사이버 복원력 도입을 위한 평가모델 연구

황재호[1], 오호성[2], 서수연[1], 민무홍[3]
[1]성균관대학교 실감미디어공학과 석박통합과정
[2]한국문화진흥(주) 뉴서울컨트리클럽
[3]성균관대학교 학부대학 조교수
ashiereki@g.skku.edu, hsoh@newseoulgolf.co.kr, sooyon1119@g.skku.edu, iceo@skku.edu

Research on evaluation models for cyber resilience adoption

Jaeho Hwang[1], Hosung Oh[2], Sooyon Seo[1], Moohong Min[3]
[1]Dep. of Immersive Media Engineering, Sungkyunkwan University
[2]Korea Culture Promotion Corporation, newseoul country club
[3]University College, Sungkyunkwan University

요 약

사이버 공격과 위협은 예측 불가능한 수준으로 높아지고 있어 해킹 위협을 완벽히 차단하고 예방하는 것은 현실적으로 불가능하다. 따라서 사이버 공간의 공격이 발생했을 경우 신속한 대응 및 시스템의 생존성 보장을 위해서 사이버 복원력이 필요하다. 우리는 정부, 공공기관, 기업이 사이버 복원력 개념을 도입하고 내재화를 위한 평가모델을 연구하였다.

1. 서론

디지털 기술은 일상의 변화와 기술 산업의 발전을 넘어 정치 · 경제 · 사회문화 등 국가와 사회의 모든 부문에서 혁신의 기반이 된다. 글로벌 패권 경쟁의 심화, 저성장 및 양극화, 기후 변화 등 대내외적 변화와 위기에 대한 해법이자 국가 경쟁력과 지속 가능한 발전의 근원으로 디지털 기술과 이를 활용한 사이버 공간의 중요성이 그 어느 때보다 높은 시점이라 볼 수 있다.

사이버 공간은 다양한 하드웨어와 소프트웨어로 정의되는 컴퓨터 네트워크로 연결성과 개방성이 급격히 확대되며 기하급수적으로 복잡한 구조이다. 무질서한 배열로 악의적인 공격자가 쉽게 숨어 악용할 수 있는 다양한 보안 취약점을 내포할 수 있으며, 최근 인공지능 등 혁신 기술의 발전과 디지털 자산 거래 확대에 따라 중요성이 증가하고 관련 범죄가 급증하는 추세이다. 사이버 공간의 공격이 발생했을 경우 신속한 대응 및 시스템의 생존 확률을 보장하기 위해서 사이버 복원력이 필요하다.

2022년 SK C&C에서 운영하는 IDC가 입주한 건물의 전기실에서 화재가 발생했고, 서버 작동에 필요한 전원 공급이 끊겨 카카오의 서비스를 비롯한 많은 서비스가 중단되었다[1]. 완전한 서비스 복구까지 5일이 소요되었으며, 해당 기업은 손해배상청구소송 및 이용자 이탈 등을 겪었다. 해당 기업은 국내 정보보호 관리체계 인증(ISMS) 기관임에도 불구하고, 정보보호 관리체계가 정상 작동이 되지 않은 점은 사이버 복원력을 충분히 다루고 있지 않거나, 평가항목 간 여러 방법으로 상호 작용이 되지 않음을 입증한다.

따라서, 사이버 복원력은 기업이나 조직에 있어서 중요한 요소가 될 수 있으며, 우리는 본 연구를 통해 **사이버 복원력 도입 시 고려해야 할 평가모델에 대해 살펴보고 국내 정보보호 관리체계 인증과 상생할 수 있는 평가모델을 제시**하고자 한다.

2. 선행연구

사이버 복원력의 개념과 특징을 정의하고, 국내 · 외 공신력 있는 기관에서 제시된 사이버 복원력 정책 동향과 방향성의 문헌 연구를 수행했다.

2.1. 사이버 복원력의 정의

복원력이란 개념은 생태학적 관점, 재난연구 등 생물학 및 사회학 관점에 맞춰 연구를 진행했으며, '사이버 복원력'이란 개념은 사이버 공간 등장 이후 사이버 공간에 위협을 주는 여러 요소에 대응하기 위해 생겨났다. 즉, 재난연구에서 사용되던 복원력 개념을 사이버 공간에 결합시킨 개념이다. 최근 급격히 증가하고 있는 사이버 침해사고나 기술환경 변화 등에 따라 사이버 복원력에 대한 필요성이 대두되기 시작했으며, 다양한 기관에서 용어의 개념에 대해 정의하고 있다[13].

본 연구는 사이버 복원력에 대한 다양한 정의 중 미국국립표준기술연구소(NIST)에서 제시한 **'사이버 자산을 사용하거나 이를 활용하는 시스템에 대한 공격을 예측(Anticipate)하고, 견디며(Withstand), 이로부터 회복(Recover)하고 적응(Adapt)하는 능력'**으로 정의하고 연구를 진행했다.

2.2. 선진국 정책 동향

2.2.1. 미국

바이든 정부의 사이버안보 정책 기조는 2021년 3월 3일 발표된 「잠정 국가안보 전략 지침」을 기반으로 추진하였으며, 미국 국가안보 전략 발표를 통해 위협을 관리하기 위한 정책 수립, 구현 및 검토 등을 위한 필요 사항을 제시하고 있다[12].

특히, 사이버 안보가 중요하다는 인식하에 미국 내 사이버 방어가 효과적으로 집행될 수 있도록 오류 발생 시 신속한 복원력 구축을 제시했다. R&D 우선순위 역시 큰 흐름에서 벗어나지 않는다. '24년 회계연도 예산에 대한 다중 기관 연구 및 개발 우선순위는 탄력적이고 안전한 통신을 우선시하고, 사이버 공격 및 공급망 공격으로부터 중요한 인프라와 민감한 네트워크를 방어 하는 등, 시스템의 보안 및 사이버 복원력에 초점을 두고 있다[2].

2.2.2. EU(European Union)

EU는 기업 및 조직의 사이버 보안 책임성 강화, 제품의 보안, 신뢰성 향상, 사이버 복원력(Cyber Resilience)을 강조하고 있다[3].

EU는 사이버 복원력 법 제정을 추진하고 있으며 주요 내용으로는 디지털 요소가 있는 제품에 대한 계획, 설계, 개발, 생산, 납품 및 유지보수 등 제조업체, 수입업체 및 유통업체 전체 라이프 사이클에 사이버 보안 의무를 부과하는 규정이 담겨 있다[4].

장치나 네트워크에 대한 직/간접 또는 논리적, 물리적인 데이터 연결을 포함하는 디지털 요소를 가진 제품을 규율 대상으로 한다.

EU 사이버 보안 입법의 방향성을 보면 사이버 복원력을 지속해서 강조하고 있으며, EU 디지털 및 사이버 보안 정책이 핵심 개념으로 자리 잡고 있다.

2.3. 국내 · 외 기관 동향

2.3.1. CPMI(Committee on Payments and Market Infrastructures)

글로벌 기관 중 CPMI, 국제결제은행의 산하 위원회로 FMI(Financial Market Infrastructure)의 사이버 복원력 제고를 위해 2016년 사이버 복원력 가이던스를 발표했다. 가이던스는 국제 기준인 금융시장 인프라에 관한 원칙(PFMI)을 기반으로 사이버 공격에 대비하여 마련해야 하는 업무 복원력 관련 조치 사항 및 이에 대한 충족도 측정을 위한 세부 권고사항을 명시했다[5]. 관리체계 항목은 5개의 주요 관리 항목과 3개 지원 항목으로 구성되었으며, 사이버 공격의 범위가 매우 광범위한 점을 감안하여 금융당국, 금융기관, IT업체, 수사기관 등 관련 기관 간 협력 강화 필요성을 강조했다. 해당 관리체계는 CPMI 산하 사이버 복원력 평가전문단이 진행하며, 각국의 자체평가, 검토 및 확인 작업을 통해 지속적인 발전을 시키고 있다[11].

<표 1> CPMI 사이버 복원력 체계 관리 항목

평가항목	내용
지배구조	사이버 복원력 의사결정 체계 수립
식별	중요도 및 외부 위협 평가를 통해 위험도 측정
보호	기밀성, 무결성, 가용성 확보 및 보호 방안 마련
탐지	잠재적 위협 요인을 신속하게 확인 및 탐지
대응 및 복구	업무 지속 계획에 의거한 서비스 재개 및 복구
테스트*	5개 주요 항목의 시나리오 바탕 취약점 평가
상황인지*	공격 별 대응 방안 마련 및 이해관계자와 정보 공유
학습과 발전*	사전 예방 능력 및 관리체계 지속 발전 도모

* 표시 항목은 지원 항목

2.3.2. NIST(National Institute of Standards and Technology)

미국국립표준기술연구소(NIST)는 사이버 보안 관련 위협 관리를 위해 표준, 지침 및 사례 등을 포함한 프레임워크를 지난 2013년부터 발표하여 지속적인 발전을 해오고 있다.

본 프레임워크는 세계적으로 널리 인정받는 평가 기준으로 여겨지고 있으며, 중요 핵심 인프라를 보호하고 복원력 제고를 위한 주요 방법론을 제시하고 있다.

사이버 보안 프레임워크는 5개의 주요 평가항목으로 구성되어 있다. 널리 통용되는 5개 개념에서 다시 23가지 카테고리로 나뉘며 카테고리별 사이버 보안 결과 및 보안 제어에 관한 내용을 기술한 총 108개의 하위 카테고리로 정의하고 있다[6].

아래(표2)는 사이버 보안 위험 관리에 대한 라이프 사이클을 종합적으로 보여준다.

<표 2> NIST 사이버 보안 프레임워크

평가항목	내용
식별	사이버 복원력 의사결정 체계 수립
보호	중요도 및 외부 위협 평가를 통해 위험도 측정
탐지	기밀성, 무결성, 가용성 확보 및 보호 방안 마련
대응	잠재적 위협 요인을 신속하게 확인 및 탐지
복구	업무 지속 계획에 의거한 서비스 재개 및 복구

2.3.3. IACS(International Association of Classification Societies)

국제선급협회(IACS)는 해상업계의 ICT 기술 도입이 사이버 공격의 주요 표적이 되고 있다는 점을 인지하여 사이버 위협에 대응하기 위해 사이버 보안 통합 요구사항(Unified Requirement:UR E27)을 수립했다.

이를 기반으로 2024년 각 선급에서는 선박 건조 시 조선소 및 제조사에 사이버 보안 관련 요건 준수를 강제화할 예정이다.

IACS UR27은 선내 시스템의 사이버 복원력에 대한 전반을 목표로 하고 있으며 선내 시스템 및 장비의 복원력에 대한 최소 요구사항 및 위협관리 5가지 요소가 UR27에 기술되어 있다[7].

<표 3> IACS 통합 요구사항 위협 관리 항목

평가항목	내용
식별	선상 시스템, 인력, 자산, 데이터 등 사이버 위협에 대응하기 위한 조직의 자산 이해
보호	사이버 위협으로부터 선박 보호 및 운송 연속성을 위한 보호장치 개발
탐지	사이버 사고 발생을 미연에 방지하고자 탐지 및 식별을 위한 조치 방안
대응	사이버 사고 발생 시 적절한 조치 및 활동 개발
복구	사이버 사고 발생 시 운송에 필요한 모든 서비스를 복구하기 위한 적절한 조치 및 개발

2.3.4. CISA(Cybersecurity and Infrastructure Security Agency)

사이버보안 및 인프라보안국(CISA)은 미국의 필수 인프라에 대한 보안 및 복원력 평가를 수행한다. CISA는 중요 인프라의 위협을 더 잘 이해하고 복원력을 강화할 기회를 파악하며, 정책 및 투자 결정을 위해 인프라 복원력 계획 프레임워크를 제시한다[8].

CISA는 ICT 인프라뿐만 아니라 정부 시설, 방위산업 기지부터 교통 시스템 등 국가에서 운영하는 광범위한 인프라 복원력 방안을 제공한다.

<표 4> Infrastructure Resilience Planning Framework

평가항목	내용
기반 마련	복원력 계획 작업 정의, 범위 산정, 리소스 검토
인프라 식별	인프라 식별 및 종속성 평가
위험평가	위협과 위험에 대한 취약성 평가
조치개발	위험 해결 및 복원력 강화를 위한 실행 계획 개발
실행 및 평가	인프라 복원력 실행에 따른 성공 측정

2.3.5. 한국은행

한국은행은 금융권에서 빈번하게 발생하는 해킹, 악성코드 배포 등에 대응하기 위해 사이버 보안을 확장한 개념인 사이버 복원력 평가 방안을 모색했다.

한국은행이 정의한 사이버 복원력은 지능적으로 발전하고 있는 사이버 공격으로부터 핵심 업무를 신속하게 복구하여 업무를 재개할 수 있는 능력을 말한다. 해당 능력을 배양하기 위해 FMI(Financial Market

Infrastructure)와 국제 기준인 Guidance on cyber resilience for financial market infrastructure를 기반으로 「사이버 복원력 평가 지침서」를 국내 상황에 맞게 8개 항목 59개 세부 지표로 구성했다[9].

주요 특징으로는 크게 두 가지가 있다. 첫째. 복구목표시간(RTO, Recovery time objective)을 3시간으로 규정하고 있으나 본 평가 지침서에는 국제 기준에 맞춰 2시간으로 권고했다. 둘째. 사이버 위협에 신속히 대응하기 위해 에코시스템을 만들어 시스템 내 참가자 간 상호의존성에 따른 사이버 위협을 식별하고, 사이버 사고 발생 시 효율적인 의사소통 및 정보 공유에 대한 평가를 추가했다.

<표 5> 한국은행 사이버 복원력 평가 지침서

평가항목	내용
지배구조	정책의 수립, 구현 및 검토업무 수행
식별	핵심 업무와 정보자산, 시스템접근 등 분류 및 파악
보호	기밀성, 무결성, 가용성 확보 및 보호 방안 마련
탐지	사이버 침해 가능성 및 비정상적인 공격 탐지
대응 및 복구	주요 업무를 2시간 이내 재개 가능토록 시스템 설계
테스트	사이버 복원력 관리체계 모든 구성 요소 테스트
상황인지	사이버 공격에 대한 대응과 복구 능력 제고
학습과 발전	사이버 복원력 관리체계 지속적인 재평가 및 개선 실시

3. 사이버 복원력 평가모델 구성요소

본 장에서는 2장에서 연구한 이론적 고찰을 바탕으로 실효성 높은 평가모델을 수립하기 위해 사이버 복원력 평가모델의 목적 및 목표를 제시했다. 평가모델의 목적과 목표는 평가모델 수립의 방향성이 되어 실효성 높은 평가모델을 도출하는데 기준이 된다.

3.1. 사이버 복원력 목적 및 목표

명확한 목표와 목적을 설정하는 것은 인프라 보안 및 복원력의 평가항목과 세부 이행과제를 정의하는 토대이기 때문에, 성공적인 계획 수립을 위해서는 필수적으로 진행되어야 한다.

성공적인 목적 및 목표 개발에는 중요한 인프라 시스템뿐만 지속 가능성, 환경, 형평성 등 다양한 요소를 고려해야 한다. 다만, 우리는 인프라 복원력 중 정보 기술에 국한된 사이버 복원력에 대한 평가모델을 제안하기 때문에 NIST에서 제시하는 「사이버 복원력 시스템 개발」을 참고하고자 한다. 이를 근거로 사이버 복원력 목적은 다음과 같이 도출했다[10].

<표 6> 사이버 복원력 목적

목적	내용
1. 예측 (Anticipate)	선제적 대응을 위한 적극적 사이버 방어 전환을 위해 지연, 회피, 방지, 계획, 준비, 변화 방법을 활용하여 사전에 예측함
2. 내구성 (Withstand)	위협이 발견되지 않은 때라도 잠재적인 위협의 실현을 견디기 위한 전략을 내구성이라고 함
3. 회복 (Recover)	사이버 공격 이후 중요한 기능을 수행하기 위하여 회귀, 재구성, 대체, 탐지 방법을 활용
4.적응 (Adapt)	사이버 재공격 방지를 위해 취약점 교정, 방어 강화, 위협에 대한 제어 및 훈련을 말함

사이버 복원력 목표는 시스템이 운영 환경에서 임무 보장 및 복원력을 위해 라이프 사이클 동안 무엇을 달성해야 하는지에 관한 것이다.

사이버 복원력 목표 설정이 명확해야 복원 우선순위와 제대로 된 평가를 가능하게 한다[10].

<표 7> 사이버 복원력 목표

목표	내용
방지 또는 회피 (Prevent or Avoid)	본 목표는 다른 위험 대응 접근방법을 위한 조직의 연관성과 관련된다. 위험 회피 또는 위협 회피는 가능한 위험 대응 접근방법의 하나이고 제한된 환경에서 가능하다. 위협 이벤트를 막는 것은 가능한 위험 대응이다
준비 (Prepare)	본 목표는 예측된 사고를 예방하기 위해 조직의 지속 계획, 지속 운영 계획(COOP), 연습, 훈련, 중요 시스템 및 인프라를 위한 사고 대응 및 회복 계획과 관련된다.
지속 (Continue)	본 목표는 중요 자산의 식별과 관련된다. 중요 자산 및 서비스를 식별하여 비즈니스 연속성을 보장한다.
제한 (Constrain)	본 목표는 특히 중요하고 높은 가치의 자산에 적용된다. 민감한 정보를 포함하고 처리하는 자산은 위협으로부터 손해를 제한하는 것과 관련된다.
재구성 (Reconstitute)	본 목표는 손상된 기능을 회복하여 서비스가 지속될 수 있도록 인프라 구성을 재구성하는 것을 말한다.

이해 (Understand)	본 목표는 다른 모든 목표의 달성을 지원한다. 특히, 준비, 재구성, 변환 및 재설계와 관련되며 사이버 위협 등에 대해 중요 자원의 상태를 유지하는 것을 말한다.
변환 (Transform)	본 목표는 필수 자산과 필수 기능 보장을 위해 민감하게 환경 변화를 예측하여 비즈니스 기능과 프로세스를 효과적으로 수정한다.
재설계 (Re-architect)	본 목표는 시스템 구조와 임무 구조에 적용된다. 임무 또는 비즈니스 기능을 지원하는 시스템의 기술구조를 포함한다.

3.2. 사이버 복원력 기술 및 구성요소

위 3.1. 장에서 제시된 사이버 복원력 목적과 목표 설정이 완료되면, 이를 달성하기 위한 핵심 기술을 도출할 수 있다.

해당 기술은 아래 표와 같으며, 국내 정보보호 관리체계 평가항목에서 제시하는 기술과 일치 여부 검토를 위해 최종 평가모델 제안 시 새로 도출된 평가지표와 정보보호 관리체계 평가지표의 연관성을 확인한다.

(그림 1) 사이버 복원력 구성요소

4. 사이버 복원력 도입을 위한 평가모델 제안

본 장에서는 3장에서 도출된 사이버 복원력 평가항목 6개와 평가지표 15개를 국내 정보보호 관리체계와 상생 가능토록 연관성이 높은 평가항목 간 매칭을 수행했다. 또한, 위험 유형을 사이버 공격과 재난 상황 발생 2개로 구분하여 실제 정부, 공공기관 및 기업에서 적용이 용이하도록 시간의 경과에 맞춰 사이버 복원력 평가모델을 제안했다.

4.1. 사이버 복원력 평가항목

사이버 복원력의 단계별 평가항목 도출을 위해 국내 · 외 기관에서 적용 중인 사이버 복원력 평가항목을 비교 분석하고, 3장에서 도출한 사이버 복원력 구성요소 달성에 충족되는 최종 평가항목을 도출한다.

<표 8> 국내·외 기관 사이버 복원력 평가항목 비교

구분	CPMI	NIST	IACS	CISA	한국은행	평가항목
지배구조	○				○	정책
기반마련				○		
식별	○	○	○	○	○	식별
위험평가				○		
탐지	○	○	○		○	예측
조치개발				○		
테스트	○				○	내구성
보호	○	○	○		○	
대응및복구	○	○	○	○	○	회복
상황인지	○				○	
학습및발전	○				○	학습및발전
실행및평가				○		

사이버 복원력 평가항목은 6단계로 도출되었으며 정책, 식별, 예측, 내구성, 회복, 학습 및 발전으로 구성되어 있다.

정책(Policy)은 사이버 복원력의 중요성을 인지하고, 사이버 복원력을 강화하기 위한 계획을 수립 및 점검하여 평가하는 영역. **식별(Identification)**은 보호해야 할 우선순위를 정하고 핵심 업무와 이를 지원하는 정보 자산을 구분하는 영역. **예측(Anticipate)**은 외부의 위협에 대해

선제 대응을 위한 적극적 사이버 방어 방식을 제시하는 영역. **내구성(Withstand)**은 외부의 위협으로부터 견딜 수 있는 시스템의 내재적 강도와 관련된 영역. **회복(Recover)**은 사이버 공격 이후 신속한 시간 안에 시스템 기능의 복구 가능 여부와 관련된 영역. **학습 및 발전(Learning & Evolving)**은 사이버 복원력 관리체계에 사이버 위협 경감 전략을 반영하고, 조직 내 모든 부문에서 사이버 복원력 관리체계의 지속적인 재평가 및 개선 등 사이버 위협에 대한 조직 내 인식 강화 영역이다.

<표 9> 사이버 복원력 평가항목 도출

단계	평가 항목	정의
1	정책	▶ 기반 마련하기 커뮤니티는 계획 작업을 정의하고 범위를 정하며 계획 작업을 실행할 계획 팀을 구성하고 기존 데이터, 계획, 연구, 지도 및 기타 리소스를 검토
2	식별	▶ 중요 인프라 식별 커뮤니티에 인프라를 식별하고 우선순위를 정하고 인프라 시스템 간의 종속성을 평가하는 방법에 대한 지침 제공
3	예측	▶ 위험 평가 커뮤니티를 대상으로 프로세스 진행 위협과 위험에 대한 취약성을 평가하고 이로 인해 초래될 수 있는 결과를 평가하는 것을 포함하여 중요 인프라의 위험 평가 수행
4	내구성	▶ 조치 개발 잠재적 솔루션을 식별하고 우선순위를 정하여 위험을 해결하고 인프라 복원력을 강화하기 위한 전략적 실행 계획 개발에 대한 지침 제공
5	회복	▶ 실행 및 평가 인프라 복원력 프로젝트와 전략을 커뮤니티 및 지역 계획과 프로세스에 통합하여 성공을 측정하는데 중점
6	학습 및 발전	▶ 비즈니스 연속성 확보 사이버 위협 경감 전략을 반영하고, 지속적인 재평가 및 개선 등 사이버 위협에 대한 조직 내 인식 강화

4.2. 사이버 복원력 평가지표

4.2.1. 정책(Policy)

정책은 위협을 관리하기 위한 정책 수립, 구현 및 검토 등을 위한 필요 사항을 제시한다. 정책에서 주요하게 보는 평가지표는 크게 3가지로 첫째. 관리주체 설정 및 범위 선정, 둘째. 정책의 수립, 셋째. 정책의 유지관리이다.

관리주체 설정 및 범위는 사이버 복원력 평가모델을 조직에 내재화하고 문제 발생 시 평가모델이 즉시 작동될 수 있도록 기반 조직을 구성하는 것이다.

정책의 수립은 내부 규정과 관련 지침을 경영진 승인을 받고 제정하여 임직원 및 관리자에게 명확하게 제시하여야 한다.

정책의 유지관리는 관련 법령 및 규제, 상위 조직 및 관련 기관 정책과의 연계성, 조직의 대내외 환경 변화 등에 따라 주기적으로 검토하여 필요한 경우 제·개정하고 그 내용을 이력 관리하는 것이 필요하다.

<표 10> 사이버 복원력 평가항목 A.정책

사이버 복원력 평가모델		정보보호 관리체계 인증
평가 항목	평가 지표	
A. 정책	A.1. 관리주체 설정 및 범위 선정	1.1.1. 경영진의 참여 1.1.2. 최고책임자 지정 1.1.3. 조직구성 1.1.4. 범위설정 1.1.6. 자원할당
	A.2. 정책의 수립	1.1.5. 정책 수립
	A.3. 정책의 유지관리	2.1.1. 정책의 유지관리 2.1.2. 조직의 유지관리

4.2.2. 식별(Identification)

식별은 조직에 인프라를 식별하고, 중요도에 따라 우선순위를 정하여 인프라 시스템 간의 종속성을 평가하는 방법에 대한 지침을 제공한다.

평가항목 식별에 관련된 지표는 첫째. 자산의 식별, 둘째. 인적 자산의 식별, 셋째. 물리 자산의 식별을 말한다. 국내외 사이버 복원력 가이드라인에 공통으로 제시되는 중요한 평가지표로 사이버 공격 및 재난 발생 시 우선으로 복구해야 하는 자산을 정의할 수 있다.

<표 11> 사이버 복원력 평가항목 B.식별

사이버 복원력 평가모델		정보보호 관리체계 인증
평가 항목	평가 지표	
B. 식별	B.1. 자산의 식별	1.2.1. 정보자산 식별 2.1.3. 정보자산 관리
	B.2. 인적 자산의 식별	2.2.1. 주요 직무자 지정 및 관리 2.2.2. 직무분리
	B.3. 물리 자산의 식별	2.4.1. 보호구역 지정 2.4.2. 출입통제 2.4.3. 정보시스템 보호 2.4.4. 보호설비 운영

4.2.3. 예측(Anticipate)

예측은 위협과 위험에 대한 취약성을 평가하고 이에 따라 초래될 수 있는 결과를 예측하여 중요 인프라의 위험 평가를 수행하는 것을 말한다. 예측에 부합하는 평가지표는 첫째. 모니터링, 둘째. 예비사이트, 셋째. 체계 이중화를 평가지표로 선정했다. 모니터링은 위험에 대한 대응체계를 구축하여 대응체계에 맞춰 실시간 탐지를 통해 사고가 발생하지 않도록 조치하는 것을 말한다. 예비사이트와 체계 이중화는 사고가 발생해도 서비스가 구동되도록 자산을 분산화하여 비즈니스 연속성을 보장하는 것을 말한다.

<표 12> 사이버 복원력 평가항목 C.예측

사이버 복원력 평가모델		정보보호 관리체계 인증
평가 항목	평가 지표	
C. 예측	C.1. 모니터링	2.10.1. 보안시스템 운영 2.11.1. 사고예방 및 대응체계 구축 2.11.2. 취약점 점검 및 조치 2.11.3. 이상행위 분석 및 모니터링
	C.2. 예비사이트	2.12.1. 재해, 재난 대비 안전조치
	C.3. 체계이중화	2.12.2. 재해복구 시험 및 개선

4.2.4. 내구성(Withstand)

위험을 해결하고 인프라 복원력 강화를 위해 전략적 실행 계획에 대한 지침을 제공하는 내구성은 실제 사고가 발생하였을 때의 대응 행동과 사고 발생을 낮추기 위한 인프라의 내재적 강도를 의미한다.

인프라를 보호하기 위해서 사고 이전에 솔루션에 대한 정책을 사전에 정의하고, 사고 발생 시 해당 정책이 신속히 적용되어 안전하게 인프라가 운영될 수 있도록 인프라의 안전성을 보장한다.

<표 13> 사이버 복원력 평가항목 D.내구성

사이버 복원력 평가모델		정보보호 관리체계 인증
평가 항목	평가 지표	
D. 내구성	D.1. 서버보안	2.6.2. 정보시스템 접근
	D.2. 네트워크보안	2.6.1. 네트워크 접근
	D.3. 단말기보안	2.10.9. 악성코드 통제
	D.4. 패치관리	2.10.8. 패치관리
	D.5. 데이터관리	2.9.3. 데이터베이스 접근

4.2.5. 회복(Recover)

회복은 회귀(수용할 수 있다고 알려진 이전의 상태를 복제하는 것), 재구성(수용할 수 있는 수준으로 중요한 기능을 복제하는 것), 대체(손상된, 의심스러운 시스템 요소를 새로운 것으로 대체 하는 것)의 관점에서 정지된 서비스가 신속하게 재개될 수 있는 능력을 말한다.

<표 14> 사이버 복원력 평가항목 E.회복

사이버 복원력 평가모델		정보보호 관리체계 인증
평가 항목	평가 지표	
E. 회복	E.1. 복원 우선순위 선정	2.9.3. 백업 및 복구관리
	E.2. 복원 목표시간 선정	2.11.5. 사고대응 및 복구
	E.3. 대체시스템	2.9.1. 변경관리

4.2.6. 학습 및 발전(Learning & Evolving)

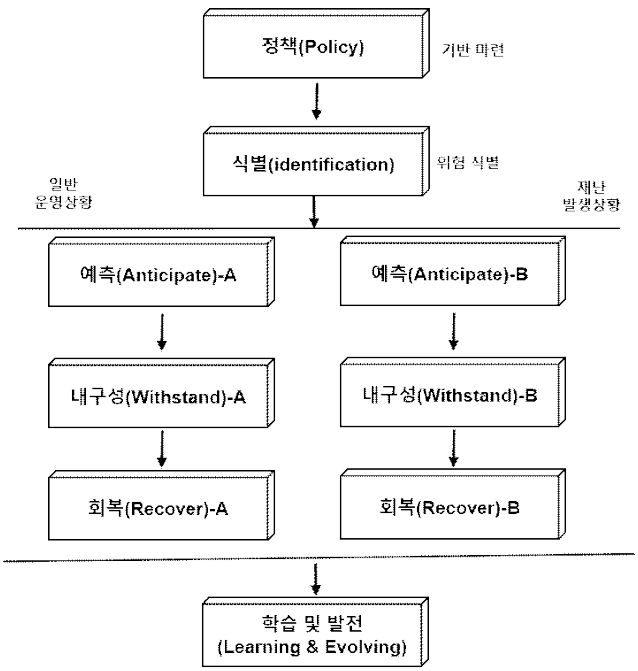
사전 예방 능력 제고를 위해 A-E 까지 평가지표 및 대응체계를 상시 점검하여, 문제점 분석 및 개선점을 측정 기준, 모범사례 등을 활용하여 검토하고, 사이버 복원력 향상과 발전을 지속해서 도모하는 것을 말한다.

<표 15> 사이버 복원력 평가항목 F.학습 및 발전

사이버 복원력 평가모델		정보보호 관리체계 인증
평가 항목	평가 지표	
F. 학습 및 발전	F.1. 분석 및 개선	2.11.4. 사고대응 훈련 및 개선
	F.2. 지속적 훈련	2.12.1. 재해, 재난대비 안전조치
		2.12.2. 재해복구 시험 및 개선

4.3. 사이버 복원력 평가모델 제안

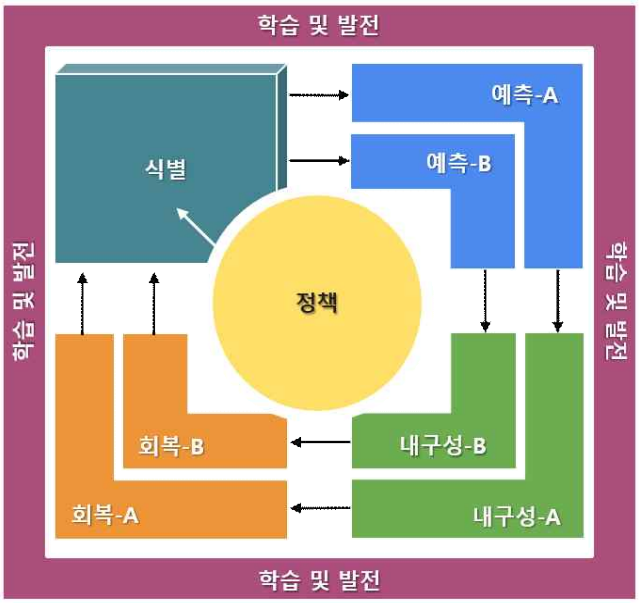
우리가 새롭게 제시한 평가모델은 국내 정보보호 관리체계의 평가지표와 일치되어 있음이 증명되었다. 다만, 국내에서 발생 된 침해사고 및 재난 상황 시 정보보호 관리체계가 정상 작동하지 않는 것은 평가지표 간 분절성 및 상호 호환성이 미흡함을 나타낸다. 따라서, 우리는 일반 운영 상황과 재난 발생 상황으로 구분하여, 각 상황에 맞춰 이행과제를 수행해야 한다.



(그림2) 사이버 복원력 최종 평가 모델(도식화)

<표 16> 재난 발생 상황 시 이행과제

평가 항목	일반 운영상황	재난 발생상황
예측	일반적인 시스템 운영 시 예측되는 취약점을 파악하고 사전평가 수행	위험 유형을 구분하여 예측되는 취약점을 파악하고 사전평가 수행
내구성	잠재적 솔루션 식별 (예: Fault tolerance, Fail over) 1) 일반 운영 상황에서 장애 허용 및 극복을 위한 시스템 및 프로세스 식별/운영 2) BCP 기반 전략적 실행 계획 수립 및 운영	재난상황 기반 잠재적 솔루션 식별/수립/운영 1) 식별: Resilience System 2) 수립/운영: Resilience Process
회복	내구성 수립계획 기반(BCP) 일반 상황과 재난 발생상황에 따라 다른 복원 업무 수행 + 정상 프로세스 유지	



(그림 3) 사이버 복원력 최종 평가모델(구조화)

5. 결론 및 향후연구

최근의 사이버 공격은 기기 고장, 정전 등 기존 IT 운영 위협 발생 요인과는 달리 백업자료도 함께 감염시켜 일반적인 복구만으로는 사태를 수습하기 어렵다. 결국, 사이버 공격을 완전하게 차단한다는

것은 사실상 불가능하며, 대부분 신고나 사고 발생 후 대응하는 수준에 불과하므로 사이버 복원력 개념은 앞으로 더욱 중요해질 것이다.

본 연구는 국내·외 기관에서 적용한 사이버 복원력 평가항목을 분석하여 새로운 평가항목과 평가지표를 도출했다.

도출된 평가항목과 평가지표를 국내 정보보호 관리체계와 비교 분석한 결과, 평가지표의 일치성을 확인했고 이를 통해 우리는 국내 정보보호 관리체계도 사이버 복원력 개념을 수용하고 있음을 입증했다.

하지만, 정보보호 관리체계 인증을 취득한 국내 기관이나 기업이 사이버 침해사고 또는 재해 · 재난 사고가 발생했을 경우 정보보호 관리체계가 정상적으로 작동하지 않는 이유는 평가항목 간 또는 평가지표 간 분절성으로 문제 해결이 가능한 상관관계의 모호함이 존재하기 때문이다.

사이버 복원력 목적과 목표는 평가지표 간 상호의존, 종속성, 연계를 통한 사고 대응을 강조하기 때문에 우리가 제시한 평가모델이 비즈니스 연속성을 보장할 것으로 예상한다.

향후에는 본 연구에서 제안한 평가모델을 기반으로 위험 유형을 범주화시켜 위험에 따라 적용되는 평가지표를 구별함으로써 구체적으로 조직에 적용할 기준을 마련하려 한다. 또한, 정보보호 관리체계 인증 기준에 사이버 복원력의 개념을 대입하여 현재의 3개 영역에서 1개 영역을 추가하여 '사이버 복원력 요구사항'으로 재구성하는 후속 연구를 진행하고자 한다.

본 논문은 2023년도 상반기 방송통신정책연구(디지털 서비스의 사이버 복원력 확보 방안 연구)의 지원을 받아 수행한 연구임.

참고문헌

[1] 이광석 "카카오 먹통 사태로 본 플랫폼 독점 문제" 문명과 경계 제6호 p.151-179 2023.03.

[2] ETRI, 주요국 사이버보안 정책 동향 및 시사점, 전자통신동향분석 제38권 제4호, 2023년 08월

[3] 고은아, 김홍빈, 김진규, 윤주연 "EU의 디지털 미래 구축을 위한 사이버보안(Cybersecurity) 방향과 시사점" KISA INSIGHT VOL.4 2023

[4] European Commission, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020" COM(2022) 454 final, 2022/0272(COD), 2022.09.

[5] PFMI(Principles for Financial Market Infrastructures) : BIS CPMI와 IOSCO가 마련한 금융시장인프라 및 관계당국이 금융시장을 안전하고 효율적으로 운영하기 위해서 준수해야할 기준 (2012.04.)

[6] CIS(Center for Internet Security) Controls®, COBIT 5, ISA(International Society of Automation) 62443-2-1:2009, ISA 62443-3-3:2013, ISO(International Organization for Standardization)/IEC(International Electrotechnical Commission) 27001:2013, NIST SP 800-53 Rev. 4

[7] Cyber resilience of on-board systems and equipment, E27, Apr 2022 Withdrawn (Rev.1Sep 2023)

[8] CISA, Infrastructure Resilience Planning Framework(IRPF), May 2023(Version 1.1)

[9] 한국은행 "사이버 복원력 평가 지침서", 2018.01

[10] NIST, 사이버 복원력 시스템 개발

[11] CPMI-IOSCO - Guidance on cyber resilience for financial market infrastructures

[12] White House, National Security Strategy, 2022.10.12.

[13] 국방정보시스템 사이버복원력 수준 평가를 위한 성숙도모델에 관한 연구