JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 26, No. 4: 582~590, Apr. 2022

보안관제 업무 연관성 분석을 통한 ISMS-P 기반의 외주용역 관리 방법 제안

고도균[1] · 박용석[2*]

Proposal of ISMS-P-based outsourcing service management method through security control business relevance analysis

Dokyun Ko[1] · Yongsuk Park[2*]

[1]Graduate Student, Graduate School of Information Security, Sejong Cyber University, Seoul, 05000 Korea
[2*]Professor, Graduate School of Information Security, Sejong Cyber University, Seoul, 05000 Korea

요 약

사이버공격으로 인한 보안위협이 지속되고 있어 보안관제는 신속한 탐지와 대응을 위해 전문성을 가진 용역사업 형태로 주로 운용된다. 이에 따라 보안관제 용역 운영에 대한 다수의 연구가 진행되었다. 그러나 결과적인 관리, 지표, 측정 등의 연구로 업무과정에 대해 세부적으로 연구되지 않아 현장에서 업무 혼선이 빚어져 보안사고 대응이 원활하지 않다. 본 논문에서는 이런 문제점을 ISMS-P 기반의 용역관리 방법을 제시하고 그 방법을 업무 연관성 분석을 통해 시나리오기법과 ISMS-P 보호대책 요구사항 64개 항목의 맵핑(Mapping)으로 도출된 각 항목을 체크리스트화 하여 사용업체의 용이한 외주용역 관리 방법을 제안한다. 또한 주기적 보안준수 이행과 중장기적으로는 ISMS-P의 취득 및 갱신에 도움이 되고 관련 인원들의 보안의식 제고에도 기여할 것으로 기대한다.

ABSTRACT

As security threats caused by cyber attacks continue, security control is mainly operated in the form of a service business with expertise for rapid detection and response. Accordingly, a number of studies have been conducted on the operation of security control services. However, due to the research on the resulting management, indicators, and measurements, the work process has not been studied in detail, causing confusion in the field, making it difficult to respond to security accidents. This paper presents ISMS-P-based service management methods and proposes an easy outsourcing service management method for client by checklisting each item derived from the mapping of 64 items of ISMS-P protection requirements through business relevance analysis. In addition, it is expected to help implement periodic security compliance and acquire and renew ISMS-P in the mid- to long-term, and to contribute to enhancing security awareness of related personnel.

키워드 : 정보보호 컨설팅, 보안관제, ISMS-P, 외주용역, 업무영역

Keywords : Information Security Consulting, Security Control, ISMS-P, Outsourcing, Business Area

Received 7 February 2022, **Revised** 12 February 2022, **Accepted** 16 February 2022

*** Corresponding Author** Yongsuk Park (E-mail:yongspark@sjcu.ac.kr, Tel:+82-2-2204-8062)
Professor, Graduate School of Information Security, Sejong Cyber University, Seoul, 05000 Korea

Open Access **http://doi.org/10.6109/jkiice.2022.26.4.582** print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

기업들이 아웃소싱을 고려하는 이유를 간단히 설명하면 비용절감과 위험분산, 그리고 정보시스템의 성과 향상을 통해 기관운영의 생산성과 효율성을 극대화하여 고유의 핵심 업무에 집중할 수 있도록 지원하는데 있다. 기업 활동을 크게 관리활동과 서비스 활동으로 나누어 볼 때 이에 소요되는 비용 역시 관리비용과 서비스비용으로 구분할 수 있다. 만일 기업 내에서 관리하는 비용이 외부기관에서 관리하는 비용보다 많이 소요된다면 당연히 외부기관에 위탁해서관리하게 된다. 또 한편으로는 정보시스템 부서의 운영비용이 매년 20 ~ 30% 정도 증가하며, 정보기술의 변화속도가 너무나 급속하게 이루어지기 때문에 일반적으로 대규모의 투자자금이 소요되고, 선진 IT 기술을 적시에 받아들이고 유지하는 데는 자체 전산부서로는 불가능하기 때문에 이러한 정보기술을 자체적으로 보유 및 유지하는데 위험과 불확실성이 따르게 되므로 이를 외부 전문 업체에 위탁함으로써 위험을 어느 정도 감소시킬 수 있다.[1]

위와 같이 아웃소싱의 장점만이 있는 것은 아니다. 용역업체의 인력 이전으로 인한 기술 축적 미흡과 업무 인수인계 누락이 발생할 수 있으며, 위탁된 업무를 다시 타 업체 이전 및 내부에서 수용하기가 어려워진다. 그러나 가장 큰 문제는 많은 권한이 용역업체에 이관되거나 쉽게 활용할 수 있어 보안사고 유발 및 업체에 대한 통제력이 약해진다.

최근 다양한 보안위협을 예방, 탐지, 대응하기 위해 보안관제 서비스 용역사업이 증대되고 있다. 그에 따라 많은 보안관제 서비스 용역 운영의 효율성 증대, 수준평가 및 그 표준 지표 개발, 보안 강화 대책 수립, 관리방안 등 연구되고 있으나 사용업체와 외주용역의 업무 연관성에 대한 분석이 없어 제시된 방안이 외주용역만 기준을 두고 있어 법으로 정하는 기준의 기업, 기관 등에서 실시해야 하는 ISMS-P 효율적 운영에는 도움이 되지 못한다. 보안관제 업무는 더 중요해 지고 그 형태가 자체적 운영보다는 용역 서비스로 기울어지고 있고 사용업체에서 용역업체에게 요구하는 업무의 항목도 다양해졌다. 그 결과 업무별 애매모호한 영역으로 보안사항 미준수가 빈번해지고 해당 인력들의 보안의식 수준이 하향평준화와 보안 사고로도 이어질 수 있다.

본 논문에서는 이런 문제점을 업무 연관성 분석을 통해 확인 할 것이고 시나리오별 ISMS-P 보호대책 요구사항 64개 항목의 맵핑(Mapping)으로 도출된 각 항목을 체크리스트로 작성해 ISMS-P 기반의 보안관제 외주용역 관리 방법을 제안한다. 더불어 국내보안인증체계는 향후 그 적용대상을 넓혀갈 것으로 예상되어 보안관제 용역서비스를 이용하는 모든 기관 및 업체에 중장기적인 ISMS-P 활동에도 큰 도움이 될 것으로 기대한다.

Ⅱ. 관련 연구

보안관제는 사이버위협으로부터 신속히 대응하기 위한 수단으로 탐지, 분석, 대응, 보고의 단계로 업무가 수행된다. 이를 기반으로 그 운용의 형태가 자체 운용과 용역 운용으로 크게 분류되고 용역 운용이 파견과 원격의 형태로 다시 분류되게 된다. 자체 운용과 달리 용역서비스 형태는 내외부적 보안과 서비스 수준에 대한 관리가 필요하게 되었다. 이는 보안관제만이 아닌 IT기반 용역 전체에 해당되고 서비스의 대상만 다를 뿐, 밀접한 주제의 연구가 이어졌었다.

우선 정보시스템구축운영에 대한 보안관리강화에 관한 연구에서는 ISMS-P 보안대책 64개 항목을 이용한 용역을 효과적으로 관리하는 기준과 체크리스트를 제시하는 것을 목표로 하고 이를 사업의 각 단계별로 적용가능한 기술적·관리적 대응방안을 토대로 하여 기업의 보안관리 강화 활동이 적당한 것인지를 판단하기 위한 수준 진단 지표의 개발을 목적으로 한다.[1] 이와 비슷한 연구로 외주용역의 보안수준을 계량화하여 측정하는 모델을 설계하는 연구를 통해 그 신뢰성을 보장하고 기업 자체적인 외주용역의 보안수준을 평가 할 수 있는 방법이 될 수 있다고 제시한다. 그러나 기업의 업종, 규모 등 특징을 고려하지 않고 보안점검 가중치의 객관성이 부족한 한계는 존재한다.[2]

보안관제 분야에서는 세부 업무 항목에 관한 연구에서 센터의 관리 인력의 업무가 아닌 보안관제요원의 업무 항목만 도출하여 리스트화해 체계적인 성과 평가와 업무에 대한 프로세스 개선 지표로의 활용을 기대했다. 여건과 환경의 고려는 되지 않았지만 보안관제의 업무 영역에 대한 기준을 세부 항목으로 나누어 도출함으로서 그 평가와 개선에 기여하였고[3], ISO/IEC 27001과 K-ISMS를 참조한 공공기관의 아웃소싱 보안관제 수준

측정지표에 관한 연구에서 보안관제 담당 전문가와 보안관제 및 정보보호 컨설팅 전문 업체 전문가를 대상으로 내용 타당성에 대한 설문을 통해 신뢰성 있는 공공기관의 아웃소싱 보안관제 특성을 반영한 아웃소싱 보안관제 수준 측정 모델을 정립하였으며, 제시된 모델을 활용하여 공공기관의 아웃소싱 보안관제 수준을 자체적으로 평가할 수 있도록 하였다.[4]

앞선 관련 연구들은 관리 방안과 그 평가, 수준 측정 지표 등을 용역업체 기준으로 연구되었다. 그래서 사용업체와 용역업체의 업무 연관성을 고려하지 않고 한쪽 기준에만 치우쳐진 연구로 업무에 있어 각자의 역할에 혼선을 빚고 책임소지도 불명확해진다. 결국 용역 서비스 업무의 세부적인 과정들에 대해서는 명확한 연구가 되지 않고 업무 결과에 대한 연구만 되어 업무 중 보안 미준수 상황과 외주용역 관리 방법이 미흡하다는 한계가 있다.

Ⅲ. 보안관제 업무 연관성 분석

기본적인 보안관제 시스템의 업무 및 운영 활동은 통합보안관리시스템(ESM) 및 이·기종 보안시스템의 가용성, 성능, 용량 등을 체크하고 지속적으로 관리하며 장애 발생 요인을 최소화하여 보안관제 서비스의 안정성과 신뢰성을 강화할 수 있다.[5] 근래의 들어서는 빅데이터 기반 보안관제 시스템(SIEM)을 많이 운영 중이며, 그 외 대표적 보안관제 시스템의 종류와 그 기능 표 1을 통해 확인해 보았다.

Table. 1 Security Control System

System name	System function
DDoS	Detecting and blocking DDoS attacks
Firewall/WAF	External/internal communication control
IPS	Prevent harmful activities
Spam system	Blocking harmful emails
APT system	Intelligent persistent malicious behavior analysis/blocking
Virus system	Malicious code detection, treatment, deletion
SIEM	System log monitoring

세부 업무로는 보안시스템의 장애 대응 및 처리, 보안시스템의 가용성, 성능, 용량, 백업, 패치, 장애 관리 그리고 이벤트 분석/대응, 이벤트 분석보고, 정책 제안 및 변경 등이 있다. 아래의 표 2는 사용업체와 용역업체 간의 보안시스템별 업무연관성을 실제 각 시스템에서 모니터링 계정과 관리자 계정의 접속 및 운영을 통해 분석하여 그 영역을 분리 하여 표로 나타내었다.

Table. 2-a Work Relevance Analysis

System	Client	Outsourcing
DDoS	Report policy, filter policy, ACL policy, user policy, patch/backup/recovery policy, log linkage policy	Traffic/session monitoring, event monitoring, system resource monitoring, current visitor monitoring, raw data analysis, patch/backup/restore
Firewall/WAF	Filter policy, ACL policy, user policy, patch/backup/restore policy, log link policy, interface network policy	Traffic monitoring, allow/block policy check, raw data analysis, patch/backup/restore
IPS	Report policy, filter policy, ACL policy, user policy, patch/backup/recovery policy, log linkage policy	Event rule creation and change and reporting, event monitoring, system resource monitoring, current visitor monitoring, raw data analysis, patch/backup/recovery
Spam system	Report policy, filter policy, ACL policy, user policy, patch/backup/recovery policy, virus scan policy, system policy (sending time and retries, bulk mail, bulk mail)	Spam email content monitoring (normal email is confidential, so it is not possible), patch/backup/restore
APT system	Report policy, filter policy, ACL policy, user policy, patch/backup/restore policy, system interworking policy, attachment /malware download	Check threat detection history, check analysis results, check system log, perform patch/backup/restore

Table. 2-b Work Relevance Analysis

System	Client	Outsourcing
Virus system	Report policy, ACL policy, user policy, patch/backup/recovery policy, agent policy (OS, software, distribution policy, threat detection)	Agent status monitoring (policy, OS, software, threat detection), patch/backup/recovery
SIEM	Report policy, ACL policy, user policy, patch/backup/recovery policy, log linkage policy	Monitoring interlocking device logs, creating important log event rules for each device, performing patch/backup/restore

Ⅳ. 시나리오 구성

업무 연관성 분석[3]과 시나리오기법[1]을 통해 업무상 실제 발생할 수 있는 일들에 대해 총 10가지 시나리오를 선정하였다. 이 중 3가지는 주요 시나리오로 선정하여 ISMS-P 위반사항 분석[6]과 관련 사례와 함께 나타내 그 유효성을 입증 하고 그 외 7가지 기타 시나리오들을 통해 다양한 미래상황 예측으로 체크리스트 항목 도출의 근간이 되게 했다.

4.1. 주요 시나리오

주요 시나리오 3가지를 선정하여 그 상황을 작성하고 이를 ISMS-P의 보안대책 항목에 위반되는 사항을 확인했다. 또한 그에 따른 보안대책을 제시하고 사나리오별 상황과 유사한 실제 보안사고 사례를 통해 그 유효성을 입증한다.

4.1.1. 시나리오 1

메일과 관련된 상황으로 외주용역 업체가 사내 메일 내용 확인이 지속될 시 발생할 수 있는 보안사고이다. 실제 관련 보안사고인 2016년 LG화학의 결제대금 송금 피해[7]도 지속된 메일내용 노출이 원인이 되었다.

A업체는 현재 회사 내 정보보안을 위해 관제 및 유지보수 용역계약을 맺고 외부 인력들이 상주하여 업무수행 중이다. 최근 증가된 메일공격들로 인해 스팸차단 시스템에 많은 필터들이 적용되다 보니 잦은 오탐으로 내부 직원들의 업무에 차질이 빚어지고 담당자에게 항의하는 일들이 벌어진다. 이에 원활한 업무를 위해 용역업체 직원들에게 관리자 계정을 통해 차단된 메일을 요청 시 사용자에게 전달하게 하거나 의심되는 스팸메일에 대한 분석을 맡기게 된다. 그러나 문제는 권한이 차등된 협력사용 계정이 아닌 관리자 계정으로 관리하다 보니 메일을 통해 전해지는 내부의 중요문서, 거래내용, 개인정보 등 민감한 내용 및 자료들의 접근과 수집이 가능해지게 되었다.

문제는 직접적으로 내용을 캡처하거나 문서를 다운받아 유출하지 않아도 메일과 첨부문서 내용을 직접 확인한 용역업체 직원 김 씨가 사적인 자리에서 회사 일에 대한 이야기 중 자주 언급하게 되고 경쟁업체에 있던 김 씨의 친구 이 씨는 이 정보를 통해 A업체와의 경쟁에서 유리한 위치를 선점하고 A업체는 원인파악 조차 힘들어 억울하게 지속적인 피해를 입고 있다.

위 상황에서 인적보안, 외부자보안, 접근통제 항목에 대해 보안대책 위반이며 이에 대한 구체적 보안대책으로는 용역업체 직원에게 차등된 권한의 별도 계정으로 메일 내용확인과 스캔, 첨부파일다운 등 을 제한한다. 사용자 요청 시 메일 전달과 스팸메일 모니터링을 담당하고 첨부파일 분석이 필요할시 사용업체에서 다운로드하여 전달한다.

4.1.2. 시나리오 2

물리적으로 분리되지 않은 관리자 PC에 접근되는 상황으로 외주용역 업체에서 쉽게 접근하고 관리자 계정으로 작업할 시 발생할 수 있는 보안사고이다. 실제 관련 보안사고인 2016년 인사혁신처 무단침입 사건[8]은 물리적으로 분리는 되어있는 환경이었지만 일반인도 쉽게 접근할 수 있었다는 것이 원인이 되었다.

B업체는 원활한 사내·외 시스템의 서비스 운영관리 및 보안 관리를 위해 관리자 PC를 용역업체와 같은 공간에 두고 별도의 관리 없이 사용하게 하였다. 현재로서는 별도의 공간을 마련하고 출입통제에 대한 방안 도입이 어려운 상황으로 경영진들은 해당 사안에 대해 큰 관심 없이 승인을 하게 된다. 그로인해 시스템 운영 및 보안관리가 신속하고 효율적으로 수행된다고 생각했다. 물론 업무 담당자들도 편리한 업무로 만족하는 상황이다.

문제는 평소와 같이 업무 중 용역업체 박 씨는 대수롭지 않게 관리자 PC에 앉아서 방화벽 정책변경 작업을 위해 윈도우 로그인부터 방화벽 로그인까지 순차적으로 하고 작업도 마무리하게 된다. 그러나 통제되지 않은 일반사무실이기에 오픈된 공간이었고 내부에는 CCTV 녹화에 힘들기 때문에 이를 악용한 협력업체 정씨는 박 씨 뒤에서 관리자 계정을 훔쳐보고 DB서버로 가는 방화벽 필터를 삭제하고 퇴근 후 PC방에서 DB접속 후 개인정보를 탈취하여 다크웹(Dark Web)을 통해 판매하여 금전적 이득을 취하게 된다. 물론 다음날 방화벽 필터는 다시 되돌려 놓았고, 그가 퇴사한 후 B업체에서는 직원들의 개인정보가 유출된 것을 확인하지만 관리자 PC에서 관리자 계정으로 분리되지 않은 사무실 내에서의 사고라 수사가 쉽지 않은 상황이다.

위 상황에서 물리보안, 접근통제, 시스템 및 서비스 운영관리와 보안관리 항목에 대해 보안대책 위반이며 이에 대한 구체적 보안대책으로는 물리적으로 관리자

PC에 접근이 불가하게 해야 하고 출입통제시스템을 통해 출입자 확인 및 출입구 CCTV 녹화를 한다. 관리자 계정으로 작업이 필요시 작업자 이름과 그 작업이력과 접속로그를 기록 및 보관하고 사용업체 담당자의 확인이 필요하다.

4.1.3. 시나리오 3

보안시스템의 차단정책 변경에 관한 상황으로 이에 대한 관리자의 관리감독이 미흡할 시 발생할 수 있는 보안사고이다. 실제 관련 보안사고인 2021년 KT 유무선 네트워크 먹통 사고[9]도 작업 승인서 내용 불이행, 관리자 부재 등 관리감독의 미흡이 원인 되었다.

오랜 기간 동안 보안관제 용역서비스를 받아오던 C업체는 보안장비 차단정책에 대한 관리 및 설정을 용역업체에게 일임한 상태이고 고착화된 이런 업무형태로 인해 담당자들의 관심도 없는 상황이다.

용역업체 막내 최 씨는 업무를 시작한지 한 달이 막 되어갈 시점이었다. 선임근무자의 지시로 침입차단시스템(IPS)의 차단룰을 개발하여 평소대로 간단히 담당자에게 사내 메신저를 통해 간단히 적용 작업 공유를 하고 자신이 개발한 차단룰을 적용했다. 그 후 10분 뒤 C업체로 홈페이지에 접속할 수 없다는 수많은 전화가 오고 업무는 마비되게 된다. 단순 서버 문제라 생각한 담당자는 서버를 재기동 시켜보지만 별다른 효과가 없었고 이에 뒤늦게 시스템 로그 모니터링 시스템을 확인하여 IPS에서 홈페이지로 가는 패킷을 모두 차단한다는 것을 확인했다. 추가한 차단룰을 차단정책에서 제외하고 홈페이지 정상접속에 문제는 없었지만 언론 보도를 통해 C업체의 내부관리 문제 등 이미지에 큰 타격을 입게 되었다.

위 상황에서 시스템 및 서비스 운영관리 항목에 대해 보안대책 위반이며 이에 대한 구체적 보안대책으로는 보안시스템 차단정책을 변경하기 위해용역업체는 차단룰 개발 및 적용보고서를 작성하여 사용업체에게 승인 후 정책적용을 실시하고 사용업체는 보고서를 별도로 관리하고 담당자 및 책임자의 철저한 확인을 통해 용역업체에게 작업을 지시하고 그 이력을 기록한다.

4.2. 기타 시나리오

3가지 주요 시나리오만으로는 다양한 미래상황예측이 부족하다. 이에 7가지의 기타 시나리오를 통해 현재 문제점으로 인한 미래 상황 예측과 상황별 ISMS-P에서 요구하는 보안대책을 간략히 나타내어 다양한 상황의 보안 관리를 위한 체크리스트 항목 도출에 이용하였다.

4.3. 시나리오 4

인터넷 또는 보안시스템을 통해 악성코드 분석을 위해 파일 다운하여 업무 간 악성코드 감염, 전파 등 보안사고 발생

4.3.1. 보안대책

관련 업무를 위한 전용망, 전용PC, 가상환경 등을 별도로 구축하고 악성코드 분석을 실시하고 그 결과보고서를 확인 및 내부 전파한 다음 분석한 PC의 백신 치료 또는 가상환경 이미지 삭제 등 수행한다.

4.4. 시나리오 5

DDoS 침해사고 시 대응절차에 대한 문제로 대응시간 지연으로 대민서비스 장애 등 보안사고 발생

4.4.1. 보안대책

침해사고 발생에 대한 역할 및 책임을 명확히 하고 용역업체에서 탐지 및 보안장비 차단, ISP 업체 협조요청 등 대응 시 사용업체 담당자는 내부 유관부서 도움 요청, 상급기관 보고, 별도 구축된 대피소 우회 작업 등 실시한다.

4.5. 시나리오 6

패치/백업/복구 관련 시나리오로 백업 작업 및 보관 등을 용역 업체가 주로 작업하기 때문에 백업데이터 누락과 유출 등 보안사고 발생

4.5.1. 보안대책

책임자 및 담당자를 지정하고 관리대장을 기록하고 데이터 보관에 대해서는 물리적으로 떨어진 매체로 하고 그 접근을 제한한다. 백업의 복구에 대해서는 데이터를 담당자에게 요청하여 전달 받는다.

4.6. 시나리오 7

상급 또는 연계된 보안 네트워크를 통해 공유되는 차단룰의 적용 누락 및 내부 통신과의 마찰을 고려하지 않은 적용으로 침해사고와 통신장애 발생

4.6.1. 보안대책

용역업체에서는 누락을 방지하기 위해 일일보고서 등으로 관리하고 사용업체에서는 보고된 차단룰을 검토해 내부 통신에 이상 없으면 용역업체에게 작업권한을 승인하여 등록하게 한다.

4.7. 시나리오 8

백신에 탐지된 바이러스의 오판단 및 관련 파일을 직접 분석하다 감염, 전파 발생

4.7.1. 보안대책

바이러스 탐지되면 용역업체는 사용업체에게 보고 후 사용자에게 PC 분리 조치를 요청하고 백신 벤더(Vnedor)사에게 문의한다. 사용업체는 직접 분석 판단이 필요할 시 PC 회수 및 조사팀을 꾸려 조사 실시한다.

4.8. 시나리오 9

방화벽, IPS 등 차단장비의 로그의 유출로 유해 행위들이 우회되어 피해 발생

4.8.1. 보안대책

용역업체가 로그를 확인할 수 있어도 그 로그를 데이터로 다운받을 때는 관리자 계정을 통해 그 이력을 남기고 사용업체에게 승인을 받는다. 사용업체는 로그 데이터를 보관하고 폐기를 담당한다.

4.9. 시나리오 10

프로젝트 수행 인원의 퇴직이나 신규 투입 시 비밀유지서약서 및 개인정보보호서약서 누락으로 기밀 유출 시 법적 책임 또는 손해배상청구의 어려움 발생

4.9.1. 보안대책

용역 업체에서는 정보보호서약서 내용을 숙지하여 준수하고 사용업체에서는 인력의 입·퇴사 시 서약의 징구를 확인하고 안전한 곳에 보관한다.

Ⅴ. 체크리스트 도출과 활용방안

업무 연관성 분석과 시나리오들을 토대로 보안관제 업무영역 체크리스트를 그림 1의 ISMS-P 보안대책 요구사항 64개 항목[10]과 맵핑(Mapping)하여 생성한다. 이를 통해 해당 체크리스트의 신뢰성과 타당성을 보장할 수 있고 보안관제 외주용역 관리에 좀 더 용이성을 가질 수 있다. 또한 체크리스트로 지속적, 상시적 보안관리로 ISMS-P 기반의 보안의식제고와 보안사항 준수를 통해 향후 인증 취득 및 갱신에 소모되는 시간과 노력 등 소모되는 에너지를 아낄 수 있다.

2. Security measures requirements (64 items)	2.1 Policy, Organization, and Asset Management
	2.2 Human security
	2.3 Outsider security
	2.4 Physical security
	2.5 Authentication and Permission Management
	2.6 Access control
	2.7 Encryption Enforcement
	2.8 Information system introduction/ development security
	2.9 System and service operation management
	2.10 System and service security management
	2.11 Accident prevention and response
	2.12 disaster recovery

Fig. 1 ISMS-P Security Measure Requirements

표 2와 시나리오기법을 토대로 업무 영역을 사용업체와 용역업체로 분리하여 생성된 체크리스트를 표 3을 통해 확인 할 수 있다.

Table. 3-a Check List

Check Item	YES	NO (write down the reason)
1. Does the user actually supervise when working on patches/backups/recovery?		
2. Does the backup comply with the period and retention period? (Backup work is a outsourcing/data storage is a client		
3. After backup, was it stored in a physically separated place through a designated storage medium?		
4. When recovering a backup, does the outsourcing make a request through a statement of reason and approve it and take out data from the client?		
5. Does the outsourcing prepare management documents such as patches/backups/ recovery, and review and store them by the client?		
6. Is patch update management and work carried out by the outsourcing and the patch file storage by the client?		

Check Item	YES	NO (write down the reason)
7. Does the administrator's account only connect to the designated PC? (PC in charge of the client)		
8. Is the administrator's PC physically separated from the outsourcing?		
9. Are log monitoring and packet download done by the outsourcing, and are the main settings, policy application, user account settings and privileges restricted by the client when requested?		
10. Is the outsourcing suggesting addition or exclusion of the blocking policy, and is the operation carried out after the client review and approval (including permission approval for system operation)?		
11. Is the client configuring the PC and network for malicious code analysis, and the outsourcing establishing the environment such as virtual environment and vaccine in the PC?		

Table. 3-b Check List

Check Item	YES	NO (write down the reason)
12. For malicious code analysis, the outsourcing conducts analysis after prior report, and the client checks the PC when the analysis is completed?		
13. In the event of a DDoS accident, the outsourcing requests detection/blocking and cooperation from ISP companies, and the client requests internal related departments, reports to higher agencies, and detours from shelters?		
14. When using the spam blocking system, the outsourcing monitors and checks the spam status, and other tasks are working at the client due to the risk of internal confidentiality and personal information security accidents?		
15. Is the confidentiality pledge and personal information protection pledge managed and kept by the client, and the outsourcing is familiar with and complying with the contents?		

체크리스트와 시나리오의 적합성과 상호관계를 알아보기 위해 ISMS-P 보안대책 요구사항 항목과 시나리오의 연관성을 그림 2에 체크리스트와의 연관성을 그림 3으로 보여준다.

ISMS-P Security measures requirements	Scenarios
2.1 Policy, Organization, and Asset Management	8
2.2 Human security	1, 10
2.3 Outsider security	1, 10
2.4 Physical security	2
2.5 Authentication and Permission Management	9
2.6 Access control	1, 2
2.7 Encryption Enforcement	-
2.8 Information system introduction/development security	-
2.9 System and service operation management	2, 3, 6, 7, 8, 9
2.10 System and service security management	2, 7, 6, 8, 9
2.11 Accident prevention and response	4, 5, 8
2.12 disaster recovery	4, 5, 8

Fig. 2 Relation between ISMS-P security measures requirements and scenarios

ISMS-P Security measures requirements	Check List
2.1 Policy, Organization, and Asset Management	-
2.2 Human security	7, 14, 15
2.3 Outsider security	14, 15
2.4 Physical security	3
2.5 Authentication and Permission Management	7, 10
2.6 Access control	7, 8, 14
2.7 Encryption Enforcement	-
2.8 Information system introduction/development security	-
2.9 System and service operation management	1, 2, 3, 4, 5, 9, 10
2.10 System and service security management	1, 5, 6, 11, 12
2.11 Accident prevention and response	11, 13
2.12 disaster recovery	11

Fig. 3 Relation between ISMS-P security measures requirements and checklist

그림 2, 그림 3 으로 도출된 시나리오와 체크리스트가 각각 ISMS-P 보호대책 요구사항과 연관성을 토대로 종합적 적합성을 맵핑도[11] 그림 4로 구성하였다.

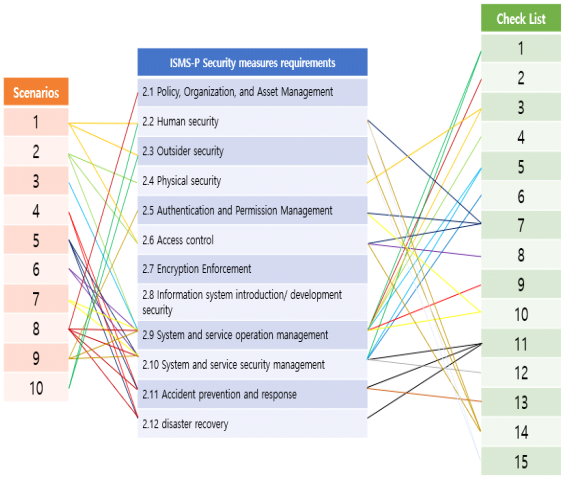

Fig. 4 Comprehensive conformity mapping diagram of scenarios, checklists and ISMS-P security measures requirements

도출된 체크리스트는 365일 24시간이라는 관제업무의 특성상 근무자마다 근무 후 작성하게 하고 이를 용역업체와 사용업체가 각각 작성하여 '아니오' 항목에 대한 집계와 그 사유를 정리하여 월 단위 보고 또는 회의를 통해 상호 보완하여 보안 관리 개선이 가능하다. 결국 업무 연관성 분석과 ISMS-P 요구사항을 준수하는 체크리스트를 도출하고 활용함으로써 외주용역 보안관리 방법을 제안하는 것이다.

Ⅵ. 결 론

보안관제 서비스 용역이 일반화되고 점점 증대되고 있는 상황에서 그에 따른 보안사고 및 위험에 많이 노출이 되고 있다. 이전의 많은 연구에서 보안관제 서비스 용역의 잠재적 위험 감소 및 방지를 위해 의견들을 제시하였고 이를 참고로 보안이 한층 개선된 것은 사실이다. 그러나 많은 연구들이 업무 연관성을 포함한 연구는 부족하다고 느껴진다. 또한 결과로 도출된 관리 방안 및 지표 등이 용역업체의 전적인 업무로만 보이는 경향이 있다. 하나의 업무에도 사용업체와 용역업체가 유기적으로 엮여 있어 외주용역이라는 사업이 있는 곳이라면 그 업무가 단독적으로 수행되면 안 된다. 그러나 오래된 관행과 참고 가이드 등 자료가 없는 상태에서 보안항목 미준수와 위험에 노출되고 있는 것을 인식하지 못한다.

본 논문에서는 위의 문제점들을 해결하기 위해 업무 연관성 분석을 통해 ISMS-P 기반의 외주용역 관리 방법을 제안하며, 이를 사용업체와 용역업체의 업무로 분리하고 체크리스트로 관리하여 애매모호한 업무영역에서 업무혼선 없이 보안항목 준수까지 이끌어낼 것으로 기대되며 보안관제 용역사업 간 보안수준 향상에도 큰 도움이 될 것이다. 또한 앞서 제시된 시나리오별 ISMS-P 보안대책 64개 항목과 맵핑하여 만든 체크리스트 항목을 활용방안 같이 관리 시 보안관제 외주용역 관리가 용이하다. 또한 법률상 기준에 따라 그 대상이 한정되어 있지만 많은 기관 및 업체들이 인증 받아야 하고 점점 그 대상이 확대 될 것으로 예상되는 국내 기준의 정보보안인증체계 ISMS-P 활동을 생활화하여 향후 취득과 갱신에 도움이 될 것이고 내·외부 직원들의 보안의식 제고도 기대할 수 있다.

물론 보안시스템 벤더(Vendor)사 별 다른 계정권한과 관제용역사업의 형태에 따른 체크리스트를 제시하지 않은 한계점은 존재하지만 업무의 연관성을 통해 놓칠 수 있는 보안사항과 그 관리방안이 사용업체와 용역업체 양사 모두의 가이드가 될 수 있을 것으로 보인다. 향후 포괄적인 체크리스를 보안관제 용역 형태의 따라 재편하고, 시스템 계정 권한의 기준이 국내 및 국제 통합 시 이를 포함한 연구로 이어져야 할 것이다.

References

[1] E. S. Lee, "A Study on Enhancing Security Management of Outsourcing for Information System Establishment and Operation," Ph. D. dissertation, Korea Polytechnic University, 2020.

[2] J. W. Moon, "An Empirical Study and Designing of Security Level Quantify Model for ICT Outsourcing," M. S. theses Sangmyung University, 2015.

[3] J. S. Park, "A Study on Detailed Work Items of Security Monitoring and Control Services," M. S. theses, Dongguk University, 2014.

[4] J. H. Kim, "A Study on Measurement Indicator of Outsourced Security Monitoring and Control Level in Public Organizations," Ph. D. dissertation, Soongsil University, 2014.

[5] J. M. Lee, "An Empirical Study on the Auditing Methods for Outsourcing of Security Monitoring & Control," M. S.

theses, Konkuk University, 2013.
[6] S. K. Yeon, D. H. Sin, and N. R. Park, *ISMS-P Certification Practice Guide Considering Cloud Environment*, Seoul, Acorn Pub., 2020.
[7] T. J. Ko, (2017, june). Trade scam, Have you ever heard of scams?. joseplus. Available: https://www.joseplus.com/news/newsview.php?ncode=1065590650621360
[8] S. H. Kim, (2016, April). The internal assistant for civil service exam preparation students was the Ministry of Personnel Management and Innovation. hankookilbo. Available: https://www.hankookilbo.com/News/Read/201604080475235837
[9] K. H. Lee, (2021, octorber). [KT's Internet is messed up] A human-made disaster who destroyed common sense... The government was also perplexed. bloter. Available: https://www.bloter.net/newsView/blt202110290193newsview.php?ncode=1065590650621360
[10] KISA, “ISMS-P Certification Standard Guide”, 2019.
[11] T. S. Yoon and Y. S. Park “Establishment and Effectiveness Analysis of Emergency Vehicle Priority Signal Control System in Smart City and Directions for ISMS-P Technical Control Item Improvement,” *Journal of the Korea Institute of Information and Communication Engineering*, vol. 25, no. 9, pp. 1166-1175, Sep. 2021.

고도균(Dokyun Ko)
목포해양대학교 전자공학과(학사)
세종사이버대학교 정보보호대학원 석사과정
현재 SK Shieldus 관제사업4팀 선임
※관심분야 : 정보보호 컨설팅, 보안관제, ISMS-P, 모의해킹, 클라우드

박용석(Yongsuk Park)
서강대학교 컴퓨터학 (학사)
뉴욕(POLY) 대 (석사, 박사)
AT&T (Bell) Labs, 삼성전자
현재 세종사이버대학교 정보보호대학원 주임교수
현재 세종사이버대학교 IT학부 교수
※관심분야 : IT서비스 및 보안, 산업보안, 4차산업혁명, 클라우드, IoT 등