Headline

보안 가시성 확보와 틈새(Gray Zone) 해소 전략

Cloud 사업그룹 Cloud 보안컨설팅팀 백성광 팀장

■ 개요

우리는 변화의 시대를 넘어 '변혁의 시대'에 접어들었다. 1990 년대 인터넷의 시작은 시스템을 구축하고 서비스를 제공하는 과정 속에서 정보 유통과 소통의 폭발적 증가를 이끌었고, 우리는 이 서비스를 기반으로 다양한 정보를 주고받으며 현대인의 삶을 영위하고 있다.

서비스를 제공하는 기업들은 자체 데이터센터와 서버(On-Premise) 환경에서 IT 자원을 관리해 왔다. 그리고, 클라우드(Cloud) 시장의 성장과 기술의 발전으로 필요에 따라 IT 자원을 탄력적으로 사용할 수 있게 되면서, 클라우드를 도입해 업무와 서비스에 활용하고 있다. 최근에는 인공지능(AI) 기술이 급속히 발전하며 다양한 분야에서 AI 서비스를 접목하고 있다. 기업들은 경비절감 등 효율성 높이기 위해 인공지능(AI) 도입하고 있으며 정부・공공기관은 AI 역량확보와 경쟁력 강화를 위해 규제해왔던 망분리를 완화하고 개선하고 있다.(N2SF : National Network Security Framework, 금융분야 망분리 개선 로드맵)

■ 해커의 Target, 보안의 틈새(Gray Zone)

On-Premise 환경에서 Cloud 와 AI 기술로의 전환이 가속화되면서, 조직이 인지하지 못했던 보안 취약점이 발생하고 있다. 해커들은 이러한 틈새를 금전적, 군사적·정치적 목적 등 다양한 이유로 노리고 있다.

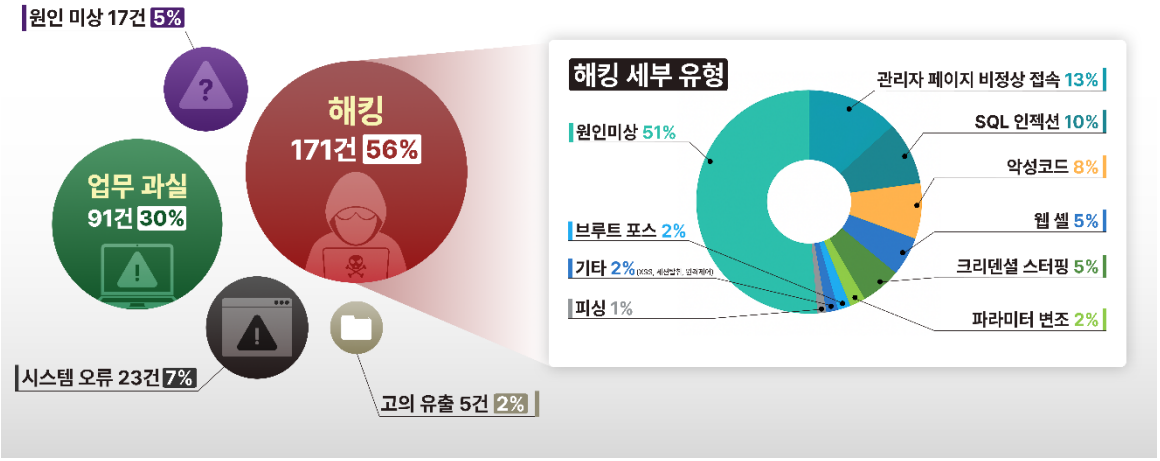
보안의 틈새(Gray Zone)는 관리되지 않고 방치된 자산, 위험관리 활동의 부재, 인적 실수 등으로 발생한다. 보안사고 사례를 보면, 그 원인은 대부분 VPN 등의 서비스 표면 취약점이나 웹 및 애플리케이션(Application) 취약점에 대한 식별 및 조치 부족, 또는 외부 인터넷 통제 미흡으로 업무용 사용자 PC 가 악성코드에 감염되면서 발생한 경우가 많았다.

기업들은 일부 IT 서비스를 클라우드를 통해 운영하는 추세이며, 이에 따라 많은 보안담당자들은 클라우드 영역에서의 보안 관리에 어려움을 호소하고 있다. 이는 개발 부서가 자체 승인만으로 클라우드 서비스를 사용할 수 있어 보안 부서가 이를 인지하지 못한 채, 보안성 검토가 이루어지지 않거나, 클라우드 환경에서 어떤 서비스의 어떤 기능을 확인하고, 발생하는 로그를 어떻게 관리해야 하는지에 대한 명확한 기준이 부족하기 때문이다. 마치 구름 속을 들여다보는 듯한, 보안 가시성이 확보되지 않은 회색지대(Gray Zone)를 노린 해킹 사고가 빈번히 발생하고 있다.

글로벌 헬스케어 랜섬웨어(UnitedHealth Group, Change Healthcare 등), Snowflake 클라우드 플랫폼 MFA 계정 탈취, Yes24 랜섬웨어 감염 등 일반 기업을 대상으로 금전적 목적의 보안사고가 지속적으로 발생하고 있다. 국가 간 분쟁의 경우, 우크라이나-러시아 전쟁(2022 년~현재)을 전후로 양국은 정부 및 금융기관 대상 DDoS(디도스) 공격, WhisperGate 등 데이터 와이퍼 악성코드 배포, 위성통신 해킹, 피싱 및 군사 데이터 탈취 등의 사이버 공격을 감행했으며, 이스라엘-하마스/이란 간 분쟁에서도 정부·언론 서비스를 향한 DDoS 공격과 전력망 운영사에 대한 해킹이 이루어졌다.

우리나라도 1953 년 휴전 이래 북한과의 대치가 지속되고 있으며, 사이버공간에서도 북한의 공격은 끊임없이 이어져 왔다. 7.7 디도스 공격(2009 년), 3.20 사이버 테러(금융사·방송사 해킹, 2013 년), 서울시 교통망·통신망 해킹 시도(2019 년), 한국수력원자력 공격(2020 년) 등 수많은 사이버 공격이 발생했다. 최근 발생한 S 통신사의 BPF 해킹 사건 또한 사이버 안보 위협의 일환으로 해석하는 시각이 많다. 아울러 중국-대만 간 갈등 고조에 따라, 미국의 전략적 거점인 우리나라를 겨냥한 사이버공격 시도도 더욱 증가할 것으로 예상된다.

해커의 공격방식은 다양하지만, 공격의 대상은 대부분 조직 시스템 내 존재하는 취약점에서 시작된다. 개인정보보호위원회가 2025 년 5 월 발표한 '개인정보 안전관리 체계 강화 추진 방향' 자료에 따르면, 지난해 국내 보안사고 중 56%가 시스템 취약점을 노린 해킹에 의해 발생한 것으로 나타났다.



* 출처 : 개인정보위 (2025.5.21)

그림 1. 지난해 개인정보 유출사고 원인유형

사이버 보안사고 관련 뉴스기사를 접하면 낯선 용어나 기술적인 설명으로 인해 이해가 어려울 수 있으나, 대부분은 시스템의 취약점을 통해 해킹이 발생하고, 정보가 유출된다는 내용이다. 해커들은 조직 내 가장 약한 고리, 즉 시스템의 취약점을 타깃으로 삼아 침투한다.

■ 보안의 틈새(Gray Zone) 찾고, 메꾸자

사람들은 건강한 삶을 통해 행복을 추구하며, 이를 위해 규칙적인 식사, 수면, 운동을 실천하려고 노력한다. 또한 정기적인 건강검진을 통해 자각하지 못한 질병을 조기에 발견·치료하여 건강을 유지한다.

조직의 튼튼한 사이버 보안을 위해서도 기본적인 활동이 필요하다. 보안의 기본은 보안 솔루션을 운영하고, 침해사고를 모니터링·대응하는 것, 보안 관리체계(Information Security Management System)를 마련하고 위험을 관리(Risk Management)하는 것이다. 그리고 기술 환경의 변화로 발생하는 보안의 틈새(Gray Zone)를 해소하기 위해서는 새로운 기술을 적용한 보안 전략이 필요하다.

1. 보안솔루션의 구축 및 운용

2000 년대 초반부터 많은 전문가들은 보안을 '성(Castle)'에 비유해 설명해 왔다. 조직 내부(내부망)와 외부(인터넷)를 명확히 구분하고, 외부의 위협을 차단하기 위해 방화벽, 침입탐지시스템(IDS), 침입방지시스템(IPS) 등 네트워크 경계에 방어체계를 구축하는 방식은 중세 성곽의 높은 성벽과 해자를 통해 침입을 막는 구조와 유사하다.

조직이 사이버 보안체계를 구축할 때 가장 먼저 고려해야 할 것은 보안 솔루션이다. 성벽을 세우고 성문에 경비를 배치해 출입을 통제하듯, 내부와 외부를 구분할 수 있는 방화벽을 구성하고, 외부에서 내부로 유입되는 위협을 탐지하고 차단하기 위해 WAF 및 IPS 등의 침입 차단 시스템을 구축해야 한다. 이후 내부 단말(PC) 통제, 시스템 접근 통제, 계정 관리, DB 암호화, 백업 및 복구 시스템 등을 구축함으로써 보안 활동의 기반이 마련된다.

해킹 사고는 취약점을 통해 침입한 후, 단말(PC, 서버)에서 정보 수집, 주변의 다른 취약한 시스템 검색, 악성코드/백도어 설치, 랜섬웨어 설치, 정보유출, 금전요구 등의 절차로 진행된다. 침입 후 설치되는 랜섬웨어 등 최근에 발생한 사고들의 지능화된 알려지지 않은 악성코드를 백신 등으로는 탐지하기 어려우므로 해당 악성 행위 탐지 및 대응이 가능한 EDR(Endpoint Detection & Response)의 도입은 기존 보안솔루션을 확인되지 않았던 회색지대(Gray Zone) 해소하고 가시성을 확보하는데 도움이 된다.

담당자의 경험 부족이나 조직의 비용 부족으로 인해 Cloud 에서도 회색지대가 다수 발생하고 있다. Cloud 인프라의 보안을 위해 방화벽, IPS, 접근제어, CloudTrail 을 이용한 로그모니터링 등을 적용하고 있지만, 조직에서 운영하고 있는 보안상태를 명확히 인지하기 어렵다. Cloud 서비스의 보안 가시성 확보를 위해 보안상태를 실시간으로 파악할 수 있는 CSPM(Cloud Security Posture Management)과 워크로드의 실행 환경 위협을 탐지·방어하고 취약점을 관리하는 CWPP(Cloud Workload Protection Platform) 솔루션이 필요하다. 또한, 각 보안 솔루션에서 발생한 보안 이벤트를 SIEM(Security Information and Event Management)을 통해 통합 수집하고, 이벤트 간 연관 분석을 통해 침해 시도를 식별하고 차단해야 한다. 보안 솔루션이 적용되지 않은 영역(예: 서버 접속 계정의 적정성 검토, 서비스 관리 페이지의 계정 권한 검토 등)은 인적 자원을 활용하여 기준과 절차에 따라 지속적으로 관리해야 한다.

2. 보안 관리체계 마련 및 위험관리 활동

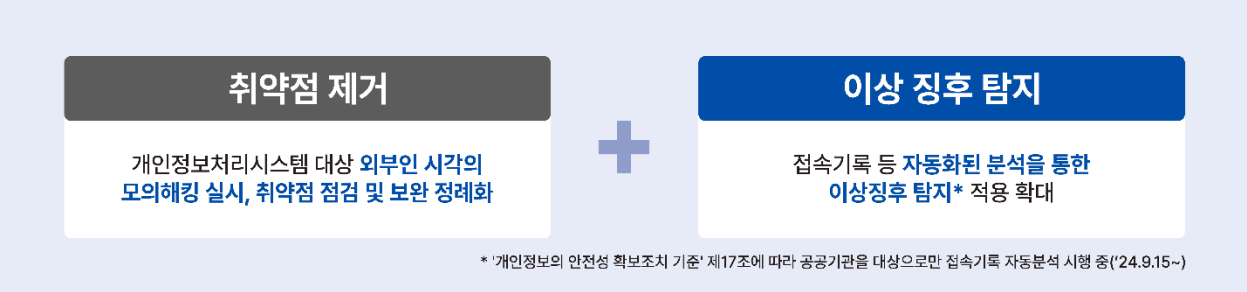
보안 솔루션을 통해 외부의 위협으로 부터 조직을 보호하는 성(Castle)을 쌓았다면, 이제는 이를 체계적으로 운영할 관리체계를 갖추어야 한다. 기준(규정)을 수립하고, 담당 조직을 구성하여 경비대장, 망루병, 경계병 등의 역할을 부여해 운영하는 것이다. 동시에 성곽, 수로, 해자 등의 방어 시설이 튼튼한지 수시로 점검하고 보수해야 한다.

사이버 보안도 마찬가지다. 내부 시스템과 정보 자산을 보호하기 위해 규정·지침·절차를 수립하고, 정보보호 기획, 솔루션 운영, 침해 대응, 보안 점검 등을 수행할 조직을 구성해야 한다. 연간 계획을 수립하고, 경영진의 승인 아래 주기적으로(연간/분기/월간/일간 등) 계획된 보안 관리를 실행해야 한다.

위험 관리 활동이란 보호해야 할 자산(시스템, 정보, 인력 등)을 식별하고, 알려진 취약점을 점검·제거·관리하는 것이다. 자산 식별에는 정보, 하드웨어, 소프트웨어, 시설, 인력 등이 빠짐없이 포함되어야 한다.

식별된 시스템에는 CCE(Common Configuration Enumeration), CVE(Common Vulnerabilities and Exposures) 등 알려진 취약점이나, 소스코드/웹/모바일 애플리케이션에 존재하는 취약점을 점검하고 제거해야 한다. 기능상 제거가 어려운 경우, 시스템 교체나 기능 개선 등의 계획을 수립하고, 접근 통제 및 사후 모니터링 등 보완 대책을 병행해야 한다.

신규 시스템 도입이나 변경이 발생할 경우, 자산 관리대장을 갱신하고 해당 시스템의 취약점을 제거하는 것이 가장 기본적이면서 중요한 절차다. 개인정보보호위원회는 '개인정보 안전관리 체계 강화 추진 방향'에서 취약점 제거를 보안의 최우선 과제로 제시하고 있다.



* 출처 : 개인정보위원회

그림 2. 추진과제: ①즉각적·기술적 조치사항(1)

최근 ISMS 인증을 받은 기업에서도 보안 사고가 발생하면서 "인증을 받았는데 왜 사고가 나느냐"는 질문을 받는 경우가 많다. ISMS-P(Information Security Management & Personal Information System)는 조직의 보안 활동을 구조화하기 위한 '틀'이며, 인증은 건강검진처럼 상태를 확인하고 부족한 부분을 개선하기 위한 과정이다.

건강하기 위해 잘 먹고, 잘자고, 열심히 운동하지만, 여러가지 주변 환경 등의 영향으로 병이 발생하고 건강이 악화되는 것처럼 매년 예방 측면에서 ISMS-P 인증 유지를 통해 매년 발견되는 보안관리 미흡한 부분과 취약점을 개선하면서 보안을 강화해야 한다.

그림 3. 한국인터넷진흥원(KISA)홈페이지>ISMS-P 인증 제도 소개>인증기준

3. 보안의 틈새(Gray Zone)를 찾고 해소하다

이스라엘 역사상 가장 강력한 왕 다윗은 난공불락으로 여겨지던 예루살렘 성을 함락시켰다. 깊은 계곡으로 둘러싸인 산악 요새였지만, 외부에서 내부로 연결된 식수용 터널을 통해 성 내부로 침투했다. 강력한 성이 무너진 원인은 구조적·관리적 취약점이었다.

조직의 사이버 보안도 마찬가지다. 보안 솔루션과 ISMS-P 체계를 갖추고 매년 점검을 수행하더라도, 인지되지 못한 회색지대(Gray Zone)는 여전히 존재할 수 있으며 이것이 해커의 주요 타깃이 된다. 손자병법의 '지피지기 백전불태(知彼知己 百戰不殆)'처럼, 우리가 보호해야 할 시스템, 자산, 데이터 등을 명확히 파악하면 취약점을 제거하고 공격 노출을 줄일 수 있다. 더불어 최근 보안 사고의 유형과 공격 패턴을 분석하고, 해커의 시각에서 시스템을 점검한다면 회색지대를 효과적으로 해소할 수 있을 것이다.

ISMS-P 는 각 항목을 '적정/미흡'으로만 평가하므로 '충분히 안전한가'에 대한 정성적 평가는 어렵다. 따라서 보안성숙도 모델이나 MITRE ATT&CK 프레임워크*와 같은 기준을 병행해 운영하는 것도 효과적인 방법이다.

구분	CMMI	CMMC	C2M2
목적	조직의 프로세스 성숙도와 운영 효율성 개선	사이버보안 역량의 성숙도 평가 및 DoD 준수	IT/OT 사이버보안 역량 증진 및 위험 관리
적용 분야	업종 무관, 비즈니스 전반 (소프트웨어, 서비스 포함)	방위산업, DoD 계약/협력사 (FCI, CUI 취급 조직)	주요 기반시설(에너지, 통신 등) 및 모든 산업
구성 /범위	프로젝트/조직 전체 프로세스 영역 (최대 22 개)	17 개 보안 도메인/ 3~5 개 성숙도 레벨	10 개 도메인/350 개 이상 사이버보안 실천항목
성숙도 단계	5 단계(초기~최적화)	3~5 단계(Foundational~Expert, 버전에 따라 다름)	각 도메인별 4 MIL 단계 (MIL0~MIL3, C2M2 v2 기준)
평가 방식	공식 심사/외부 평가, 내부 개선/벤치마킹 목적	외부 감사(3rd-party), 자기평가 (저단계), DoD 요구사항	자기진단 및 외부 평가 병행, 도메인별 개별 측정
대표 특징	운영, 프로젝트, 서비스 전반의 프로세스 통합·최적화	NIST SP 800-171 연계, 보안 규정 준수, 법적 필수	실제 보안 실무, 조직 내/외부 위험관리, 인적·과정·기술 균형
필수성	선택(벤치마킹, 경쟁력 강화를 위한 국제 표준)	필수(방위산업/DoD 협력사는 반드시 준수)	선택(기반임계 산업군은 요구/권장)

표 1. 성숙도 모델 비교-프렉시티(Perplexity) 정리 자료

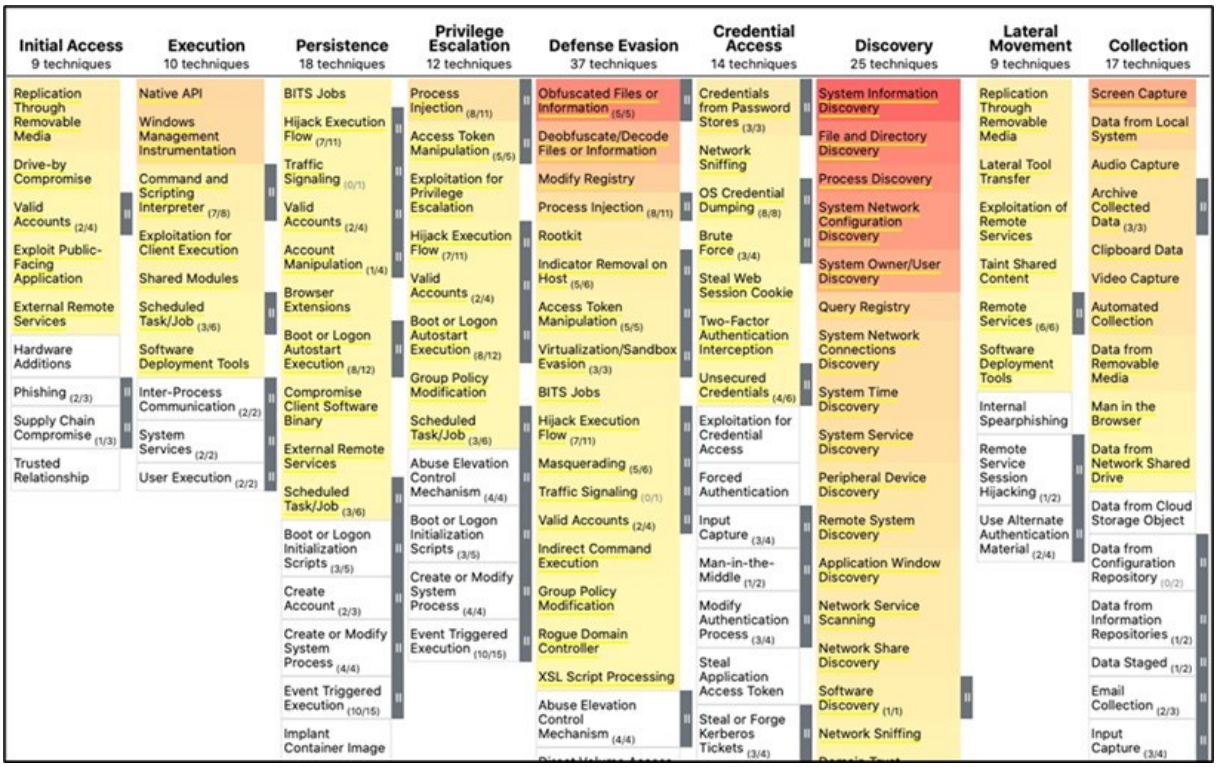


그림 4. MITRE ATT&CK Metrix - Navigator 중 일부 발췌

* MITRE ATT&CK 프레임워크 : MITRE ATT&CK는 Adversarial Tactics, Techniques and Common Knowledge의 약자로 공격자들이 실제로 사용하는 전술(Tactics), 기술(Techniques), 절차(Procedures)을 체계적으로 분류한 지식 기반 매트릭스이다.

마지막으로, 조직의 사이버 보안에도 분명한 '목표와 전략'이 필요하다. 목표가 없다면 보안의 일관성과 실행력을 확보하기 어렵다. 목표는 위험 완화와 자원 우선순위를 결정하는 기준이 되며, 보다 효율적이고 효과적인 보안 운영을 가능하게 한다.

보안 전략은 중장기 계획 또는 마스터플랜을 통해 수립된다. 과거에는 기업들이 보안 방향을 설정하고 실행 가능한 활동을 담은 마스터플랜을 마련했지만, 현재는 ISMS 인증이나 솔루션 도입으로 대체되는 경우가 많다. 그러나 종합적이고 효과적인 사이버 보안 체계를 운영하기 위해 마스터플랜은 여전히 필요하다.

■ 시사점

기술 발전, 범죄 양상, 국제 정세 변화에 따라 해커들은 끊임없이 우리 조직의 사이버 보안 회색지대(Gray Zone)를 노리고 있다.

보안 솔루션의 도입과 운영, 보안 체계 관리 및 위험 관리 등 기본적인 보안 활동을 통해 회색지대를 지속적으로 방어하고, 클라우드(Cloud) 및 인공지능(AI) 등 신기술 영역에서 보안 가시성을 확보하며, 조직 차원의 보안 목표를 수립하고 실행해 나간다면 해커의 공격과 사고로부터 조직의 사이버 안전 수준을 지속적으로 강화할 수 있을 것이다.

■ 참고 문헌

[1] 개인정보위원회, (별첨2) 개인정보 정책포럼 발표자료(개인정보 유출사고 현황 및 대응방향)

[2] KISIA, 2024년 국내 정보보호산업 실태조사 보고서

[3] 보안성숙도 모델을 활용한 정보보호 관리수준 점검 방법에 관한 연구_고려대학교 이상규

■ 참고 자료

[1] 한국인터넷진흥원, ISMS-P인증 제도소개

[2] SK쉴더스, 위협 중심 보안 전략의 핵심 도구: Rule Framework