 먼저, 정보보호서비스 활동의 특성과 유형을 고려한 정보보호서비스 대가 산정 모델 개선 방안을 제시한다. 또한 공공기관의 정보보호서비스 수준을 정량적으로 측정하고, 수행실적을 평가하여 미흡한 부분을 개선함으로써 정보보호서비스 수준과 운영관리의 품질을 보장하는 보안서비스 및 운영관리 수준 협약(S-S/OLA ; Service and Operational Level Agreement of Security) 적용방안을 제시한다. 마지막으로, 국가 및 공공기관이 정보보호서비스 대가 산정 모델 적용을 자발적으로 유도하기 위한 법제도 개선, 인센티브 부여, 서비스 품질에 대한 검증체계 방안을 제시한다.

1) 정보보호서비스 대가 산정 모델의 개선방안

정보보호서비스 대가 산정 모델은 공급자가 제공하는 정보보호서비스 수준과 제공량에 따라 대가를 차등 적용하여야 하는데, 기존의 요율제 방식과 투입공수(M/M) 방식은 일률적인 산정방식이어서 서비스 품질을 측정하는데 어려움이 있다. 이러한 문제점을 해결하기 위하여 정보보호서비스 활동의 특성과 유형을 고려한 정보보호서비스 대가 산정 모델 개선 방안을 다음과 같이 제시한다.

첫 번째, 정보보호제품에 대한 보안업데이트, 정보보호정책관리, 사고 분석 및 위협분석, 각종 보안성 인증 유지, 보안기술 자문 등 보안성 지속 서비스 대가는 서비스 활동유형별 포인트제 기반의 요율제 방식보다는 보안서비스 측정 및 차지백(S-M&C : Metering and Chargeback of Security Service) 방식을 적용하는 것을 제시한다. S-M&C 방식은 공급자가 수요기관에 정보보호서비스를 제공한 양을 측정하여 이를 근거로 서비스 대가를 산출하여 지불하는 방식이다. S-M&C 방식은 포인트제 기반의 요율제 방식보다 정보보호서비스 활동과 수준을 객관적으로 측정하여 적절한 대가를 산정할 수 있는 장점을 지니고 있다. 이를 위해서는 정보보호제품에 대한 보안성 지속서비스이기 때문에 정보보호제품

의 보안성 지속서비스 적용범위를 [표 Ⅳ-4]와 같이 개선할 필요가 있다.

[표 Ⅳ-4] 정보보호제품의 보안성 지속서비스 적용범위 개선(안)

항목	현행 서비스 내용	개선(안)
보 안 업데이트	· 룰 패턴 및 시그니처 업데이트 · IT환경 변화에 대한 패치(신규 OS, 표준, 시스템 등)	· 룰 패턴 및 시그니처 업데이트(유지) · IT환경 변화에 대한 일반 패치 업데이트는 상용 SW업데이트와 중복부분 제거(신규 OS, 표준, 시스템 등)
정보보호정책 관리	· 이용자 환경에 따른 정보보호 정책 수립 및 변경	· 정보보호 운영·지원서비스로 통합
사고분석 및 위협분석	· 사전/사후 침해사고 대응 · 제품군별 위협 분석 보고서 등	· 제품별 보안취약점 진단 및 조치 서비스를 제외한 서비스는 정보보호 운영·지원 서비스로 통합
각종 보안성 인증 유지	· 보안적합성 검증, CC인증 등 각종 보안성 인증 유지	· 각종 보안성 인증유지는 제품 개발단계에서 행해지는 인증단계로 수요기관이 부담하는 것은 적합하지 않기 때문에 삭제
보안기술자문	· 각종 모의훈련 및 교육훈련 · 보안서비스 Help Desk 운영 · 각종 정보보안감사 지원 등	· 정보보호 운영·지원서비스로 통합

두 번째, 조직의 정보보호 기획, 위험분석관리, 위협분석관리, 보안 운영 및 대응, 지원서비스 등 정보보안 관리체계 서비스 대가는 투입공수방식과 고정가격방식보다는 투입공수에 의한 고정가격방식과 서비스 가격방식을 혼합한 고정 서비스 가격방식을 적용하는 것을 제안한다. 혼합 고정 서비스 가격 방식은 투입물에 의한 산정방식이 아니라, 정보보호서비스 품질 관점에서의 산정방식이다. 정보보호서비스 요소별 서비스의 품질 수준과 운영 수준에 대한 측정 항목과 기준을 제시하여 공급자와 수요기관이 정보보호 서비스 및 운영수준 계약(S-S/OLA :

Service and Operational Level Agreement of Security)을 체결하여 이를 기준으로 투입 인력의 수와 투입된 인력에 대한 등급, 등급별 노임단가 등의 정량적 수치를 기초로 기술료와 제경비, 직접인건비, 이윤 등을 반영하여 산출하는 방식이다. S-S/OLA는 공급자와 수요기관 간의 중요한 핵심요소이기 때문에, 정보보호 서비스 대가 산출과정에서 공급자와 수요기관 간의 충분한 협의과정을 거쳐야 한다.

[표 Ⅳ-5] 정보보호 서비스 및 운영수준(S-S/OLA) 측정지표(안)

구분		측정지표	비고
S-S LA	업데이트	보안 업데이트 적용기간	
		패치 및 패턴 적용기간	
	장애	장애복구 시간	
		동일 장애 누적 횟수	
	백업	보안로그 및 시스템 로그 백업 주기	
		로그 백업 보유기간	
	침해대응	침해 시도 및 탐지 대응 시한	
		침해 시도 및 탐지, 보안사고 대응기간	
		초동 대응 및 통보 시한	
		보안사고 통보 시한	
	보고서	보안 이벤트 모니터링 결과 보고서 주기	
		정보보호시스템 가용성 체크 보고서 주기	
		장애 통보 및 처리 보고서 주기 및 시한	
	접근통제	불법 침투 및 비인가 접근 차단율	
		불법 연결 차단 시한 등	
	지원	Help-Desk 응답시한	
		Help-Desk 고객만족도	
OLA	Plan	정보보호관리체계 영역별 범위 설정 적정성	
		위험분석 관리계획 수립 및 적정성	
		위협분석 관리계획 수립 및 적정성	
		보안운영, 대응, 지원서비스 계획 수립도	
		자산 식별 및 중요도 평가 계획 수립도	
		대책 선택의 적절성	
	Do	보안취약점 진단 및 조치 이행 적정성	
		위험분석 평가 구체성 및 이행 적정성	
		분야별 보안대책 명세 및 이행 구현도	

구분		측정지표	비고
		교육훈련 및 모의훈련 적정성	
		보안운영, 대응, 지원서비스 계획별 이행 구현도	
		침해사고관리, IT재해복구 등 비상계획 신속성	
	Check	정보보호사업 보안준수사항 및 위규사항 준수도	
		자체 내부 보안감사 수행도	
		정보보호서비스 요소별 품질 관리효과 평가도	
		평가결과 품질 수준 향상 노력도 및 관리체계 재검토	
		각종 보고서 관리체계 적정성 및 통제도	
	Act	개선사항 조치 이행도	
		각종 보고서 및 요구사항 반영도	
		보안사고 및 조치결과 공유도	
		모의훈련 결과 개선조치 이행도	
		보안취약점 진단 조치 이행도	
		보안운영, 대응, 지원서비스별 개선사항 조치도	
		Help-Desk 불만사항 개선도	
		신기술 및 정책 변화 적용도	

또한, 정보보안 관리체계 서비스 제공방식을 [표 Ⅳ-6]과 같이 유형별로 수요기관이 선택할 수 있도록 Option 선택방식으로 개선하여 선택된 서비스의 제공량에 따라 측정하는 S-M&C 방식으로 추가 가격 방식을 적용하는 것을 제안한다.

[표 Ⅳ-6] 정보보안 관리체계 서비스 제공 방식의 개선(안)

서비스 영역	주요 활동	제공방식
정보보호 관리체계 서비스	· 정보보호관리체계(ISMS-P) 구축 영역별 기획 · 정보보호서비스 영역별 품질 관리 및 개선 도출 · S-PDCA별 보안관리대책 수립 기획 등	기본 → Option
위험분석 관리서비스	· 정보자산 식별 및 중요도 평가 · 서버, 보안장비, DB, 네트워크, IoT 등 인프라 취약점 진단 · 웹 취약점 및 시큐어코딩 진단 · 보안취약점 진단결과에 따른 위험분석평가 및 보호대책 수립	기본 → Option

서비스 영역	주요 활동	제공방식
위협분석 관리서비스	· 외부로부터 침해 탐지 로그/패킷 수집 · 초동 분석결과를 기초로 한 보안로그 수집·분석 · 공격자의 정보, 침투시간, 공격방법, 취약점정보, 정보자산의 피해여부 등 피해규모 파악, 복구지원 · 유형별 대응 방안 전략 수립	기본 → Option
보안운영 서비스	· 정보보호시스템 운영, 장비 이벤트 및 로그 백업 · 서버, 보안장비, DB, 네트워크, IoT 등 IT 인프라의 정기/긴급 보안패치 및 릴리즈 · 정기점검 및 장애처리, 자산 관리 업무 · 주요 IT 인프라 가용성·무결성 체크 · 정보보호시스템 패턴 생성 및 변경관리 · 정보보호 교육 및 기술동향 자문 · 정보보호시스템 운영 및 가용성, 보안동향 등 시스템 분석보고서 작성/관리	기본 → Option
보안대응 서비스	· 사이버 침해 및 보안위협 모니터링/탐지·대응 조치·분석 · 악성코드 분석 및 유포지 차단 서비스 · 해킹메일 모의훈련 및 복구테스트 서비스 등	기본 → Option
보안지원 서비스	· PC 등 Endpoint 장비에 대한 보안진단 및 조치 지원 · 보안 관련 Help-desk 운영 및 응답지원 등 · 기술 자문, 보안 동향 보고서 제공 · 원격 지원 서비스, 방문 지원 서비스 등	기본 → Option

마지막으로, 보안 컨설팅 서비스와 관제서비스에 대한 대가는 혼합 고정 서비스 가격 방식(투입공수에 의한 고정가격방식 + 서비스 가격방식)을 적용하는 것을 제안한다.

[표 Ⅳ-7] 정보보호서비스 대가 산정 모델 개선(안)

구분		SW사업대가 산정가이드	제주지역의 S기관 사례	개선(안)
정보보호서비스	보안성 지속 서비스	요율제	요율제 + SLA	· S-M&C 방식
	정 보 보 안	-	투입공수 +	· 혼합 고정 서비스 가격

구분		SW사업대가 산정가이드	제주지역의 S기관 사례	개선(안)
유형별 대가 산정 방식	관리체계 서비스		고정가격방식	방식(투입공수에 의한 고정가격방식 + 서비스 가격방식) + Option 선택형 추가 가격 방식
	보안관제서비스	투입공수	투입공수	· 투입공수 + 서비스 가격방식
	보안컨설팅 서비스	투입공수	투입공수	· 투입공수 + 서비스 가격방식
대가 정산방식		-	S-SLA 측정결과에 따른 비용 제재/보상	· S-PDCA 기반의 S-S/OLA 측정 결과에 따른 대가 제재/보상 · S-Chargeback 방식의 사후 정산체계

2) 정보보호서비스 대가 산정 모델 정착을 위한 법제 개선방안

정보보호서비스 대가 산정 모델이 정착되려면, 현재 정보보호 산업 진흥에 관한 법률 제10조에 '정보보호서비스 대가를 적정하게 지급하도록 노력해야 한다고' 권고수준으로 규정되어 있는 것을 공공기관이 반드시 도입하도록 강제성을 띠도록 개정해야 한다. 또한, 이 제도를 보다 용이하게 도입하기 위해서는 정보통신기반보호법, 정보통신망 이용촉진 및 정보보호에 관한 법률, 전자정부법 등 타 법률에도 정보보호서비스 대가 산정 모델 적용에 대한 사항을 규정할 필요가 있다. 국가기관이나 지자체 등 공공기관에서 매년 예산 편성의 기준이 되는 기획재정부의 예산편성 지침에도 정보보호서비스 대가 산정 기준을 명확하게 제시되지 않고 있어 이에 따른 개선이 필요하다.

[표 Ⅳ-8] 정보보호서비스 대가 산정 모델 적용 관련 주요 법제 개선(안)

법제도명	현행	개선(안)	비고
정보보호산업의 진흥에 관한 법률	제10조(정보보호제품 및 정보보호서비스의 대가) ① 공공기관등은 정보보호사업의 계약을	제10조(정보보호제품 및 정보보호서비스의 대가) ① 공공기관등은 정보보호사업의 계약을	개정

법제도명	현행	개선(안)	비고
	체결하는 경우 정보보호산업의 발전과 정보보호제품 및 정보보호서비스의 품질보장을 위하여 적정한 수준의 대가를 지급하도록 노력하여야 한다.	체결하는 경우 정보보호산업의 발전과 정보보호제품 및 정보보호서비스의 품질보장을 위하여 **적정한 수준의 대가를 지급하여야 한다.**	
정보통신기반 보호법	제24조(기술개발 등)	제24조(기술개발 등) **③ 관리기관의 장은 정보통신기반시설의 정보보호사업의 계약을 체결하는 경우 정보보호산업의 발전과 정보보호제품 및 정보보호서비스의 품질보장을 위하여 적정한 수준의 대가를 지급하여야 한다.** **④ 제3항에 따른 비용의 지급 및 관리 등에 필요한 사항은 정보보호산업의 진흥에 관한 법률 제10조의 적용과 연계되도록 하여야 한다.**	신설

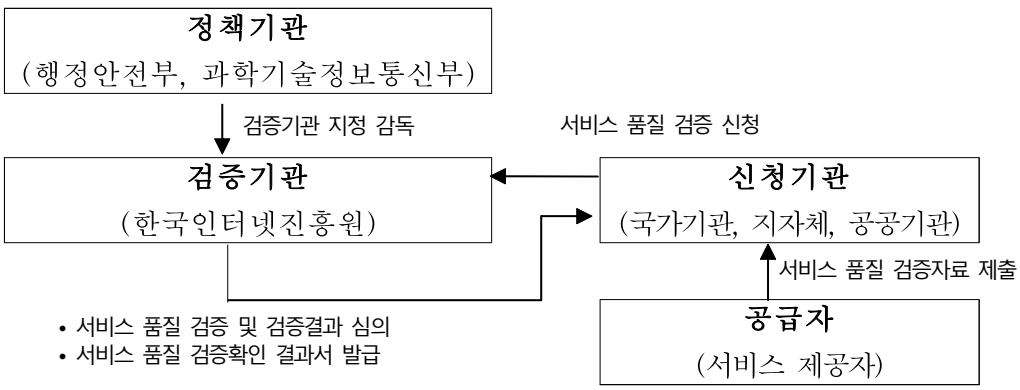
3) 정보보호 적용 인센티브 및 서비스 품질 검증체계 도입 제안

국가기관 및 지자체, 공공기관이 정보보호서비스 대가 산정 모델을 자발적으로 도입하기 위해서는 국가차원의 '정보보호 적용 인센티브제도'를 도입해야 한다. 지방자치단체인 경우, 매년 실시되는 지방자치단체 합동평가에 [표 Ⅳ-9]와 같이 '정보보호서비스 대가 산정 모델 적용 및 품질 개선율'에 대한 평가항목을 신설하여 도입 기관에 인센티브를 제공할 것을 제안한다. 이 평가를 통해 정보보호서비스 대가 산정 모델이 지방자치단체에 정착하는데 큰 영향을 미칠 것으로 판단된다.

[표 Ⅳ-9] 지방자치단체 합동평가 주요항목 개선(안)

분야	평가항목	
	현행	개선(안)
평화와 번영의 한반도	·관리적 정보보안 역량 개선율 ·사이버위기대응 역량 개선율 ·기술적 정보보안 역량 개선율	·관리적 정보보안 역량 개선율 ·사이버위기대응 역량 개선율 ·기술적 정보보안 역량 개선율 **·정보보호서비스 대가 산정 모델 적용 및 품질 개선율(신설)**

또한, 공급자가 제공하는 정보보호서비스에 대한 품질 수준이 지금 대가 수준에 적합한지를 한국인터넷진흥원 등 국가 공인 평가기관을 통해 보다 객관적이고 공정한 평가하여 인증을 할 필요가 있다. 행정안전부와 과학기술정보통신부가 정보보호서비스 품질 검증기관을 지정 감독권한을 지닌 정책기관으로, 한국인터넷진흥원과 TTA 등 검증기관에서 수요기관인 국가기관이나 공공기관에서 정보보호서비스 품질에 대한 검증 신청 시 객관적이고 체계적인 평가기준에 의하여 평가 후 서비스 품질 확인 결과서를 발급하는 검증체계를 구축할 것을 제안한다.



[그림 Ⅳ-1] 정보서비스 품질 검증체계 제시(안)

Ⅴ. 결 론

1. 연구결과 요약

본 연구는 기존의 문헌과 도입기관의 사례 분석을 토대로 정보보호서비스 품질, 정보보호서비스 대가 산정 모델 적용, 정보보호성과의 연구 모형을 도출하고 이에 따른 요소별 측정 항목을 도출한 후 정보보호서비스 대가 산정 모델 도입에 따른 적용이 정보보호성과에 어떠한 영향을 미치는지 살펴보고자 하였다.

앞 서 확인한 정보보호서비스 품질과 정보보호서비스 대가 산정 모델 적용이 정보보호성과에 미치는 영향에 관한 가설 검증 결과를 요약하면 [표 Ⅴ-1]과 같다.

[표 Ⅴ-1] 가설 검증 결과 요약(총괄)

가설	내용		결과
가설 1	**정보보호서비스 품질이 정보보호성과에 미치는 영향**		**부분 채택**
		신뢰성이 재무적 성과에 미치는 영향	기각
		반응성이 재무적 성과에 미치는 영향	기각
		전문성이 재무적 성과에 미치는 영향	기각
		대응성이 재무적 성과에 미치는 영향	**채택**
		연속성이 재무적 성과에 미치는 영향	기각
		신뢰성이 비재무적 성과에 미치는 영향	기각
		반응성이 비재무적 성과에 미치는 영향	**채택**
		전문성이 비재무적 성과에 미치는 영향	기각
		대응성이 비재무적 성과에 미치는 영향	**채택**

가설	내용		결과
		연속성이 비재무적 성과에 미치는 영향	기각
가설 2	**정보보호서비스 대가 산정 모델 적용이 정보보호서비스에 미치는 영향**		**부분 채택**
		보안성 지속 대가가 신뢰성에 미치는 영향	**채택**
		보안성 지속 대가가 반응성에 미치는 영향	기각
		보안성 지속 대가가 전문성에 미치는 영향	기각
		보안성 지속 대가가 대응성에 미치는 영향	**채택**
		보안성 지속 대가가 연속성에 미치는 영향	기각
		위험관리 대가가 신뢰성에 미치는 영향	기각
		위험관리 대가가 반응성에 미치는 영향	기각
		위험관리 대가가 전문성에 미치는 영향	기각
		위험관리 대가가 대응성에 미치는 영향	**채택**
		위험관리 대가가 연속성에 미치는 영향	기각
가설 3	**정보보호서비스 대가 산정 모델 적용이 정보보호성과에 미치는 영향**		**부분 채택**
		보안성 지속 대가가 재무적 성과에 미치는 영향	**채택**
		보안성 지속 대가가 비재무적 성과에 미치는 영향	**채택**
		위험관리 대가가 재무적 성과에 미치는 영향	기각
		위험관리 대가가 비재무적 성과에 미치는 영향	기각

첫 번째, 정보보호서비스 품질은 정보보호성과에 긍정적인 영향을 부분적으로 미치고 있음이 확인되었다. 정보보호서비스 품질의 측정항목 중 대응성은 정보보호성과 중 재무적 성과와 비재무적 성과의 향상에 직접적인 영향을 미치고, 반응성은 비재무적 성과 향상에 직접적인 영향을 미치고 있음을 알 수 있다.

두 번째, 정보보호서비스에 대한 적정한 비용 산정을 위한 정보보호서비스 대

가 산정 모델 적용은 정보보호서비스 품질 향상에 긍정적인 영향을 부분적으로 미치고 있음이 확인되었다. 정보보호서비스 품질의 측정항목 중 반응성, 전문성, 연속성을 제외하고, 보안성 지속 대가와 신뢰성, 대응성 간에 직접적인 영향이 있음을 보여주고 있으며, 위험관리대가는 신뢰성 간에 직접적인 영향이 있음을 보여 준다. 이 결과는 조직의 보안리스크가 발생하지 않도록 정보보호서비스에 대한 대응력과 신뢰성을 높이기 위한 보안성 지속서비스 비용과 보안이나 침해사고 대응능력에 대한 신뢰성을 높이기 위한 위험관리 비용에 대한 집중적인 적용이 정보보호서비스 품질 향상에 직접적인 영향을 미치고 있음을 알 수 있다.

마지막으로, 정보보호서비스 대가 산정 모델을 기관에 도입하여 이에 따른 적용이 정보보호성과에 긍정적인 영향을 부분적으로 미치고 있음이 확인되었다. 이 결과는 보안성 지속서비스 대가에 대한 적용이 재무적 성과와 비재무적 성과의 향상에 영향을 미치고 있지만, 위험관리 대가에 대한 적용은 정보보호성과에는 직접적인 영향을 미치지 못하고 있음을 알 수 있다.

현행 정보보호서비스 대가 산정 모델의 운영상 문제점에 대한 개선방안을 다음과 같이 제시하고자 한다.

첫 번째, 정보보호서비스 품질에 대해 대가로 산정하기 위한 기준의 GAP이 공급자인 정보보보업계와 수요자인 공공기관 간의 차이가 크다보니 현실적으로 정착하는데 큰 걸림돌이 되고 있다. 이를 개선하기 위해서는 현재 정보보호 산업진흥에 관한 법률 제10조에 '정보보호서비스 대가를 적정하게 지급하도록 노력해야 한다고' 권고 수준의 명문화한 것을 '정보보호서비스 대가를 적정하게 지급하도록 해야 한다'고 강제성이 있도록 개정해야 할 필요가 있다.

둘째, 공공기관이 자발적으로 정보보호서비스 대가 산정 모델 도입을 유도하기 위한 '정보보호 적용 인센티브'를 마련할 필요가 있다.

셋째, 국가 공인 평가기관을 통해 정보보호서비스 대가 적용 대비 서비스 품질 수준을 보다 객관적이고 공정한 평가하여 인증을 할 필요가 있다.

마지막으로 정보보호서비스 대가의 적용을 정보보호시스템 및 정보보호서비스에만 한정하지 말고 CCTV, IoT, 융합기술 등 정보화분야로 확대 적용하는 것이 보안위협으로부터 사전 예방 및 신속한 대응을 하는데 용이할 것이다.

2. 연구의 한계와 향후 연구과제

본 연구는 다음과 같은 한계점을 지니고 있다. 첫 번째, 정보보호서비스 대가 산정 모델을 적용한 기관이 한 곳밖에 없어서 도입기관을 대상으로 한 연구가 수행되었기 때문에 모든 공공기관에 적용하는데 한계가 있다. 향후에는 다수의 국가기관이나 공공기관을 대상으로 정보보호서비스 품질과 이에 따른 대가 산정 모델 효과를 파악하여 정보보호서비스 대가 산정 방식의 측정방법을 살펴볼 필요가 있다.

두 번째, 설문대상을 제주지역의 S기관 종사자와 그와 관련된 ICT 프로젝트를 수행하는 제주지역 ICT업체 종사자로 한정하여 연구가 이루어져서 회수된 설문지 샘플 수가 적다. 향후에는 설문대상을 확대하고, 많은 설문 샘플 수를 확보하여 명확하고 구체적인 연구를 할 필요가 있다.

세 번째, 정보보호서비스 대가 산정에 대한 연구에 대한 기존 문헌이 많지 않아 연구모형을 도출하는데 한계가 있었다. 정보보호서비스 품질에 관한 연구는 선행연구가 다수 이루어졌기 때문에, 향후에는 정보보호서비스 대가 산정 모델만을 구체적으로 연구할 필요가 있다.

본 연구는 위와 같은 한계점을 지니고 있지만, 지방자치단체의 정보보호서비스 대가 산정 모델 도입이 정보보호성과에 어떠한 영향을 미치는지에 대한 실증연구를 했다는 점, 현행 정보보호서비스 대가 산정 모델의 문제점과 개선방안을 도출했다는 점에서 기존 연구와 다른 관점에서의 연구이며, 향후 정보보호서비스 대가 산정 모델의 도입을 검토하는 국가 및 공공기관이나 공공과 정보보안 산업과의 상생할 수 있는 건전한 정보보호 산업의 생태계 조성과 관련된 정책 수립 시 유용한 참고자료로서 활용될 수 있는데 의미를 갖게 될 것으로 기대된다.

참 고 문 헌

1. 국내 문헌

경지훈, "IT 보안 서비스 품질의 측정 방법에 관한 연구", 2016., 한남대학교 대학원

곽동성, 강기두, "서비스품질의 측정에 관한 고찰", 經營學論集/24(1), 1997., 29-57, 中央大學校 經營硏究所

곽동성, 강기두, "서비스품질지각에 대한 개별구성요인의 영향력과 고객만족과의 관련성에 관한 연구 ", 韓日經商論集/15(-), 1998., 133-161, 韓日經商學會

김경규, 신호경, 박성식, 김범수, "정보자산보호성과가 조직성과에 미치는 영향에 관한 연구: 관리활동과 통제활동을 중심으로", Journal of Information Science Theory and Practice/40(3), 2009., 61-77, 한국과학기술정보연구원

김경선, "기술보호활동이 기업성과에 미치는 영향에 관한 실증연구", 2016., 성균관대학교 일반대학원

김대인, "금융기관 내부보안서비스품질과 내부고객만족 및 조직성과의 관계", 2019., 서울벤처대학원대학교

김상현, "PC보안 강화를 위한 취약점 점검항목 개선연구", 2019., 건국대학교 정보통신대학원

김진홍, "공공기관의 아웃소싱 보안관제 수준 측정지표에 관한 연구", 2014., 숭실대학교

김혜영, "기업의 보안환경이 보안 위험에 대한 낙관적 편견에 미치는 영향 연구", 2018., 중앙대학교 대학원

김홍진, "IT프로젝트팀의 투입요인이 프로젝트 성과에 미치는 영향에 관한 연구 ", 2018., 숭실대학교 대학원

김희망, "中小企業의 情報保護를 위한 效率的 支援方案", 2018., 성균관대학교

남기찬(Kichan Nam),김주희(Juhee Kim), "SLA의 수행 단계별 성숙도가 SLA 성과에 미치는 영향에 관한 연구", Journal of information technology

applications & management/14(1), 2007., 1-20, 한국데이타베이스학회
노춘민, "보안서비스품질이 서비스가치, 고객만족 및 재이용 의도에 미치는 영향", 2013., 경상대학교 경영대학원
문성계, "정보시스템의 효율적인 운영을 위한 SLA 평가지표 및 사용자 평가모델", 2010., 숭실대학교 대학원
박상수, "개인정보 유출과 정보전이가 기업가치에 미치는 영향에 관한 연구", 2018., 조선대학교 대학원
박성식, "기업의 정보자산 보호활동 실태 및 성과에 대한 영향 연구", 2009., 연세대학교 정보대학원
박유진,박은주,Park You-Jin,Park Eun-Ju, "A Study on an Estimation of Adjusted Coefficient for the Maintenance of Information Security Software in Korea Industry", 한국전자거래학회지/16(4), 2011., 109-123, 한국전자거래학회
박정국, "정보보호 관점에서 조직성과에 미치는 영향요인 분석", 2015., 동국대학교
박정한, "사이버위기 관리를 위한 정보보안 통합에 관한 연구", 2017., 공주대학교 대학원
백민정, "정보윤리활동이 정보보안성과에 미치는 영향에 관한 연구", 2010., 단국대학교 대학원
선한길, "국내 기업의 정보보호 정책 및 조직요인이 정보보호 성과에 미치는 영향", 2005., 국민대학교 대학원
손태현, "기업의 정보보호활동이 정보보안과 정보경영 성과에 미치는 영향", 2015., 명지대학교 대학원
심명섭, "IT 외주용역에서 보안수준 향상에 관한 실증적 연구", 2013., 건국대학교 정보통신대학원
안다솜,정지원,김영민,오상익,박남제, "소프트웨어 개발보안 관리체계에서의 교육과 인증체계 및 개선방안 제안", 한국정보과학회 학술발표논문집/2018(12), 2018., 941-943, 한국정보과학회
안선옥, "AHP기반 security ROI를 활용한 정보보호 적용성과 분석 연구", 2009., 고려대학교 컴퓨터정보통신대학원

오상익, 정원치, 박남제, "국가·공공기관 적용을 위한 정보보호관리체계 모델 개선 및 적용 방안", 한국정보과학회 학술발표논문집/2019(6), 2019., 1162-1164, 한국정보과학회

오상익, 박남제, "공공기관 정보보호서비스 대가 산정 모델의 개선 방안", 한국정보기술학회논문지/17(7), 2019., 123-131, 한국정보기술학회

우정훈, "SERVQUAL을 활용한 ISMS 성과측정 모형 개발에 대한 실증연구", 2015., 忠北大學校

이용우, "국가 주요 정보통신 기반시설의 사이버위협에 대한 보호대책에 관한 연구", 2011., 한남대학교 경영산업대학원

이재균, "연구자 중심의 보안관리체계 연구", 2018., 중앙대학교 대학원

이재훈, "개인정보보호 적용의 성과측정방법에 관한 연구", 2013., 중앙대학교 대학원

이현석, "ISMS-P의 外主人力 保安統制 方式 考察", 2019., 성균관대학교 정보통신대학원

임동성, "수탁사 개인정보 보호 관리 수준 점검 활동이 정보보안 성과에 미치는 영향에 관한 실증 연구", 2018., 전남대학교

장상수, "정보보호 관리체계 운용이 정보보호 성과에 미치는 영향에 관한 실증연구", 2011., 전남대학교 대학원

정유영, "정보 유출 사고가 기업 가치에 미치는 영향", 2015., 한양대학교 대학원

조연호, "情報保安솔루션 保安性 持續 서비스 對價 算定 政策 硏究", 2015., 高麗大學校 情報經營工學專門大學院

최명길,황원주,김명수, "정보보호정책의 성숙도에 영향을 미치는 요인에 관한 연구", 정보보호학회논문지/18(3), 2008., 131-142, 한국정보보호학회

최찬영, "금융기관을 위한 효율적인 사이버보안 적용 및 피해 산출 예측 모델 연구", 2019., 호서대학교 벤처대학원

홍기향, "정보보호 통제와 활동이 정보보호 성과에 미치는 영향에 관한 연구", 2004., 국민대학교 대학원

황성민, "보안관제에서의 보호동기요인이 자기효능감과 보안신뢰를 통해 정보보안성과에 미치는 영향", 2018., 건국대학교 정보통신대학원

2. 국외 문헌

Böhme, R., "Security Metrics and Security Investment Models", In IWSEC, pp. 10-24, 2010.

Cronbach, L.J., "Coefficient alpha and the internal structure of tests", Psychometrika, vol.16, 297-334., 1951

Hagen, L.K., "The bilingual brain: Human evolution and second language acquisition", Evolutionary Psychology, 6, 43 - 63., 2008

Parasuraman,A.,V.A.Zeithamland L.L.Berry(1985),"A Conceptual Model of Service Quality and Its Implications for Future Research,"Journal of Marketing,49(4),41-50.

Parasuraman,A.,V.A.Zeithamland L.L.Berry(1988),"SERVQUAL : A Multiple-Item Scale for Measuring Consumer Perceptions of ServiceQuality,"Journal of Retailing,64(1),12-40.

3. 기타

국가정보원,과학기술정통부,방송통신위원회,행정안전부,금융위원회, “2018 국가정보보호백서”, 2018.5

과학기술정보통신부,한국인터넷진흥원, "정보보호시스템 구축을 위한 실무가이드", 2018.6

과학기술정보통신부,한국인터넷진흥원, "주요정보통신기반시설 기술적 취약점 분석·평가방법 상세가이드", 2017.12

미래창조과학부, 한국인터넷진흥원, "지식정보보안 컨설팅전문업체 지정 등에 관한 고시 해설서", 2013.11

서귀포시, "2016~2018년 정보보호시스템 통합 유지관리 및 보안성 지속서비스 용역 완료보고서(통계요약)", 2018.12

서귀포시, "2017~2019년 2분기 사이버 침해 대응 분석 및 정보보호서비스 현황 통계분석 보고서(통계요약)", 2019.9

한국SW산업협회, "SW사업 대가산정 가이드(2019 개정판)", 2019.6

한국인터넷진흥원, "보안서비스에 대한 보안SLA의 효율적 운영방안 개발", KISA-WP-2010-0013, 2010.7

한국인터넷진흥원, "정보보호서비스 대가 산정 가이드", 2015.6

한국정보보호산업협회, "2018년 국내 정보보호산업 실태조사 보고서", 2018.12

한국정보보호산업협회, "일체형 정보보호제품의 보안성 지속서비스 원가분석", 방송통신정책연구 REF 17-방통(융합)-26, 2017.12., 과학기술정보통신부, 정보통신기술진흥센터

행정안전부, “2019년 지방자치단체 합동평가 지표 매뉴얼”, 2019.7

International Organization for Standardization(ISO)/International Electrotechnical Commission(IEC).(2016). Information security management(ISO/IEC Standard No. 27001).

NIST, https://www.researchgate.net/profile/Nicole_Radziwill/publication/318311904_Cybersecurity_Cost_of_Quality_Managing_the_Costs_of_Cybersecurity_Risk_Management/links/5962b402458515a35751ac26/Cybersecurity-Cost-of-Quality-Managing-the-Costs-of-Cybersecurity-Risk-Management.pdf?origin=publication_detail, pp. 189-197, Sep. 2010.

KISA 인터넷보호나라, https://www.krcert.or.kr/main.do

국가법령정보센터, https://www.law.go.kr

한국SW산업협회, https://www.sw.or.kr

정보보호산업진흥포털, http://www.kisia.or.kr

서귀포시, “http://www.seogwipo.go.kr”

[부록] 설문지

설 문 지

NO.			

지방정부의 정보보호서비스 대가 산정 모델 도입이 정보보호 성과에 미치는 영향에 대한 연구

안녕하십니까? 귀하와 귀사의 무궁한 발전을 기원합니다.

본 설문지는「지방정부의 정보보호서비스 대가 산정 모델 도입이 정보보호 성과에 미치는 영향에 대한 연구」를 목적으로 자료를 수집하기 위한 것입니다.

본 설문은 무기명으로 실시되며 응답하신 자료는 통계법 제13조에 따라 비밀보장과 익명성이 보장되어 이 연구를 위해서만 통계 처리되며, 순수한 학문적 목적으로만 사용되게 될 것입니다.

문항마다 특별한 정답이 따로 있는 것이 아니므로, 귀하의 생각이나 경험과 일치한다고 생각하는 그대로를 체크하시면 됩니다.

바쁘신 와중에도 소중한 시간을 내어 주신 여러분께 감사드리고 항상 행복하시길 기원합니다.

감사합니다.

2019년 9월

제주대학교 대학원 융합정보보안학협동과정

연 구 자 : 오 상 익
지도교수 : 박 남 제

응답대상 : 정보보호서비스 공급 및 수혜 경험이 있는 사람
문의사항 : 오 상 익(raitsu58@jejunu.ac.kr, 010- -)

※ 본 설문에 관한 문의사항이나, 응답결과의 송부는 위의 연락처로 주시기 바랍니다.
※ 설문지는 총 6페이지이며, 응답시간은 10~15분정도 소요됩니다.

설 문 응 답 방 법

※ 귀하의 생각과 가장 일치하는 항목에 '○' 또는 '√'표를 해주시기 바랍니다.

예시)

문항	영향정도						
	매우 그렇다	그렇다	약간 그렇다	보통	약간 그렇지 않다	그렇지 않다	전혀 그렇지 않다
1) 정보보호서비스 품질은 기관의 정보보호 성과 향상에 큰 도움이 된다.	√⑦	⑥	⑤	④	③	②	①

※ 위와 같이 응답하신 경우, 귀하는 정보보호서비스 품질이 기관의 정보보호성과 향상에 큰 도움이 된다고 생각하는 것을 의미합니다.

□ 정보보호서비스의 종류와 주요 활동은 아래와 같습니다.

서비스 영역	주요 활동
정보보호 관리체계 서비스	.정보보호관리체계(ISMS-P) 구축 영역별 기획 .정보보호서비스 영역별 품질 관리 및 개선 도출 .S-PDCA별 보안관리대책 수립 기획 등
위험분석 관리서비스	.정보자산 식별 및 중요도 평가 .서버, 보안장비, DB, 네트워크, IoT 등 인프라 취약점 진단 .웹 취약점 및 시큐어코딩 진단 .보안취약점 진단결과에 따른 위험분석평가 및 보호대책 수립
위협분석 관리서비스	.외부로부터 침해 탐지 로그/패킷 수집 .초동 분석결과를 기초로 상세로그 수집 및 정밀 분석 .공격자의 정보/시간, 공격방법, 보안취약점 등 침해 피해규모 파악, 복구지원 .유형별 대응 방안 전략 수립
보안운영 서비스	.정보보호시스템 운영, 장비 이벤트 및 로그 백업 .서버, 보안장비, DB, 네트워크, IoT 등 IT 인프라의 정기/긴급 보안패치 및 릴리즈 .정기점검 및 장애처리, 자산 관리 업무 .주요 IT 인프라 모니터링 및 가용성.무결성 체크 .정보보호시스템 패턴 생성 및 변경관리 .정보보호 교육 및 기술동향 자문 .정보보호시스템 운영 및 가용성, 보안동향 등 시스템 분석보고서 작성/관리
보안대응 서비스	.사이버 침해 및 보안위협 모니터링/탐지·초동 분석 .보안 위협 징후 실시간 대응 조치 및 보고 .악성코드 분석 및 유포지 차단 서비스 .해킹메일 모의훈련 및 복구테스트 서비스 등
보안지원 서비스	.PC 등 Endpoint 장비에 대한 보안진단 및 조치 지원 .보안 관련 Help-desk 운영 및 응답지원 등

□ 정보보호서비스 품질에 대한 대가 산정 모델은 아래와 같습니다.

산정형태	산출방식
요율방식	정보보호제품 도입단가 × (유지보수비율(%) + 정보보호서비스 대가 요율(%))
투입공수	투입인력 수 직접인건비 + 제경비 + 기술료 + 직접경비 + 부가가치세
License	제조사의 License 정책에 의한 연간 이용료 적용

Ⅰ. 다음은 “정보보호 서비스 품질 수준”에 대한 생각입니다. 평소 느끼시는 데로 해당된다고 생각하는 곳에 “√”하여 주십시오.

Ⅰ-1. “신뢰성”에 대한 질문입니다.

측정문항		매우 그렇다	그렇다	약간 그렇다	보통	약간 그렇지 않다	그렇지 않다	전혀 그렇지 않다
1	나는 정보보호서비스를 통해 조직의 정보보호 관리체계에 대한 신뢰가 향상되었다고 생각한다.	⑦	⑥	⑤	④	③	②	①
2	나는 정보보호서비스를 통해 내부 관리적, 기술적, 물리적 보안 규정에 대한 신뢰가 향상되었다고 생각한다.	⑦	⑥	⑤	④	③	②	①
3	나는 정보보호서비스를 통해 기관의 대외 신뢰도가 전반적으로 향상되었다고 생각한다.	⑦	⑥	⑤	④	③	②	①

Ⅰ-2. “반응성”에 대한 질문입니다.

측정문항		매우 그렇다	그렇다	약간 그렇다	보통	약간 그렇지 않다	그렇지 않다	전혀 그렇지 않다
1	나는 정보보호서비스 담당 직원이 고객 욕구 변화에 따른 신속한 대응능력을 갖추었다고 생각한다.	⑦	⑥	⑤	④	③	②	①
2	나는 정보보호서비스 담당 직원으로부터 빠른 기술지원을 받았다고 생각한다.	⑦	⑥	⑤	④	③	②	①
3	나는 정보보호서비스 담당 직원이 고객 불만에 대한 처리 속도가 빠르다고 생각한다.	⑦	⑥	⑤	④	③	②	①

Ⅰ-3. “전문성”에 대한 질문입니다.

측정문항		매우 그렇다	그렇다	약간 그렇다	보통	약간 그렇지 않다	그렇지 않다	전혀 그렇지 않다
1	나는 정보보호서비스 담당직원은 고객의 질문에 답변할 충분한 전문지식과 정보를 가지고 있다고 생각한다.	⑦	⑥	⑤	④	③	②	①
2	나는 정보보호서비스 담당직원이 보안 관련 법률 및 제도, 관리적, 물리적, 기술적 보호조치에 대한 전문지식을 보유하고 있다고 생각한다.	⑦	⑥	⑤	④	③	②	①
3	나는 정보보호서비스를 통해 위험분석 및 평가의 적절한 업무 수행이 가능해졌다고 생각한다.	⑦	⑥	⑤	④	③	②	①

Ⅰ-4. “대응성”에 대한 질문입니다.

측정문항		매우 그렇다	그렇다	약간 그렇다	보통	약간 그렇지 않다	그렇지 않다	전혀 그렇지 않다
1	나는 정보보호서비스를 통해 보안 사고를 예방하는데 효과적이라고 생각한다.	⑦	⑥	⑤	④	③	②	①
2	나는 정보보호서비스를 통해 보안사고 발생 시 신속한 대응이 가능하다고 생각한다.	⑦	⑥	⑤	④	③	②	①
3	나는 정보보호서비스를 통해 정보유출 등 보안사고가 감소되었다고 생각한다.	⑦	⑥	⑤	④	③	②	①

Ⅰ-5. “연속성”에 대한 질문입니다.

측정문항		매우 그렇다	그렇다	약간 그렇다	보통	약간 그렇지 않다	그렇지 않다	전혀 그렇지 않다
1	나는 정보보호서비스를 통해 정보보호교육 및 훈련 활동에 적극적 참여 및 지원이 증가하였다고 생각한다.	⑦	⑥	⑤	④	③	②	①
2	나는 정보보호서비스를 통해 정보보호에 대한 관심과 인식이 증가했다고 생각한다.	⑦	⑥	⑤	④	③	②	①
3	나는 정보보호서비스를 통해 지속적인 정보보호활동이 이루어지고 있다고 생각한다.	⑦	⑥	⑤	④	③	②	①

Ⅱ. 다음은 “정보보호 서비스 대가 모델 적용 수준”에 대한 생각입니다. 평소 느끼시는 데로 해당된다고 생각하는 곳에 “√”하여 주십시오.

Ⅱ-1. “보안성 지속 대가”에 대한 질문입니다.

측정문항		매우 그렇다	그렇다	약간 그렇다	보통	약간 그렇지 않다	그렇지 않다	전혀 그렇지 않다
1	나는 조직이 정보보호서비스 품질 향상을 위한 보안성 지속서비스 비용에 적용를 아끼지 않는다고 생각한다.	⑦	⑥	⑤	④	③	②	①
2	나는 조직이 정보보호서비스 품질 향상을 위해 서비스에 대한 적정한 대가를 산정하여 이에 대한 적용를 아끼지 않는다고 생각한다.	⑦	⑥	⑤	④	③	②	①
3	나는 정보보호서비스 품질 대가는 지금 내고 있는 금액 이상으로 거래가치가 있다고 생각한다.	⑦	⑥	⑤	④	③	②	①

Ⅱ-5. “위험관리 대가”에 대한 질문입니다.

측정문항		매우 그렇다	그렇다	약간 그렇다	보통	약간 그렇지 않다	그렇지 않다	전혀 그렇지 않다
1	나는 정보보호서비스 불만에 대한 개선비용에 적용를 아끼지 않는다고 생각한다.	⑦	⑥	⑤	④	③	②	①
2	나는 사이버 침해 대응 불만족에 대한 환불비용(손해배상 등)에 적용를 아끼지 않는다고 생각한다.	⑦	⑥	⑤	④	③	②	①
3	나는 하락된 기관의 대외 신뢰도 회복을 위한 관리비용에 적용를 아끼지 않는다고 생각한다.	⑦	⑥	⑤	④	③	②	①

Ⅲ. 다음은 “정보보호 성과”에 대한 생각입니다. 평소 느끼시는 데로 해당된다고 생각하는 곳에 “√”하여 주십시오.

Ⅲ-1. “재무적 성과”에 대한 질문입니다.

측정문항		매우 그렇다	그렇다	약간 그렇다	보통	약간 그렇지 않다	그렇지 않다	전혀 그렇지 않다
1	나는 정보보호서비스를 통해 보안사고 손실이 감소하였다고 생각한다.	⑦	⑥	⑤	④	③	②	①
2	나는 정보보호서비스를 통해 보안사고 처리비용(처리시간 단축 등)을 절감하였다고 생각한다.	⑦	⑥	⑤	④	③	②	①
3	나는 보안적용의 효율성이 증가되었다고 생각한다.	⑦	⑥	⑤	④	③	②	①

Ⅲ-2. “비재무적 성과”에 대한 질문입니다.

측정문항		매우 그렇다	그렇다	약간 그렇다	보통	약간 그렇지 않다	그렇지 않다	전혀 그렇지 않다
1	나는 정보보호서비스를 통해 경영진과 직원의 보안에 대한 관심과 인식이 증가되었다고 생각한다.	⑦	⑥	⑤	④	③	②	①
2	나는 정보보호서비스를 통해 기관의 보안 수준(무결성, 기밀성, 가용성)이 향상되었다고 생각한다.	⑦	⑥	⑤	④	③	②	①
3	나는 정보보호서비스를 통해 공급자와 협력자의 신뢰와 관계가 향상되었다고 생각한다.	⑦	⑥	⑤	④	③	②	①
4	나는 정보보호서비스를 통해 조직의 정보보호역량이 증가되었다고 생각한다.	⑦	⑥	⑤	④	③	②	①
5	나는 정보보호서비스를 통해 기관의 대외 이미지와 신뢰도가 증대되었다고 생각한다.	⑦	⑥	⑤	④	③	②	①

Ⅳ. 다음의 질문은 응답자의 개인적인 사항에 관한 것입니다. 해당되는 곳에 "√"하여 주시기 바랍니다.

1. 귀하의 성별은?

① 남자 ② 여자

2. 귀하의 연령은?

① 20대 ② 30대 ③ 40대 ④ 50대 이상

3. 귀하의 학력은?

① 고졸 ② 대졸(2년) ③ 대졸(4년) ④ 대학원졸

4. 귀하가 근무하고 있는 직종은?

① 공무원 ② ICT업체

5. 귀하의 직급은?

① 사원급 ② 임원급 ③ (공무원)5급 이상 ④ (공무원)6급
⑤ (공무원)7급 ⑥ (공무원)8급 이하

6. 귀하가 현재 근무하고 있는 직장의 근속년수는?

① 3년 미만 ② 3~5년 이하 ③ 5~10년 이하 ④ 10년 이상

귀하의 성실한 답변에 감사드립니다.

감사의 글

직장생활을 하면서 새로운 도전을 위해 석사학위과정에 문을 두드렸을 때가 엊그제 같은데 어느새 2년이라는 시간이 지나고 이 논문이 나오기까지 수많은 사람들의 도움을 받았습니다. 부족한 저를 이 자리까지 올 수 있게 도움을 주신 분들이 없었다면 논문이 나올 수 없었기에 이 자리를 빌려 감사의 마음을 전하고자 합니다.

먼저 부족한 저를 지금까지 아낌없는 믿음과 지도로 이끌어 주신 박남제 교수님께 진심으로 감사드립니다. 아직까지도 많이 부족하지만, 교수님의 가르침을 항상 마음속에 새기고 계속 발전하는 모습을 보여드리도록 노력하겠습니다.

또한, 논문심사 시 날카로운 지적과 따뜻한 조언을 해주신 변영철 교수님과 조정원 교수님께 진심으로 감사드립니다.

석사과정 동안 친하게 다가와 함께 고민하고 많은 도움을 주면서 즐거운 석사생활을 하게 해준 박정훈님, 정원치님, 정유진님, 김현주님, 최익서님, 고민수님 등 제주대학교 대학원 융합정보보안학협동과정 석사과정 원우들 모두에게도 감사하다는 말을 전하고 싶습니다.

직장생활 하면서 학업활동이 쉽지 않았음에도 옆에서 물심양면으로 도와주신 서귀포시 김영진 자치행정국장님, 정보화지원과 양은권 과장님, 김홍자 정보보호팀장님, 정보화지원과 직장 동료들 그리고 홍동국님, 양용석님, 정윤창님, 오영관님, 허용순님, 윤세명님, 김성철님, 김동은님, 오춘자님, 현수진님, 정종필님, 오승은님, 김미현님 그 외 지면상 올리지 못한 도움주신 많은 분들과도 진심으로 감사의 마음과 기쁨을 함께 나누고자 합니다.

언제나 한결같이 믿어주시고 아낌없는 사랑을 베풀어주신 부모님 그리고 인자하시고 정이 많으신 장인어른 이영교님, 장모님 홍복자님께도 감사의 마음을 전하며 기쁨을 함께 나누고자 합니다.

마지막으로 부족한 저에게 석사과정동안 불평불만 없이 학비를 지원해주면서도 항상 곁에서 배려와 용기를 북돋아주고 사랑의 힘이 되어준 이 세상에서 가장 사랑하는 아내 이정선님, 건강하게 잘 커준 큰아들 현석, 논문 작성기간 동안 “아빠는 축구 같이 해준다고 해놓고 안 해준다.”고 불평하던 밝고 올곧게 잘 자라준 막내아들 서준에게 지면으로나마 미안함과 고마움의 뜻을 전하며 그동안 노고에 조금이나마 보답하고자 하는 심정으로 이 논문을 바칩니다.

논문이 완성되기까지 주변에서 끝없는 격려와 도움을 주신 많은 분들께 이 글을 통해 감사의 마음을 전하며, 앞으로 더욱 발전할 수 있도록 끊임없이 노력하겠습니다. 감사합니다.

2019년 12월

오 상 익