https://doi.org/10.33778/kcsa.2021.21.1.025

코로나19 환경에서 무중단 보안관제센터 구성 및 운영 강화 연구

강 동 윤*, 이 재 우*, 박 원 형**

요 약

본 연구의 목적은 코로나19 바이러스 유행 시기에 교대근무체계로 운영하는 보안관제센터를 무중단으로 유지하기 위한 연구 이다. 사이버 보안위협에 대응하는 보안관제 시설은 24시간 365일 실시간으로 운영해야 하는 필수 보안시설이며, 보안운영 및 관리적인 부분에서 매우 중요하다. 만약 감염병 유행, 시스템 장애, 물리적 영향 등 보안관제 시설이 폐쇄되거나 영향이 있는 경우 실시간 사이버 보안위협에 대응 할 수 없으며, 보안문제에 치명적이 될 수 있다. 최근 코로나19 바이러스 유행으로 인한 시설 폐쇄, 장마철로 인한 보안시스템 가용성 장애 등 보안관제 시설 운영을 할 수 없는 사례가 확인되고 있으며, 이 외에도 물리적 영향으로 보안관제 시설을 운영 할 수 없는 상황에 대한 대비가 필요하다. 본 논문에서는 보안관제 시설을 다중화 시설로 구성하여 폐쇄되는 상황 발생 시 무중단으로 운영 할 수 있는 방안을 제안한다.

Enhancing on Security Monitoring & Control Redundancy Facilities Configuration & Operation in the COVDI-19 Pandemic Environment

Dongyoon Kang*, Jeawoo Lee**, Wonhyung Park***

ABSTRACT

The purpose of this study was to keep the Security Control Center, which operates under a shift system, uninterrupted during the COVID-19 virus epidemic. Security facilities responding to cybersecurity threats are essential security facilities that must be operated 24 hours a day, 365 days a day in real time, and are critical to security operations and management. If security facilities such as infectious disease epidemic, system failure, and physical impact are closed or affected, they cannot respond to real-time cyberattacks and can be fatal to security issues. Recently, there have been cases in which security system facilities cannot be operated, such as the closure of facilities due to the COVID-19 virus epidemic and the availability of security systems due to the rainy season, and other cases need to be prepared. In this paper, we propose a plan to configure a security system facility as a multiplexing facility and operate it as an alternative in the event of a closed situation.

Key words : Cyber Attack, Security Monitoring & Control Center, National Cyber Security Policy, Policy Countermeasures

접수일(2021년 02월 28일), 수정일(1차: 2021년 03월 18일), 게재확정일(2021년 03월 31일)

* 동국대학교 국제정보보호대학원 정보보호학과 석사과정(주저자)
* 동국대학교 국제정보보호대학원 정보보호학과 석좌교수(공동저자)
** 상명대학교 정보보안공학과 부교수(교신저자)

1. 서 론

보안관제는 현대사회에서 사이버 보안위협에 대응하기 위한 필수 보안 서비스이다. 이를 운영하기 위해 보안관제센터를 운영하여 24시간 365일 실시간으로 사이버 보안위협에 대응을 해야 한다. 만약 코로나19 바이러스 같은 감염병 유행, 시스템 장애, 물리적 영향 등 보안관제시설이 폐쇄되어 운영이 중지되는 경우 보안사고, 시스템, 보안 서비스 신뢰도 하락 등 문제가 생길 수 있으며 보안관제의 중요한 기본원칙 중 하나인 무중단의 원칙을 지키지 못 할 수 있다.

최근 보안관제 시설이 폐쇄되는 사례로는 보안관제센터에서 코로나19 바이러스 감염병 확진자가 발생하여 임시 폐쇄된 사례가 있다. 감염병 확진자로 인해 보안관제요원들이 14일간 자가격리 조치로 보안관제 업무를 수행 할 수 없게 되었다. 이러한 사례로 보아 보안관제 시설이 폐쇄되는 기간동안 보안관제 서비스를 제공할 수 없으므로 언제 발생할 지 모르는 사이버 보안위협에 대한 대응이 불가능하다.

따라서, 본 논문에서는 기존에 보안관제 전문업체에서 운영하는 하이브리드 보안관제 서비스와 함께 보안관제 다중화 시설을 구축으로 언제 발생할지 모르는 폐쇄로 보안 서비스가 중단되는 상황에 대비해 운영 할 수 있는 방안을 제안한다[1][2][3].

2. 관련연구

2.1 보안관제의 개념

보안관제의 정의는 기업의 정보, 기술과 같은 IT 자원을 해킹, 바이러스 등의 사이버 공격으로부터 보호하기 위한 일련의 활동을 의미한다[1].

보안관제의 주업무는 해킹 사실을 기관에 통보하고 분석 단계에서 파악된 공격자 정보와 취약점 정보를 활용하여 피해 시스템이 정상적으로 운영될 수 있도록 신속하게 전문기술을 제공하는 것이다. 즉, 보안관제란 사이버상의 위협으로부터 정보를 보호하기 위한 일련의 모든 활동을 총칭하는 것이다[2].

2.2 무중단의 원칙

보안관제에서의 무중단의 원칙은 사이버 공격을 신속히 탐지 및 차단하기 위해서는 24시간 365일 중단없이 보안관제 업무를 수행해야 한다. 이를 위해 보안관제센터 운영 기관 또는 민간 보안관제 업체는 적정수의 보안관제 인력을 보유하여 교대근무 체계를 구축하고 있다[1]. 이로서 불특정시간에 발생하는 사이버 공격을 실시간으로 신속하게 탐지 및 대응 하는 것이 필수이다.

2.3 보안관제센터

보안관제센터 정의는 일정한 수준 이상의 시설 및 장비와 전문 인력을 갖추어 효과적인 보안관제 업무 수행하는 시설을 말한다. 보안관제 시설은 보호구역으로 설정하여 관리해야 하며 외부인에 대한 접근통제 및 감시체계를 효율적으로 수행할 수 있는 독립된 공간에서 구축 및 운영을 해야 한다[2].

2.4 보안관제 유형

보안관제 유형은 크게 원격 관제, 파견 관제, 자체 관제로 분류된다. 원격관제는 보안관제 서비스 업체에서 보안관제에 필요한 관제 시스템을 구비하고 대상 기관의 보안장비 중심의 보안 이벤트를 중점적으로 상시 모니터링하고 침해사고 발생 시 긴급 출동하여 대응 조치하는 서비스이다. 파견관제는 보안관제 대상 기관이 자체적으로 보안 관제 시스템을 구축하고 보안관제 전문업체로부터 전문 인력을 파견 받아 관제 업무를 수행하는 서비스이다. 자체관제는 보안관제 시스템 및 전문 인력을 자체적으로 구축하고 운영하는 형태이다[2].

<표 1> 보안관제 업무유형[2].

업무 유형	주요 내용	대상 기관
원격 관제	· 일부 단위 보안 시스템의 운영 및 관리를 위탁하는 방식 · 통합 보안 관제 시스템 및 관제 인력이 원격에 위치함	일반기업 포탈 업체
파견 관제	· 자체 구축한 보안 관제 시스템의 운영 및 관리를 위탁하는 방식 · 전문 인력이 대상 기관에 파견되어 관제 업무 수행	공공 분야 금융권
자체 관제	· 자체 보안 관제 시스템의 운영 및 관리를 자체적으로 수행 · 기관 자체 정규직, 계약직 보안 인력을 통한 관제 업무 수행	국정원, 경찰청 등 대규모 통신사 등

2.5 보안관제 전문업체 지정 제도

보안관제 전문업체 지정제도는 국가사이버안전관리규정 제10조의2 및 보안관제 전문기업 지정 등에 관한 공고 등 법적근거를 바탕으로 국가·공공기관에서 설치·운영하는 보안 관제센터에 전문인력 파견, 운영 지원 등 보안관제 업무를 수행할 수 있는 전문기업을 매년 1회 지정하는 제도이다

아래의 <표 2>는 2021년 01월 기준으로 17개 보안관제 전문업체 지정 현황 표이다[4].

<표 2> 2021년 보안관제 전문업체 지정 현황[4].

번호	업체명	홈페이지
1	㈜이글루시큐리티	http://www.igloosec.co.kr
2	한국통신인터넷기술㈜	http://www.ictis.kr
3	㈜안랩	http://www.ahnlab.com
4	한전KDN㈜	http://www.kdn.com
5	㈜싸이버원	http://www.cyberone.kr
6	에스케이인포섹㈜	http://www.skinfosec.com
7	㈜윈스	http://www.wins21.co.kr
8	롯데정보통신㈜	http://www.ldcc.co.kr
9	㈜에이쓰리시큐리티	http://www.a3security.co.kr
10	㈜시큐어원	http://www.secureone.co.kr
11	㈜ktds	https://www.ktds.com
12	삼성에스디에스㈜	http://www.samsungsds.com
13	㈜파이오링크	http://www.piolink.com
14	㈜가비아	https://www.gabia.com
15	㈜LGCNS	http://www.lgcns.co.kr
16	㈜시큐아이	https://www.secui.com
17	씨엠티정보통신㈜	http://www.cmtinfo.co.kr

2.6 백업

백업(backup)은 임시 보관을 일컫는 말로, 정보 기술에서는 데이터 백업(data backup)이라고 하며, 데이터를 미리 임시로 복제하여, 문제가 일어나도 데이터를 복구 할 수 있도록 준비해 두는 것을 말한다[5]. 보안장비의 시스템 장애에 대해서는 예상 할 수 없는 영향이 있을 수 있기 때문에 주기적인 백업은 필수이다.

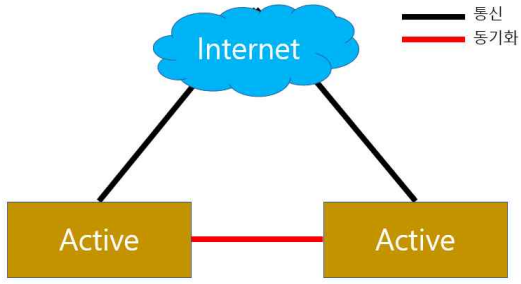
2.7 다중화

다중화(redundancy)는 시스템의 일부에 어떠한 장애가 발생 하였을 경우에 대비하여, 장애 발생 다음에도 시스템 전체의 기능을 계속 유지하도록 예비 장치를 평상시부터 백업으로서 배치해 운용하는 일이다[3]. 보안관제에서는 보안장비의 시스템 장애를 대비하기 위해 예비 시스템으로 이중화로 운영하고 있는 경우가 많다.

2.7.1 액티브(Active)-액티브(Active)

액티브(Active)-액티브(Active)는 고속의 채널을 통해 동작 계열과 대기 계열이 완전 동일 상태를 유지하고 문제 발생 시 빠른 계열 변경(fail-over)이 가능하고, 빠른 서비스 응답과 로드밸런싱을 지원하는 웹 서버 이중화 방법이다[6].

아래의 (그림 1)과 같이 액티브(Active)시스템 장애 시에도 다른 액티브(Active)시스템이 동작한다.

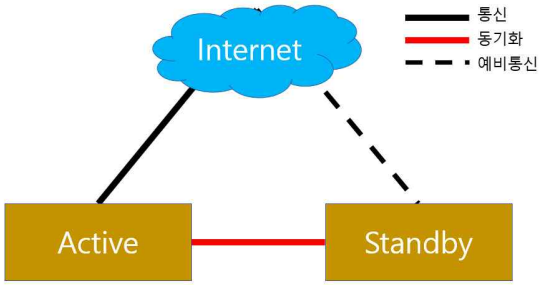


(그림 1) Active-Active 시스템 네트워크 구성

2.7.2 액티브(Active)-스탠바이(Standby)

액티브(Active)-스탠바이(Standby)는 한 서버가 액티브 상태로 정상 서비스하고 있을 때, 다양한 원인으로 인한 장애가 발생하여 서비스가 불가능 할 경우, 스탠바이 서버에 있는 다중화 기술이 운영 서버의 장애 발생을 감지한다. 그리고 다중화 기술을 사용하여 자동으로 스탠바이 서버에 모든 서비스를 올려준다[7].

아래의 (그림 2)과 같이 액티브(Active)시스템 장애를 대비하여 스탠바이(Standby)시스템이 대기 중이다.



(그림 2) Active-Standby 시스템 네트워크 구성

2.8 집적정보 통신시설 보호지침

집적정보통신시설"이라 함은 법 제2조 제2호에 따른 정보통신서비스를 제공하는 고객의 위탁을 받아 컴퓨터장치 등 전자정부법 제2조 제13호에 따른 정보시스템을 구성하는 장비(이하 "정보시스템 장비")를 일정한 공간(이하 "전산실")에 집중하여 관리하는 시설을 말한다[8].

정보통신망 이용촉진 및 정보보호 등 에 관한 법률 제 46조에는 “타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 정보통신서비스 제공자(이하 “집적정보통신시설 사업자”라 한다)는 정보통신시설을 안정적으로 운영하기 위하여 대통령령으로 정하는 바에 따른 보호조치를 하여야 한다.“로 명시되어 있으며, 보안관제 시설에서도 시설보호 및 서비스 유지가 필요하다[9]. 정보통신망 이용촉진 및 정보보호 등에 관한 법률과 집적정보 통신시설 보호지침을 준수하여 보안관제 시설을 구축하고 운영해야 한다.

3. 제안하는 보안관제센터 무중단 운영

3.1 Active-Standby 보안관제 시설구축 및 운영방안

Active-Standby 보안관제 시설 구축은 주로 자체 보안관제 및 원격보안관제를 위한 운영방안으로 아래 <표 3>과 같이 평시 본사에서 보안관제 서비스를 수행하며, 운영 중지 시 근거리에 있는 지역으로 예비 보안관제 서비스를 수행 할 수 있다. 이는 시스템 장애나 물리적 영향으로 운영이 중지되는 상황에서 대체 운영 될 수 있는 Standby 시설을 구축하는 것 이다.

<표 3> Active-Standby 보안관제 시설운영(예시)

구분	위치	역할
관제센터	서울	· Active 보안관제 시설 운영으로 보안관제 인력 상주
예비관제센터	수원	· Standby 보안관제 시설 운영으로 보안관제 서비스 점검 인력 상주 · Active 보안관제 시설 운영 중지 시 보안관제 인력 예비관제센터로 임시근무

하지만 Active 보안관제 시설에서 보안관제요원이 일부 인원이라도 감염병 확진이 되는 경우 Active 시설은 방역조치 및 임시폐쇄 등으로 운영 중지가 될 수 있으며, 감염인원 및 자가격리 대상 인원에 따라 소수 인원 및 대체인원으로 보안관제 서비스를 운영해야 하므로 인력과 근무시간표에 대한 문제가 발생 할 수 있다.

3.2 Active-Active 보안관제 시설구축 및 운영방안

Active-Active 보안관제 시설은 원격보안관제 서비스를 받는 기업을 위한 운영방안이다.

아래 <표 4>와 같이 Active-Active 보안관제 시설 구축은 두 곳에서 평시에 보안관제의 공동업무를 수행 하는 것이다. 만약 보안관제 한 시설이 운영 중지 되는 상황이 발생하는 경우 보안관제 서비스는 다른 한 시설에서 운영 중이기 때문에 지속적인 서비스를 유지할 수 있으며 운영 중지된 보안관제 시설 인력으로부터 운영 중 인 보안관제 시설에 인력보충이 되기 때문에 사이버 보안위협에 대한 모니터링을 수준 이상으로 수행 할 수 있다.

<표 4> Active-Active 보안관제 시설 운영(예시)

구분	위치	역할
원격관제 1센터	서울	· Active 시설 운영으로 보안관제 인력 상주 · 보안관제 시설 한 곳이 운영 중지 시 인력보충으로 보안관제 모니터링 강화
원격관제 2센터	대전	

하지만 다중화 보안관제 시설을 모두 Active로 구축하는 경우 구축 비용과 보안관제 시설 별로 보안관제요원에 대한 관리가 필요하다. 예상되는 문제는 인건비 발생, 교대근무 시간표 조정 등 운영적인 문제가 발생한다.

3.3 Active-Active-Standby 보안관제 시설 구축 및 운영방안

아래 <표 5>과 같이 Active-Active-Standby 보안관제 시설 구축은 다중화로 구축 하는 경우 운영 중지 시 대체 운영 될 수 있는 시설이 많다. 이 방안의 경우 모든 유형의 보안관제에 대한 보안관제 서비스를 수행 할 수 있다. 또한 Standby시설에 전문보안인력과 시스템 복구인력을 같이 상주 할 경우 운영 중지되는 상황에서도 더욱 효율적으로 대응이 가능하다.

<표 5> Active-Active-Standby 보안관제 시설 운영(예시)

구분	위치	역할
원격관제센터	서울	・Active 보안관제 시설 운영으로 보안관제 인력 상주
파견관제센터	부산	
예비관제센터	대전	・Standby 보안관제 시설 운영으로 보안관제 서비스 점검 인력 상주 ・Active 보안관제 시설 운영 중지 시 보안관제 인력 예비관제센터로 임시근무

하지만 다중화로 보안관제 시설을 구축하는 경우 구축 비용과 상주해야 할 인원에 대한 인건비가 많이 발생 할 수 있다. 이는 예산이 많은 기업이나 공공기관에서만 가능 할 수 있으며, 고객사로부터 파견관제에 대한 단가가 높아 질 수 있는 단점이 있다.

3.4 하이브리드 보안관제

하이브리드 보안관제란 원격보안관제와 파견보안관제의 각각의 장점을 융합하여 운영하는 보안관제 서비스이다[10].

현재 다수 보안관제 전문업체에서 수행하는 보안관제 서비스이며 단가가 높아 대기업 고객사가 위주로 받는 보안관제 서비스이다. 이 방식을 도입 한다면 원격관제를 수행하는 보안관제 서비스 업체와 파견관제를 수행하는 서비스 대상 기업 중 한 시설이 운영 중지되는 경우를 대비해 보안관제 한 시설에서 집중 운영하여 보안 서비스에 영향이 없다. 시스템적이나 물리적인 문제가 발생이 원인인 경우 정상적인 서비스 운영을 위해 업체과 기업 간 협력하여 신속히 복구를 진행 할 수 있다.

3.5 Standby 보안관제 시설 시스템 점검 및 운영방안

보안관제센터의 다중화 시설 운영을 하기 위해서는 Standby 보안관제 시설에 대한 시스템 점검도 매우 중요하다. 보안관제 서비스를 실시간 유지하기 위해서는 즉시 운영 될 수 있어야 한다.

<표 6> Standby 보안관제 시설 점검 및 운영 항목(안)

운영항목	운영방식	점검주기(안)
비상연락체계	・Active 보안관제 시설 운영 중지 시 상황 공유 ・조직 내 연락처 최신화 ・유지보수업체연락처 최신화	상시 최신화
보안시스템 상태 점검	・보안시스템 데이터 무결성, 상태 확인 점검 ・보안시스템 백업	일 1회 점검 주 1회 백업
네트워크 통신 점검	・Active 보안관제 시설 시스템과 실시간 동기화 점검 ・네트워크 통신 전환 시 이상 확인 점검	실시간
시설관리책임자 지정	・상시적으로 운영 될 수 있도록 시설관리책임자 지정	-
모의상황 대비훈련	・Active 보안관제 시설 운영중지 모의상황 발생 시 대비 훈련	분기 1회

이를 위해 <표 6>와 같이 Standby 보안관제 시설 점검 및 운영을 위한 항목으로 비상연락체계 구성, 보안시스템 상태 점검, 네트워크 통신 점검, 시설관리책임자 지정, 모의상황 대비훈련 등 제안한다. 보안관제에 대한 보안서비스 유지 및 시설 폐쇄되는 상황을 대

비하기 위해 점검항목을 정하여 주기적으로 점검해야 하며 상시적으로 가동할 수 있는 운영방안이 필요하다.

3.6 감염병 유행에 따른 집단 시설 운영방안

보안관제 시설은 집단시설로 분류되며 실시간으로 운영해야하기 때문에 시설 폐쇄되는 상황이 발생되서는 안된다. 만약 코로나19 및 재난재해와 같은 감염병 유행으로 보안관제 시설 내 감염병 확진자 발생 시 질병관리본부 지침에 따라 시설 폐쇄해야한다[11]. 시설을 폐쇄해야하는 경우를 대비해야 하며, 아래의 <표 7>과 같이 감염병 유행에 따른 보안관제 시설 대응 수칙을 이행해야 한다.

<표 7> 감염병 유행에 따른 보안관제 시설 대응 수칙 방안(안)

항목	내용
관리체계 및 유관기관 협조체계	・시설관리자와 유관기관(보건소, 의료기관) 간 비상 연락체계 유지 및 상황 발생 시 즉시 대응 ・조직 내 감염병 신고접수 대응 담당자 지정 후 내부직원, 외부직원 관리
감염병 예방 교육	・내부직원 대상 감염병 정보 및 예방수칙, 행동요령 교육
보안관제 시설 주기적 방역	・밀폐된 시설은 감염병에 취약 ・일 1회 주기적 방역 실시
근무 간 개인위생 관리	・마스크 착용 ・손소독제 비치 ・자리 간 거리두기 ・업무상 대화 필요 시 사내 메신저 활용
근무시간표 최소화	・보안관제요원 최소인원으로 근무 ・자가격리 및 소수 보안관제요원 재택에서 보안 업무 수행
감염병 의심자 발생 시 대응	・즉시 보안관제 시설 폐쇄 및 예비관제센터 업무 전환 ・보안관제요원 중 감염병 확진자, 의심자, 비접촉자 등 분류하여 보안업무 수행

3.7 다중화 보안관제 시설 비교

3.1에서 3.4까지 제시한 보안관제센터의 다중화 시설 운영에 대한 내용을 아래 <표 8>와 같이 비교하여 상황과 여건에 맞는 보안관제 시설을 구축 해야 한다.

<표 8> 다중화 보안관제 시설 비교표.

유형	시설 수	인력 비중
A-S 시설	2	A시설에 집중, S시설 예비 준비
A1-A2 시설	2	A1시설, A2시설에 분산
A1-A2-S 시설	3	A1시설, A2시설에 분산, S시설 예비 준비
하이브리드 보안관제시설	2	원격관제시설, 파견관제시설에 분산

・A : Active 보안관제센터
・S : Standby 보안관제센터

4. 기대효과

보안관제 시설 다중운영으로 문제가 되는 점은 시설을 구축 할 수 있는 비용과 보안관제요원 인력 관리지만 이러한 문제가 해결된다면 다음과 같이 장점을 기대할 수 있다.

첫 번째, 보안관제 시설 운영중단 상황 발생 시 즉시 예비 보안관제 시설로 운영되어 대상 기관에 보안관제 서비스를 제공 할 수 있다.

두 번째, 보안관제 3대 원칙 중 무중단의 원칙을 지킴과 동시에 강화 할 수 있다.

세 번째, 대상기관에 대한 보안관제 서비스 신뢰도를 향상 시킬 수 있다.

네 번째, 보안운영, 보안정책, 사이버 보안위협의 문제를 감소할 수 있으며 사회적인 이슈와 기업의 신뢰도 하락을 방지 할 수 있다.

이러한 보안관제 시설에 대한 기대효과로 더욱 효율적으로 운영할 수 있다. 시대의 흐름에 따라 정보통신기술이 고도화되고 이에 맞는 사이버 보안 위협으로부터 대비를 해야 한다.

5. 결론

보안관제 서비스는 어떠한 상황에서도 24시간 365일 실시간 사이버 보안위협으로부터 대응해야 한다.

특히, 최근 코로나19와 같은 자연재해나 팬데믹 환경에서도 보안관제 시설이 예상치 못한 상황으로 인해 폐쇄되는 경우 보안관제 서비스 운영은 중단 되면 안된다. 이러한 특정한 상황에서 보안관제센터가 운영

되지 않으면 기업 내 자산에 피해를 줄 수 있을 뿐만 아니라 보안관제 서비스에 대한 신뢰도가 낮아질 수 있다. 이러한 다중화된 보안관제 시설을 운영하는 경우 보안관제 서비스가 중단되지 않고 실시간 대응 할 수 있다. 또한, 실시간 사이버 보안위협에 대해 대응할 수 있으며 고객사로부터 보안관제에 대한 신뢰도도 유지 할 수 있다. Standby 보안관제 시설에서는 실시간 점검과 관리를 통하여 언제든지 상시적으로 운영 될 수 있도록 한다. 본 논문은 최근 코로나19 바이러스와 같은 감염병 발생으로 인한 시설폐쇄와 시스템 장애, 자연재해, 물리적 영향 등 예상 할 수 없으며, 언제든지 발생 할 수 있는 상황에 대한 대비책으로 보안관제의 원칙 중 무중단의 원칙을 지킴과 동시에 보안관제 시설을 강화하고 유지하는 방안을 제시한다.

참고문헌

[1] SK인포섹(주) 공식블로그, "'보안관제'에 관한 모든 것", https://blog.naver.com/skinfosec2000/221116097157, 2017.10.

[2] 안성진, 이경호, 박원형. "보안관제학", 이한미디어, 2014.

[3] 위키백과, 다중화 (시스템), https://ko.wikipedia.org/wiki/%EB%8B%A4%EC%A4%91%ED%99%94_(%EC%8B%9C%EC%8A%A4%ED%85%9C), 2009.05.

[4] 한국인터넷진흥원, 보안관제 전문 기업 지정, https://www.kisa.or.kr/business/infor/inforpro_4.jsp, 202021.01.

[5] 위키백과, 백업, https://ko.wikipedia.org/wiki/백업, 2008.07.

[6] 해시넷, 위키, 액티브-액티브, http://wiki.hash.kr/index.php/액티브-액티브, 2020.08.

[7] 해시넷, 위키, 액티브-스탠바이, http://wiki.hash.kr/index.php/액티브-스탠바이, 2020.08.

[8] 국가법령정보센터, 집적정보 통신시설 보호지침, 2017.08.24.

[9] 국가법령정보센터, 정보통신망 이용촉진 및 정보보호 등 에 관한법률, 제 46조, 2020.09.10.

[10] 이글루시큐리티, 보안관제 서비스 종류, http://www.igloosec.co.kr/ig/서비스_보안관제_보안관제%20서비스%20종류, 2019.

[11] 보건복지부, 코로나바이러스감염증-19 집단시설·다중이용시설 대응 지침(2판), http://www.mohw.go.kr/react/jb/sjb0406vw.jsp?PAR_MENU_ID=03&MENU_ID=030406&CONT_SEQ=353151, 2020.02.

〔저자소개〕

강 동 윤 (Dongyoon Kang)
극동대학교 산업보안학과 공학사
현) 동국대학교 국제정보보호대학원 정보보호학과 석사과정
email: nef4529@naver.com

이 재 우 (Jeawoo Lee)
美 University of Southern California Major of System Management 석사
건국대학교 정보체계학과 박사
전) 공군 장군 예편
전) 사이버포렌식전문가협회 초대 회장
전) 한국정보보호진흥원 초대 원장
현) (ISC)² 아시아지역 대표
현) 동국대학교 국제정보보호대학원 석좌교수
email: jwlee0904@daum.net

박 원 형 (Wonhyung Park)
서울과학기술대학교 공학사, 공학석사
경기대학교 정보보호학과 이학박사
성균관대학교 컴퓨터교육학과 박사수료
전) 극동대학교 사이버보안학과 부교수/학과장
현) 상명대학교 정보보안공학과 부교수
email : whpark@smu.ac.kr