보안관제 조직을 위한 사이버보안 프레임워크 개선에 관한 연구

조 창 섭*, 신 용 태**

요 약

사이버공격이 지능화되고 고도화되면서 이를 체계적으로 대응하기 위한 보안관제센터(SOC : Security Operations Center)의 중요성이 높아지고 있고, SOC의 규모와 그 수도 늘어나고 있다. 각 기관 및 조직에서 다양한 사이버보안 표준을 활용하여 업무 절차를 만들어 사용하고 있으나 SOC는 자체 인력보다는 보안관제전문기업과 협업하는 경우가 많아 SOC환경에 맞게 개선이 필요하다. NIST 사이버보안 프레임워크(CSF : Cybersecurity Framework)와 정보보호 관리체계 그리고 보안관제전문기업의 업무절차를 비교 분석한 결과 NIST CSF가 보안관제에 적용하기 용이한 프레임워크이나 국내 SOC에 적용하기 위해서는 SOC의 운영 및 관리 부분이 추가적으로 보완될 필요가 있다. 따라서 본 연구에서는 NIST CSF를 참조 모형으로 하여 SOC환경에 필요한 관리적 항목을 도출하였으며 각 항목에 대한 필요성, 중요성, 용이성을 델파이 조사방식으로 검증하고 개선된 사이버보안 프레임워크를 제안하였다.

A Study on Improvement of Cyber Security Framework for Security Operations Center

Changseob Cho*, Yongtae Shin**

ABSTRACT

As cyber-attacks become more intelligent and sophisticated, the importance of Security Operations Center(SOC) has increased and the number of SOC has been increasing. In order to cope with cyber threats, institutions and organizations use a variety of cyber security standards to create business procedures. However, SOC often need to be improved in accordance with the SOC environment because they collaborate with managed security service specialists rather than their own personnel. The NIST cyber security framework, information security management system, and managed security service companies were compared and analyzed. As a result, it was found that the NIST CSF is a framework that is easy to apply to managed security service, The content was judged to be insufficient. Therefore, in this study, NIST CSF was used as a reference model to derive the management items required for SOC environment, and the necessity, importance and ease of each item were confirmed through an Delphi technique and an improved cyber security framework was proposed.

Key words : Security Operations Center, Security Framework, 사이버보안 프레임워크

접수일(2019년 2월 28일), 게재확정일(2019년 3월 19일)

* 숭실대학교/IT정책경영학과

** 숭실대학교/컴퓨터학부(교신저자)

1. 서 론

현재의 비즈니스 환경은 IT기술과 대부분 직접 연결되어 있고, 사이버환경의 급속한 발전은 생활의 편리함과 더불어 사이버공격에 더 많이 노출되고 있다. 그로 인해 공격자들은 더 많은 대상을 더 쉽게 공격할 수 있는 환경까지 마련해 주게 되었으며 IoT 기기들을 활용한 대규모 DDoS공격이나 가상화폐 채굴을 위한 악성코드의 증가, 지능형지속위협(APT: Advanced Persistent Threats) 공격은 점점 더 증가하고 있다[1]. 이러한 사이버보안에 대한 이슈가 지속됨에 따라 사이버공격을 체계적으로 대응하기 위한 보안관제센터(Security Operations Center, 이하 SOC)[1]의 중요성은 더욱 높아지고 있다[2].

SOC의 목적은 조직의 정보자산을 보호하여 비즈니스를 활성화 시키는데 있다. SOC는 사이버보안의 최전방에서 조직의 자산 및 정보를 보호하기 위해 사이버위협 예방, 사이버위협 모니터링, 발생 위협에 대한 대응과 복구, 피해확산 방지 활동을 수행한다. 이런 SOC의 운영 및 관리는 조직의 내부 직원으로 운영되기도 하지만 외부 보안관제전문기업[2](MSSP: Managed Security Service Provider)의 인원을 파견 받아 보안전문인력과 함께 운영 하는 경우가 많다. 이렇게 MSSP에서 파견된 인력들은 SOC의 업무뿐만 아니라 업무위탁 기관의 정보보안 업무를 전반적으로 지원하고 있다. 이러한 특성을 바탕으로 SOC의 운영 방법은 일반적인 정보화 조직의 운영 방식과 다르게 접근해야 하며 SOC의 특성에 맞는 사이버보안 프레임워크를 활용할 필요성이 있다.

현재 다양한 기관의 SOC에서 활용하고 있는 프레임워크는 ISO/IEC 27001, ISMS-P 등의 기준을 토대로 정리하여 사용하고 있으나 정보보호 전반에 걸친 물리적, 관리적, 기술적 활동을 망라하여 나열함으로 각 기관에서 필요한 항목을 재 생성하여야 하는 특성이 있고, SOC에서 바로 적용하여 활용 가능한 표준 프레임워크가 부족하다[3].

이에 본 연구에서는 기존의 사이버보안 프레임워크로 활용되는 기준들을 비교·분석하고 SOC의 환경에 맞는 필요항목과 개선사항을 도출하여 보안관제조직의 특성에 맞는 사이버보안 프레임워크를 제시하고 자 한다.

2. 관련 연구

2.1 Security Operations Center(SOC)

2.1.1 SOC의 개념과 구성

SOC는 조직의 각종 보안장비를 최신상태로 유지하며, 보안관제 대상을 24시간 365일 무 중단 모니터링 업무를 수행하여 정보자산을 보호한다. 이를 위해 SOC는 전문 인력과 시설을 갖춰야 한다. SOC는 사이버위협의 탐지뿐만 아니라 사고 발생 시 피해를 최소화하기 위하여 관계기관 간 정보공유를 수행 한다[4][5].

이러한 SOC는 그림 1과 같이 전문조직(인원), 운영 프로세스, 필요기술로 구성된다[6].

(그림 1) SOC의 구성요소

SOC의 인원(people)은 Tier1~3 (Tier1-Alert Analyst, Tier2-Incident Responder, Tier3-Subject Matter Expert/Hunter, SOC Manager)의 다양한 수준으로 구성된 조직이 필요하다[6]. 또한 보호 대상과 범위에 따라 필요한 인원을 산정하여 배치하게 된다.

1) 국내에서는 국가사이버안전센터(국가정보원), 사이버안전센터(중앙부처), 사이버침해대응센터(지방자치단체), 보안관제센터(기업) 등으로 사용되며, 해외에서는 Security Operations Center로 사용된다.

2) 국가사이버안전관리규정 제10조 2에 의거 지정된 전문기업으로 과학기술정보통신부에서 매년 지정, 사후관리 한다.
- 2018년12월 기준 18개사

SOC의 운영 프로세스(process)는 식별-예방-탐지-대응-복구 등 다양한 업무를 수행하며, 이를 통해 조직의 보안 수준을 높이고, 침해 예방 및 대응을 수행할 수 있다. 다양한 수준의 조직 구성원들은 SOC 환경에 적합한 근무체계와 업무 분장에 따라 SOC내 업무를 수행하며, 사건(incidents) 발생 시 사전에 규정한 업무 프로세스에 의해 대응 및 보고를 수행한다.

SOC에서 필요한 기술(technology)은 조직 전체의 보안 데이터 수집, 집계, 탐지, 분석 및 관리를 위한 다양한 솔루션이 준비되고 관리할 기술이 필요하다. 보호할 자산정보에 대한 주기적인 취약점관리와 사이버 위협 인텔리전스 정보 수집을 포함하여야 하며, 통합보안관리시스템(SIEM: Security Information & Event Management) 등을 통해 관제업무를 수행한다[5]. SIEM은 다양한 소스로 부터 로그, 이벤트를 수집하여 경보를 발생하고, 분석 기능 등을 제공하는 SOC의 핵심 기술에 속한다.

2.1.2 국내 SOC의 현황

민간분야의 SOC는 90년대 후반 보안관제서비스 회사가 설립(안랩코코넛, 이글루시큐리티 등)되면서 구축되기 시작하였고, 공공분야는 2003년 1.25 인터넷 대란 후 사이버보안의 중앙관리를 위해서 보안관제센터의 필요성이 대두되면서 2003년 한국인터넷진흥원, 국가정보원을 시작으로 현재는 「국가사이버안전관리규정」에 의거하여 중앙행정기관, 지방자치단체 및 공공기관은 보안관제센터를 설치·운영하고 있다. 그에 따라 국가·공공기관의 보안관제는 단위보안관제(각급기관)→부문보안관제(중앙행정기관)→국가보안관제(국가사이버안전센터)로 구성된 3단계 사이버공격 탐지·차단체계를 구축·운영하고 있다[7].

'국가 사이버안전관리체계'상의 35개 사이버안전센터를 비롯하여, 2018년 1월 기준으로 '주요정보통신기반시설'로 지정된 민간분야 149개 시설(91개 기관), 공공분야 262개 시설(141개 기관)도 SOC의 역할을 수행하는 조직이 구성되어 점차 확대되고 있다[7].

2.2 사이버보안 프레임워크

국내의 사이버보안 프레임워크에 대한 연구는 주로 기반시설에 대한 사이버보안 프레임워크를 도출하거나 개발 방안에 대한 연구[8][9]로 권성문(2017)은 NIST CSF[3]와 DoE C2M2[4]를 참조하여 기반시설 사이버보안 프레임워크를 도출하고 있으나, 사이버보안 프레임워크의 핵심인 탐지(detect)를 참조하지 않고 도출하지 않고 있다. 또 이상도(2018)는 제어시설에 대한 사이버보안 프레임워크 연구에서 NIST CSF를 국내 제어시설 환경에 맞게 도입·검토하는 것을 제안하고 있다[10]. 김민준(2010)은 정보보안 거버넌스를 쉽게 적용하기 위한 소규모 조직의 정보보안 거버넌스 프레임워크 연구를 통하여 프레임워크를 단순화하여[11] 프레임워크 도입을 쉽게 하고자 하였다.

사이버보안 프레임워크는 구성 요소, 각 구성 요소가 갖춰야 할 내용과 형식, 구성 요소 사이의 관계, 사용 예제를 담고 있어야하며, 비슷한 문제를 해결 할 때 계속 재사용할 수 있어야 한다[12]. SOC의 사이버보안 프레임워크도 실제 운영환경에 맞게 도출되고 재사용성 확보와 지속적인 수정이 이루어져야 한다.

2.2.1 NIST CSF

미국 오바마정부 "행정명령(Executive Order 13636, 2013.02)"을 통해 국토안보부 주도로 NIST에서 Cyber security Framework(CSF) 및 인센티브(안)을 개발하고 의견 수렴과정을 거쳐 2014년 2월 발표되었다. 트럼프정부 역시 행정명령(2017.5)을 통해 오바마 정부의 사이버보안대책을 연장하였고, 이를 바탕으로 NIST Cybersecurity Framework V1.1이 개정(2018.4) 되어 배포/사용 중에 있다[13][14].

CSF는 Framework Core, Framework Implementation Tier, Framework Profile로 구성되어 있다.

Framework Core는 일련의 사이버 보안 활동, 주요 인프라스트럭처 분야에서 공통적으로 적용되는 참조 자료이며, 핵심은 사이버 보안 활동 및 결과를 집행 단계에서 구현·운영 단계에 이르는 조직 전체의 의사소통을 허용하는 방식으로 업계 표준, 지침을 제시한다. 또한 Functions, Categories, Subcategories, 그리고

3) 미국 국가표준기술연구소(National Institute of Standards and Technology)에서 개발한 사이버보안 프레임워크 : Cybersecurity Framework

4) 미국 에너지부에서 작성한 사이버보안 성숙도 모델 : Cybersecurity Capability Maturity Model (C2M2)

Informative References의 요소들로 구성되며, Framework Core의 Functions는 표 1과 같이 식별(Identify), 보호(Protect), 탐지(Detect), 대응(Respond), 복구(Recovery)의 5개 기능들을 동시 및 연속적으로 구성하고 함께 고려하고 있다. 이 기능들은 각각의 범주와 108개의 하위 범주에서 구체적인 사이버보안 활동을 명시하고 있으며, 조직의 사이버보안 위험 관리의 라이프 사이클에 대한 전략적인 시각을 제공하고 있다.

<표 1> NIST CSF 코어의 구성 항목

기능	카테고리	하위 카테고리
Identify (식별)	자산 관리 (ID.AM)	6
	사업 환경 (ID.BE)	5
	거버넌스 (ID.GV)	4
	리스크 평가 (ID.RA)	6
	리스크 관리 전략 (ID.RM)	3
	공급망 리스크 관리 (ID.SC)	5
Protect (보호)	ID관리, 인증, 접근제어 (PR.AC)	7
	인식교육 및 훈련 (PR.AT)	5
	데이터 보호 (PR.DS)	8
	정보보호 추진 절차 (PR.IP)	12
	유지 (PR.MA)	2
	보호 기술 (PR.PT)	5
Detect (탐지)	이상상황 및 이벤트 (DE.AE)	5
	지속적인 보안 모니터링 (DE.CM)	8
	탐지 절차 (DE.DP)	5
Respond (대응)	대응 계획 (RS.RP)	1
	커뮤니케이션 (RS.CO)	5
	분석 (RS.AN)	5
	피해 경감 (RS.MI)	3
	개선 (RS.IM)	2
Recover (복구)	복구 계획 (RC.RP)	1
	개선 (RC.IM)	2
	커뮤니케이션 (RC.CO)	3

2.2.2 ISO/IEC 27001:2013

ISO/IEC 27001은 정보보안 관리시스템을 수립, 구현, 유지 및 지속적으로 개선하기 위한 정보보호관리체계와 관련한 국제 표준이며 2013년 개정안이 발표되어 사용 중이다. 이를 활용하여 기업 정보의 기밀성, 무결성 및 가용성을 보존하고 리스크를 적절히 관리한다. 구성은 관리과정 7개 분야 22개, 통제항목은 14개 분야 114개로 구성 되어 있다[15].

ISO/IEC 27001의 관리항목 및 통제항목은 조직의 정보보호 수준 향상뿐만 아니라 지속적인 개선에 초점을 맞추고 있다. ISO/IEC 27001을 통해 보호가 되는 조직에는 SOC 역시 포함 되고 있으며, C6, C8, C9 등의 관리과정과 A.8, A.9, A.11, A.12, A14 등의 통제항목은 SOC의 운영 및 정보보호 활동에 직접적인 영향을 미치고 있다.

2.2.3 ISMS-P

ISMS-P(정보보호 및 개인정보보호 관리체계, Personal Information & Information Security Management System) 인증은 기존에 별도로 존재하던 ISMS(정보보호관리체계, Information Security Management System)인증과 PIMS(개인정보보호 관리체계, Personal Information Management System) 인증을 통합 한 것으로, 별도로 관리 되고 있던 정보보호와 개인정보보호 관련 인증을 통합 관리하기 위해 2018년 11월 관련 고시가 개정 되어 현재 운영 중에 있다.

ISMS-P인증은 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제 47조 및 '개인정보 보호법' 제32조의2, '정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시'를 법적 근거로 하고 있으며, 시행령에서 정보보호관리체계 인증의 방법, 절차, 범위, 의무 대상자 등 다양한 사항을 규정하고 있다. ISMS-P 인증을 통해 기업은 체계적, 종합적 정보보호 대책을 구현함으로써 정보보호관리 수준을 향상 시킬 수 있고, 사고 발생 시 신속한 대응 및 피해를 최소화 할 수 있다. 또한 경영진의 정보보호 의사결정의 참여를 유도함으로써 정보보호 업무에 대한 책임성과 신뢰성을 향상시킬 수 있다[16].

ISMS-P 인증은 관리체계 수립 및 운영(16개), 보호대책 요구사항(64개), 개인정보 처리단계 별 요구사항(22개)로 구성되어 있다. 관리체계 수립 및 운영은 관리체계의 메인프레임으로서 전반적인 관리체계 운영 라이프 사이클을 구성하고 있다. 보호대책 요구사항은 총 64개 분야에 대한 인증기준으로써 정책, 조직, 교육 등 관리적 부문과 개발, 보안통제, 운영통제 등 물리적, 기술에 대한 정책 준수 및 검토 등 분야별 관리 운영

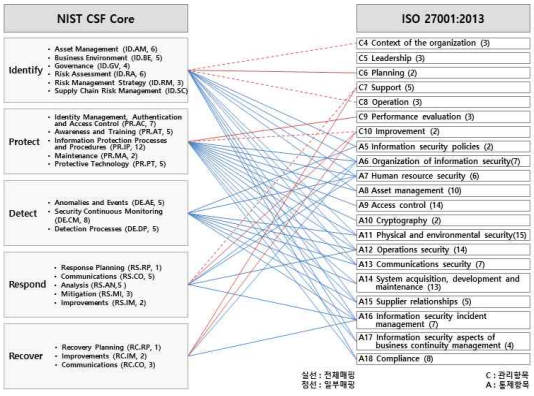
으로 구성하고 있다. 기존 ISMS에서 ISMS-P로 변경되며 추가 된 개인정보 처리단계별 요구사항은 개인정보생명주기에 따른 보호 조치와 관련된 내용으로 구성하고 있다.

3. 기존 프레임워크 비교 분석

SOC의 환경에 맞는 필요한 부분을 도출하기 위해 NIST CSF와 국제 정보보호관리체계를 비교 분석하고, 현재 보안관제전문기업의 관제 프로세스를 살펴보고 특징을 파악한다.

3.1 NIST CSF와 정보보호관리체계 비교

NIST CSF와 다양한 기관에서 프레임워크로 사용하고 있는 국제 정보보호관리체계인 ISO/IEC 27001 항목을 비교해 본 결과, NIST CSF는 정보보호의 흐름을 각각의 기능을 통해 사건의 발생 시간 순(Identify-Protect-Detect-Respond-Recover)으로 표현하는 반면, ISO/IEC 27001은 정보보호를 위한 항목들을 관리항목/통제항목으로 나누어 각각의 항목을 펼쳐서 나열하는 방식으로 표현하고 있다. 각 항목을 그림 2와 같이 매핑 하는 방식으로 비교를 수행하였다.



(그림 2) NIST CSF와 ISO/IEC 27001 항목 매핑

NIST CSF의 경우 ISO/IEC 27001의 통제항목과는 대다수 매핑이 되고 있음을 볼 수 있다. 그러나 각각의 관리항목과의 매핑은 제대로 되고 있지 않음을 확인할 수 있다. 이에 다시 한 번 관리항목에 대해서만 별도 비교를 수행하였다.

관리 항목만을 별도로 비교한 결과 표 2과 같이 ISO/IEC 27001의 관리 항목의 일부분에 대해서만 NIST CSF에 매핑이 되고 있다.

특히 C6 Planning, C7 Support, C10 Improvement 부분은 각각 NIST CSF의 Risk Management, Communication, Improvement 부분으로 매핑이 되었으나, 나머지 항목은 일부 항목만 매핑이 되거나 매핑이 되지 않는 것을 볼 수 있다. 또한, SOC 운영에 대한 SLA(Service Level Agreement), SOC에 대한 평가 지표가 NIST CSF에서는 존재하지 않음을 확인할 수 있다.

<표 2> 관리 항목 비교

NIST CSF	ISO/IEC 27001
Identify	C4 Context of the organization(일부) C6 Planning, C8 Operation(일부)
Protect	C9 Performance evaluation C10 Improvement(일부)
Detect	N/A
Respond	C7 Support(일부) C10 Improvement
Recover	C7 Support C10 Improvement

통제항목의 계획과 실행에 대한 단계별 절차들은 NIST CSF가 정보보호관리체계 보다 더 체계적이다. 이는 NIST CSF의 하위카테고리(108개)가 다른 프레임워크(ISO 27001, COBIT 등)를 참조함으로 적용 가능성이 더 높다. 정보보호관리체계는 조직 전반의 정보를 대상으로 Plan-Do-Check-Act(PDCA)주기를 바탕으로 반복적인 유지, 개선을 제공함으로 관리항목이 좀 더 포괄적이라 할 수 있다.

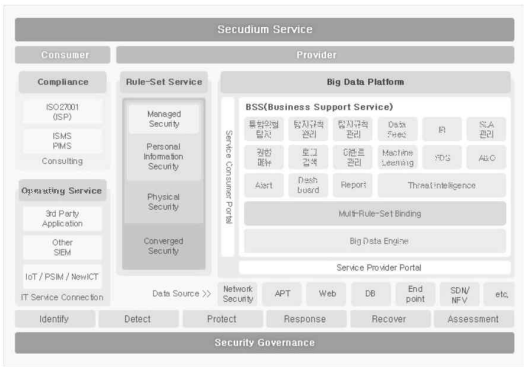
3.2 보안관제전문기업의 보안관제 프로세스

보안관제전문기업들이 사용하는 프레임워크는 보안관제 방법론 또는 보안관제 프로세스라는 이름으로 ISO/IEC 27001이나 ISMS 인증과 같은 정보보호관리체계를 포괄하고 있다는 점에서 강점을 보이며, 각 단계별 항목들은 NIST CSF와 유사한 것을 알 수 있다. 실제 다양한 조직의 SOC에서 보안관제업무를 수행하고 있는 보안관제전문기업의 보안관제 프로세스를 보

면 NIST CSF와 유사한 형태의 프로세스를 운영하고 있다.

그림 3은 보안관제전문기업인 이글루시큐리티의 보안관제 방법론을 나타낸 것으로 수집 > 예방 > 탐지/분석 > 대응 > 보고의 프로세스를 갖추고 있으며[17], 또 다른 보안관제전문기업인 SK인포섹은 그림 4와 같이 보안관제 프로세스가 NIST CSF와 유사한 Identify > Detect > Protect > Response > Recover > Assesment의 절차를 보이고 있고 평가절차가 포함되어 있다[18].

(그림 3) 이글루시큐리티 보안관제 프로세스



(그림 4) SK인포섹 보안관제 프로세스

보안관제전문기업들은 초창기부터 정보보호관리체계를 바탕으로 보안관제 및 운영 프로세스를 만들어 사용해 왔는데 절차와 일부 항목들은 최근에 발표된 NIST CSF와 유사한 면이 있다. NIST CSF에서 보호(protect) 단계를 보안관제전문기업에서는 예방(prevent) 으로 사용하고 있는데 이는 보안관제 입장에서 보호 활동은 결국 예방 활동의 일환으로 인식되는 것으로 기존의 보안관제 프로세스를 NIST CSF에 접목시키면 체계적인 프레임워크로 활용 가능하다는 것을 보여준다.

3.3 분석결과 및 개선 프레임워크 제안

SOC는 기본적으로 전문 인력들로 운영되기에 사람에 대한 관리(근무체계, 휴식, 교육 등)가 필요하며, 모니터링 및 대응을 위한 관리시스템에 대한 보호 조치와 프로세스에 대해서도 지속적인 검토 및 개선, 평가가 요구되기에 별도의 관리 기능을 도출하여 운영하는 것이 필요하다.

NIST CSF와 정보보호관리체계, 그리고 국내 보안관제전문기업의 보안관제 프로세스 등을 비교 분석 한 결과, NIST CSF의 절차적 실행 항목과 정보보호관리체계의 관리 항목, 보안관제전문기업의 보안관제 프로세스에 포함되어 있는 관리적 기능을 종합하여 SOC의 환경에 맞는 사이버보안 프레임워크를 제안한다.

제안하는 프레임워크는 앞서 비교 분석한 내용을 토대로 기존 NIST CSF의 5가지 기능에 관리 기능을 추가하여 확장된 6개 기능으로 개선하고자 한다.

관리 기능으로 추가하고자 하는 각 항목은 정보보호관리체계의 관리 항목을 참조하고 SOC의 특성을 고려하여 표 3과 같이 추가적으로 보완할 관리 항목을 도출하였다.

<표 3> 도출한 관리 항목

구분	항 목	기호
1	운영 프로세스 수립	M1
2	관리체계 인증 획득	M2
3	평가제도 수립	M3
4	인력관리 및 근무체계	M4
5	서비스수준관리	M5
6	SOC의 보호 조치	M6
7	사업관리 프로세스	M7
8	지침절차 수립	M8
9	보고체계 수립	M9

4. 개선 프레임워크의 내용 타당성

개선하고자 하는 프레임워크의 관리적 항목에 대한 내용 타당성 검증을 위해 3장에서 도출한 결과를 토대로 NIST CSF를 SOC의 프레임워크로 활용함에 있어 관리적인 부분의 부족함이 없는지, 관리 항목을 별도로 도출할 필요가 있는지 의견을 수렴하고 도출 항목의 적정성을 검증하기 위한 목적으로 전문가 집단을 구성하여 델파이 기법을 사용하였다.

그리고 결과에 대한 검증도구로는 Lawshe(1975)가 제시한 내적 타당도 비율(Content Validity Ratio; CVR)을 활용하였다.

4.1 전문가 집단 구성

델파이 기법에서 의미 있는 결과를 산출하기 위해 가장 중요한 것은 전문성을 가진 패널을 선정하는 것이다[19][20]. 따라서 본 연구에서 전문가 패널 선정의 조건은 보안관제 업무의 특수성에 비추어 정보보호관련 업무 경력이 5년 이상인자로 보안관제 업무를 실제 수행하고 있는 실무관련 전문가와 정보보호관리체계 관련 컨설팅 인력으로 구성하였다.

본 연구에서는 관리 항목에 대한 필요성과 적정성에 대해 검증하기 위해 총 17명의 전문가를 구성하였으며, 전문가 집단 구성 내용은 표 4과 같다.

<표 4> 전문가 집단 구성

구분	대 상	인원	비율
업무 영역	공공기관 사이버안전센터 운영 관리자	5	29%
	금융기관 보안관제센터 운영 관리자	2	12%
	기업 보안관제센터 운영 관리자	3	18%
	ISMS, ISO 27001 인증심사원	4	23%
	보안관제 전문기업 연구원(수석급)	3	18%
소계		17	100%
정보 보호 경력	5~7년	4	24%
	8~10년	4	24%
	10년 이상	9	52%

4.2 조사 및 결과

관리 기능의 필요성 및 도출한 관리 항목의 타당성을 파악하기 위해 1차 조사에서는 관리 기능 및 관리 항목을 상세한 설명과 함께 제시하고, 해당 기능 및 항목이 SOC에 적용할 필요가 있는지에 대해 자유롭게 기술하는 개방적 설문을 수행하였다.

설문 결과, 관리 기능의 추가를 통한 보완의 필요성에 대해서는 모두(100%) 긍정적인 의견을 보였고, CVR 값이 1로써 응답인원이 17명일 때의 최소 CVR인 0.48[5]보다 높으므로 결과가 타당하다고 볼 수 있다. 관리 항목에 대해서는 모두 필요하다는 의견이 2명(11.8%), 필요성 측면에서 일부 항목의 적용은 동의할 수 없다는 의견이 9명(52.9%), 시간 및 비용 측면에서 일부 항목에 대한 적용은 동의할 수 없다는 의견이 6명(35.3%)으로 나타났다. 이 중 M4(인력관리 및 근무체계) 항목은 13명(72.2%)이 공통적으로 M1(운영 프로세스 수립)에 포함되어야 한다는 의견을 제시하였고, CVR 값이 0.53으로 M4가 M1에 포함될 수 있는 근거라고 볼 수 있다.

1차 조사에서 관리 기능에 대해서는 필요성이 입증되었으나 관리 항목에 대해서는 일부 이견이 존재하므로 관리 항목들에 대해 정량적으로 파악하기 위해 2차 조사로써 관리 항목의 적용 여부에 대한 설문 조사를 수행하였다.

설문 조사는 1차 조사의 결과를 반영하여 관리 항목에서 M4(인력관리 및 근무체계)를 제거하고, 각 항목별로 중요하다고 생각하는지(중요성)와 적용하기 쉽다고 생각하는지(용이성)의 두 가지 관점에서 각각 5점 척도를 사용하였다. 5점 척도에서 4점 이상일 경우 해당 질문에 대한 긍정적인 반응으로 판단하였고, 결과는 표 5와 같다.

<표 5> 내용 타당성에 대한 결과

항목	중요성			용이성		
	평균	표준 편차	CVR	평균	표준 편차	CVR
M1	4.88	0.32	1.00	4.88	0.32	1.00
M2	4.12	0.32	1.00	4.12	0.47	0.88
M3	4.94	0.24	1.00	4.94	0.24	1.00
M5	4.65	0.59	0.88	4.76	0.42	1.00
M6	4.29	0.46	1.00	4.24	0.55	0.88
M7	3.71	0.46	0.41	3.65	0.48	0.29
M8	4.41	0.49	1.00	4.47	0.50	1.00
M9	3.59	0.60	0.29	3.53	0.61	0.18

5) Lawshe (1975), 17명에 대한 내용 타당도 비율(CVR)의 최소값=0.48, p=0.05

M7(사업관리 프로세스)과 M9(보고체계 수립)을 제외한 전 항목에서 중요성과 용이성이 최소 CVR 값보다 높으므로 해당 항목들이 필요하다는 근거가 될 수 있고, M7과 M9은 평균값이 타 항목보다 낮고, 중요성과 용이성의 CVR 값이 모두 최소보다 낮으므로 해당 항목들의 필요성을 입증하는 근거로는 부족하다.

M7과 M9의 평균 및 CVR 값이 다른 항목에 비해 낮은 이유로 M7은 발주자 입장과는 달리 관제업무를 수행하는 운영자 입장에서는 상대적으로 필요성이 낮게 나타났다. 이는 SLA와 인력관리부분이 사업관리의 핵심이므로 별도로 도출할 필요가 없다는 의견이며, 전문가 집단에 발주자를 포함하는 구성에 따라 달라질 수 있는 항목이다. M9는 기존의 대응절차에 포함된 내용이므로 별도의 관리 항목으로 분리할 필요가 없는 것으로 나타났다. 본 연구에서는 M7과 M9는 CVR 값을 근거로 우선 제외키로 하였다.

3차 조사에서는 2차 조사 결과를 반영하여 M7과 M9을 제외한 항목에 대하여 2차와 동일한 설문을 수행하였으며, 결과는 표 6과 같다.

<표 6> 정리된 항목의 결과

항목	평균	표준편차	CVR	우선순위
M1	4.88	0.32	1.00	2
M2	4.15	0.49	0.88	6
M3	4.94	0.24	1.00	1
M5	4.74	0.44	1.00	3
M6	4.21	0.63	0.76	4
M8	4.18	0.56	0.82	5

2차 조사의 결과와 같이 모든 항목이 의미가 있음을 알 수 있으며, 평균값과 표준편차를 기준으로 산정한 우선순위는 표 7과 같다.

<표 7> 항목의 우선순위

우선순위	항목	항목 내용
1	M3	평가제도 수립
2	M1	운영 프로세스 수립
3	M5	서비스수준관리
4	M6	SOC의 보호 조치
5	M8	지침절차 수립
6	M2	관리체계 인증 획득

4.3 보완할 항목에 대한 결과

도출된 항목들 중 M3, M5는 평가와 관련된 항목으로 분류할 수 있으며, M1, M2, M6, M8은 운영관리 항목으로 분류할 수 있다. 또한 서비스수준관리와 SOC 자체 평가 항목이 상위를 기록하였는데 이는 평가 지표를 개발하고 지속적인 관리를 통해 SOC의 수준 향상을 위한 강력한 수단으로 SOC의 필수항목으로 판단된다. 운영관리 항목들은 NIST CSF의 기능에 포함하기 어려운 항목들로 SOC를 운영하기 위한 인력관리, 절차·지침, SOC자체 통제 등으로 SOC의 특성에 따라 필요한 항목이다. 이러한 내용들을 NIST CSF와 같은 형태의 카테고리로 구분 지으면 표 8과 같이 6개로 구분 될 수 있으며 이 기능을 Management(MG)로 명명하였다.

<표 8> SOC 관리 기능의 항목

카테고리	내용
MG.SE : SOC Evaluation (SOC평가)	SOC에 대한 정기적인 수준평가를 통해 SOC의 인적, 관리적, 시스템적 수준을 파악하고 개선한다.
MG.OP : Operation (운영)	SOC의 업무소요량, 요구사항 분석 등을 통해 관제 방법을 결정하고 SOC 근무체계 및 인력관리방안을 포함하여 관제체계를 구현한다.
MG.SL : SLA (서비스수준)	SLA는 SOC의 서비스 수준을 지속적, 안정적으로 유지시켜주며, 이를 위해서는 평가지표를 개발하고, 지속적으로 개선한다.
MG.CE : Certification (인증)	SOC에 대한 정보보호관리체계 인증제도를 통해 대내외적인 서비스 수준을 관리한다.
MG.PP : Manual & Process (지침/절차)	SOC와 관련 된 지침 및 절차가 명확해야 하며, 지속적으로 변하는 위협과 자산에 따라 개선 활동을 수행한다.
MG.SP : SOC Protection (SOC보호)	SOC에 대한 물리적 기술적 보호 조치 및 관리를 통해 SOC를 보호한다

또한 SOC 관리기능의 각 카테고리 별 실제로 수행해야 하는 업무들을 표 9와 같이 19개의 하위 카테고리로 정의 하였다.

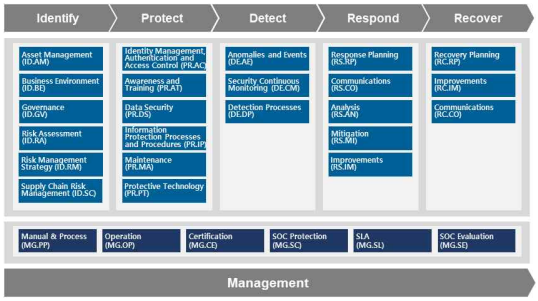
<표 9> SOC 관리 기능의 상세항목

카테고리	하위 카테고리	내용
MG.SE (평가)	MG.SE-1	SOC수준 평가 절차 개발
	MG.SE-2	SOC수준 평가
	MG.SE-3	평가 결과에 따른 개선
MG.OP (운영)	MG.OP-1	SOC 운영 근무 체계 구성
	MG.OP-2	SOC 운영 인력 관리
	MG.OP-3	SOC 운영 시스템 구성
	MG.OP-4	SOC 운영 시스템 관리
	MG.OP-5	SOC 운영 프로세스 구성
	MG.OP-6	SOC 운영 프로세스 관리
MG.SL : (서비스수준)	MG.SL-1	SLA 항목 및 지표 정의
	MG.SL-2	SLA 적용 및 운영
	MG.SL-3	SLA 항목 및 지표 개선
MG.CE : (인증)	MG.CE-1	관리체계 인증제도 취득
	MG.CE-2	관리체계에 부합 된 운영
	MG.CE-3	관리체계 운영 개선
MG.PP : (지침/절차)	MG.PP-1	지침 절차서 재·개정
	MG.PP-2	지침 절차서 관리
MG.SP : (SOC보호)	MG.SP-1	SOC 물리적 보호
	MG.SP-2	SOC 접근통제정책

4.4 개선된 프레임워크

NIST CSF에서 이미 구현되어 있는 5개의 기능(Identify-Protect-Detect-Respond-Recover)을 기반으로 Management 기능을 추가하여 그림 5와 같이 NIST CSF를 확장한 SOC를 위한 사이버보안 프레임워크를 구현하였다.

관리 기능은 SOC의 특정 단계가 아닌 전 과정에서 관여되어야 하며, 지속적으로 개선, 적용되어야 하는 순환구조로 적용하였다.



(그림 5) SOC를 위한 개선된 프레임워크 모형

5. 결 론

본 연구에서는 SOC를 위한 확장된 사이버보안 프레임워크를 제안하였다. NIST CSF를 기반으로 기존의 5개 기능에서 관리 기능을 추가하여 6개의 기능으로 재구성 하였다. 정보보호관리체계와 달리 SOC 운영 시 발생할 수 있는 일련의 시간 흐름(식별>보호>탐지>대응>복구) 및 이 흐름을 아우를 수 있는 관리 기능을 통해 일회성이 아닌 지속적인 SOC 운영 및 관리가 가능하도록 프레임워크를 구성하였다.

SOC는 사람-기술-프로세스로 구성되어 운영되지만, 이러한 요소들이 안정적이고 지속적으로 수행하기 위해서는 사전 정의된 관리절차가 필요하다. SOC는 기본적으로 전문 인력들로 운영되기에 사람에 대한 관리가 필요하며, 모니터링 및 대응을 위한 시스템과 물리적인 공간에 대한 적절한 접근통제와 관리가 필요하다. 또한 프로세스에 대해서도 지속적인 검토 및 평가, 개선이 필요하기에 별도의 관리 항목을 도출하여 운영하는 것이 중요하다.

본 연구의 향후 과제로는 NIST CSF의 상위 기능과 기능에 속해야 할 실제 하위 카테고리(108개)에 대해 SOC의 업무와 연결지어 필요한 항목을 도출할 필요가 있으며, 국내 SOC의 특성 중 아웃소싱을 통한 운영이 많으므로 조사 대상의 범위도 넓혀 발주자를 포함하여 연구할 필요가 있다.

사이버 공격은 대상과 시기를 제어 할 수는 없지만 공격과 사고에 대한 대응방법을 관리 할 수는 있다. 그러기 위해 SOC의 사이버보안 프레임워크를 준비하는데 있어 본 연구가 참조 모형이 될 수 있을 것으로 기대된다.

참고문헌

[1] Symantec, “Internet Security Threat Report”, Vol. 23, 2018.

[2] Forbes, https://www.forbes.com/sites/eycybersecurity/2017/05/09/why-your-business-needs-a-security-operations-center/#15dfe18642aa, (2019.1.15.).

[3] Stef Schinagl, Keith Schoon, Ronald Paans, “A Framework for Designing a Security Operations Centre (SOC)”, 48th Hawaii International Conference on System Sciences, IEEE, 2015.
[4] 윤오준 외, “주요국의 사이버위협정보 공유체계 분석을 통한 국내 적용모델 연구”, 융합보안논문지, 제16권, 제7호, pp.101-111, 2016.
[5] 차병래 외, “Cybersecurity를 위한 SOC & SIEM 기술의 동향”, 스마트미디어저널, 제6권, 제4호, pp.44-49, 2017.
[6] Alissa Torres, “Building a World-Class Security Operation Center: A Roadmap”, SANS, 2015.
[7] 국가정보원, 과학기술정보통신부, 방송통신위원회, 행정안전부, 금융위원회, “2018 국가정보보호백서”, 2018.
[8] 권성문 외, “기반시설 사이버보안 프레임워크 도출방안”, 정보보호학회논문지, 제27권, 제2호, pp.241-250, 2017.
[9] 이수연 외, “주요기반시설 서비스의 안정적 운영을 위한 보안 프레임워크 설계에 관한 연구”, 한국IT서비스학회논문지, 제15권, 제4호, pp.63-72, 2016.
[10] 이상도 외, “제어시설 사이버공격 대응을 위한 사이버보안 프레임워크 연구”, 예술인문사회융합멀티미디어논문지 제8권, 제4호, pp.285-296, 2018.
[11] 김민준, 김귀남, “정보보안 거버넌스 프레임워크에 관한 연구”, 융합보안논문지, 제10권, 제4호, pp.13-19, 2010.
[12] 김점구, 노시춘, “의료정보보안 기반 소프트웨어 아키텍처 설계방법”, 융합보안논문지, 제13권, 제6호, pp.35-41, 2013.
[13] 송은지, 강원영, “미국 오바마 정부 2기의 사이버보안 강화 정책”, INTERNET & SECURITY FOCUS, KISA, 2014.
[14] NIST, “Framework for Improving Critical Infrastructure Cybersecurity,” Version 1.1, 2018.
[15] ISO, https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en
[16] 한국인터넷진흥원, “정보보호 및 개인정보보호 관리체계(ISMS-P) 인증제도 안내서”, 2019.
[17] IGLOO Security, http://www.igloosec.co.kr/en/ig/Service_Managed%20Security_MSS%20Process, (2018.8.30).
[18] SK Infosec, http://www.skinfo sec.com/ko/control/method.jsp, (2018.8.30).
[19] 강용주, “델파이 기법의 이해와 적용사례”, 한국장애인고용공단, EDI보고서, 수시 08-20, 2008.
[20] 이종성, ‘델파이 방법(연구방법21)’, 교육과학사, 2001.

[저 자 소 개]

조 창 섭 (Changseob Cho)
1992년 2월 동국대학교 학사
2015년 3월 숭실대학교 IT정책경영학과 석박사 통합과정
email : aisoc@naver.com

신 용 태 (Yongtae Shin)
1985년 2월 한양대학교 학사
1994년 2월 美아이오아대학교대학원 컴퓨터공학과 석・박사
1994년 美미시간주립대 교수
1995년~숭실대학교 컴퓨터학부 교수
email : shin@ssu.ac.kr