

보안취약점 공개심의정책(VEP)의 법적 이해와 합리적 설계방안

윤상필* · 권헌영**

❖ 요약 ❖

오늘날 보안취약점은 국가 차원에서 관리해야 하는 전략자원이다. 따라서 국가전략 관점에서 취약점을 공개하는 것이 이익인지 보관하는 것이 이익인지 판단할 수 있는 절차가 필요하다. 본 연구는 이를 위해 보안취약점 공개심의의 개념을 수용하고 공개심의정책의 구체적 설계방안을 제안했다. 먼저 취약점은 사이버안보와 직결되는 요소라는 점에서 해당 기능을 수행하는 국가정보원이 실무를

전담할 필요가 있다. 아울러 공개심의정책의 상위 의사결정기구로서 국가안보실의 신기술사이버안보비서관이 주재하고 관계부처와 민간 보안업체 및 학계 전문가가 참여하는 가칭 국가취약점관리회의를 운영할 수 있을 것이다. 이러한 운영주체 및 의사결정기구에 관한 사항과 함께 공개심의의 세부 기준과 요건, 오남용 통제에 관한 사항 등을 종합적으로 다루는 법률이 필요하다.

핵심어: 취약점, 보안취약점, 취약점 공개, 취약점 공개심의정책(VEP), 사이버안보

I. 서론

2021년 12월 Log4j 취약점이 전 세계를 뒤흔들었다. Log4j(Log for Java)는 아파치 소프트웨어 재단의 Java 기반 오픈소스 툴이다. 이 툴에서 발견된 취약점을 활용해 공격자는 원격으로 코드를 실행하고 대상 시스템의 모든 권한을 탈취할 수 있다. Log4j 취약점이 위험한 가장 큰 이유는 다수의 정부와 기업들이 java를 사용하고 있기 때문이다(CISA and FBI et al. 2021, 3). 이미 벨기에 국방부가 이 취약점을 활용한 공격을 받았다(De Standaard. 2021). 중국 정부의 사이버 첩보그룹인 Aquatic Panda도 대형 학술단체를 해킹했다(Crowd Strike. 2021).

DOI: 10.35390/sejong.28.2.202205.007

* 제1저자, 고려대학교 정보보호대학원 박사

** 교신저자, 고려대학교 정보보호대학원 교수

Log4j 취약점이 공개된 지 1달 안에 벌어진 일이다.

국가의 기반시설에서부터 시민의 일상까지 모든 것이 디지털로 넘어오고 있다. 디지털 미래에서 취약점은 반드시 관리해야 하는 대상이 된다. 취약점을 관리하려면 일단 취약점을 찾아야 한다. 취약점을 찾았다면 그 존재 사실을 알려야 전 세계의 발 빠른 대응이 이루어질 수 있다. 그런데 취약점은 무턱대고 공개하기 어렵다. 취약점을 공개하면 이를 활용한 공격이 증가하기 때문이다(Arora and Krishnan et al. 2004, 19). 물론 취약점의 존재를 알고 패치가 개발되면 취약점의 효력이 줄어들긴 하지만 패치를 적용하지 않으면 공격은 유효하다. 패치도 완벽할 수 없기 때문에 변형 취약점들이 계속 나타난다. 이번 Log4j 취약점 또한 최초 발견 이후 3번의 변형이 이어졌다. 반대로 취약점을 공개하지 않아야 할 경우도 있다. 사이버안보의 관점에서 취약점은 국가와 사회를 방어하고 국익을 증진하는데 반드시 필요한 전략자원이기 때문이다. 이는 기본적으로 사이버 공간에 정해진 경계나 합의된 규칙이 없어 각국이 자국의 이익을 극대화하기 위해 서로를 해킹하고 있다는 암묵적 사실에 기인한다(Buchanan. 2020, 317).

그렇다면 국가전략 차원에서 취약점을 공개하는 것이 이익인지 취약점을 공개하지 않고 보관(retain)하는 것이 이익인지 판단할 수 있는 절차가 필요하다. 특히 취약점을 공개하지 않는 경우 정부는 취약점을 은밀하게 활용할 수 있게 된다. 따라서 취약점 공개와 보관의 판단 기준은 법적 분석을 통해 합리적으로 설계해야 한다. 이미 주요 선진국들이 VEP(Vulnerability Equities Process)라는 절차를 운영 중인 반면 국내에서는 관련 정책 논의조차 없는 상황이다. 학계에서는 제로데이 취약점을 정보기관에서 관리하고 이를 위한 정보공유체계 설립, 국회 보고의 무 등을 제안하는 연구(오일석, 2019), 안보 목적의 해외정보 수집을 위해 VEP 절차를 참고할 수 있다고 제안하는 연구(김창섭·이상진, 2021) 2건만이 확인된다.

따라서 본 연구는 취약점의 공개 여부를 판단할 수 있는 정책의 설계방안을 제안하는 데 목적을 둔다. 이를 위해 먼저 보안취약점을 국가전략 차원에서 이해하려는 접근을 시도하고 그러한 관점에서 VEP 정책의 법적 의미를 검토한다. 3장에서는 주요국이 운영 중인 VEP 정책의 핵심 요소들을 식별하고 요소별 주요 쟁점들을 도출한다. 이후 4장을 통해 취약점 공개심의정책을 국내에 수용하고 설계하기 위한 구체적인 방안들을 제시한다.

II. 보안취약점 공개심의정책(VEP)의 의의

1. 보안취약점의 개념과 특성

보안취약점이란 시스템의 보안정책을 위배하기 위해 사용될 수 있는 시스템상 설계, 실행, 운영 및 관리상의 결함 또는 약점을 말한다(Shirey. 2000, 190). 좀 더 간략하게 공격자가 악용할 수 있는 오류라고 이해할 수도 있다. 이러한 취약점 발생의 근본 원인은 사람이다. 사람은 완벽한 프로그램을 설계할 수 없기 때문이다. 코딩하는 과정에서 실수할 수도 있고 입력값이나 외부 요인으로 인해 생각지 못한 결과가 나올 수도 있다(Desai and Kroll. 2017, 25).

사람의 실수로 발생한 결함을 악용하는 작업이 있어야 하기 때문에 보안취약점은 행위자의 의도에 종속될 수밖에 없다. 선의의 행위자라면 찾아낸 취약점을 공개하거나 패치를 개발하겠지만 악의의 행위자라면 이를 공개하지 않고 악용하거나 암 시장에 판매할 것이다. 또한 공격자의 관점에서 취약점은 효과적이다. 찾아낸 사람만 알 수 있다는 은밀한 이점으로 인해 다른 누군가가 같은 취약점을 찾아 공개하거나 제거하지 않는 이상 공격자는 취약점을 영원히 활용할 수 있다(윤상필. 2021, 42-43). 게다가 공격자는 특정 취약점의 영향을 받는 버전의 모든 시스템과 서비스들을 공격할 수 있으므로 광범위한 감시나 데이터탈취, 공격 등도 가능하다(Schneier, 2017).

취약점 생태계의 특성도 중요하다. RAND 연구소에 따르면 취약점은 최초 발견 후 평균 6.9년간 유효했다. 이 중 25%는 1.5년 후 없어졌지만 25%는 9.5년이 지나도 유효했다. 또한 취약점이 발견된 후 실제 익스플로잇이 개발되기까지는 평균 22일이 소요됐으며 제로데이 취약점의 5.7%는 1년 후 외부에 의해 드러났다(Ablon and Bogart. 2017, 51-57). 취약점은 꽤 오랫동안 유효할 수 있고 누군가 찾은 취약점을 다른 사람이 찾을 가능성도 있는 것이다.

2. 보안취약점의 국가관리 필요성

취약점을 확보한 주체는 전략적 우위를 차지한다. 공격의 관점에서 취약점을 찾아 보관해두고 정보수집이나 사전조치에 활용할 수도 있지만 반대로 방어의 관점

에서 자국 기관이나 기업의 보안을 강화하는데 쓸 수도 있기 때문이다. 디지털 경쟁에서 더 많은 전략적 선택지를 얻는 셈이다. 아울러 상용 암호화 기술의 발달로 고도화되고 은밀해지는 사이버범죄를 수사하려면 취약점을 활용해야만 하는 때도 있다(Tasheva, 2017). 그러한 점에서 보안취약점을 국가 차원에서 관리해야 하는 이유는 3가지로 대별해 볼 수 있다. 첫째, 사이버 전략수단의 원천재료로서 취약점을 확보할 수 있어야 한다. 둘째, 자국의 보안과 안전을 강화하기 위해 취약점을 활용할 수 있어야 한다. 셋째, 완전한 모습의 디지털 미래에 대비해야 한다는 전략적이고 미래지향적인 시야로 취약점 문제를 바라봐야 한다.

1) 사이버 전략수단의 원천재료 확보 경쟁

각국 정부는 기본적으로 보안보다 공격을 우선한다. 불확실성이 증가하면서 위협을 미리 식별하고 예방하기 위한 선제적 접근들이 중요해졌기 때문이다(Saltzman, 2013, 41-42). 이에 따라 각국의 정보기관과 해커부대는 사이버 무기의 원천재료인 보안취약점을 직접 발굴하거나 취약점 시장에서 구매하고 있다(Buchanan, 2020, 65). 취약점 거래 생태계가 대중에게 본격적으로 알려진 계기는 2015년 이탈리아 해킹팀(Hacking Team) 유출사건이다. 당시 해킹으로 전 세계 국가들의 거래내역 약 420GB 분량의 자료들이 토렌트에 유출됐기 때문이다(Hern, 2015). 해킹팀 사건으로 유출된 취약점을 활용한 악성코드가 증가하면서 제3의 피해들도 발생했다. 실제로 해킹팀 자료 유출 후 이를 만에 Adobe Flash Player 취약점의 익스플로잇이 공개됐고 일부 취약점은 우리나라와 일본 등을 대상으로 한 공격에 활용되기도 했다(Wu, 2015).

아울러 미국은 취약점을 가장 활발하게 활용하는 국가로 알려져 있다. 본래 두 차례의 세계대전에서 암호를 해독하고 감청을 수행해 온 국가안보국(NSA: National Security Agency)은 디지털 통신이 증가하면서 특정 국가나 조직이 사용하는 시스템과 프로그램의 취약점을 찾아 은밀히 정보를 수집해왔다. 특히 1997년 클린턴 행정부 당시 미국의 기반시설과 국방부 컴퓨터가 매우 취약하다는 사실이 드러났다. 미국은 전문위원회를 구성하고 사이버위협 대응방안을 모색했다. 위원회는 NSA가 잠재적인 사이버위협을 사전에 탐지하고 완화할 수 있어야 한다고 권고했다(U.S. President's Commission on Critical Infrastructure Protection, 1997,

63). 이에 따라 1997년 국방부 장관이 NSA에게 네트워크 공격 기술을 개발하도록 했다(Black, Jr. 1997, 1). NSA는 본격적으로 소프트웨어의 취약점을 찾아 활용하기 시작했다(Kaplan. 2016, 133). 디지털 기술이 발전하면서 민간 암호기술도 강력해지고 각국의 보안과 해킹 역량도 증가했다. NSA는 네트워크를 감시하기 위해 해킹 조직인 TAO(Tailored Access Operations)를 창설했다(NSA/CSS. 2000, 31). 2001년 9.11 테러 이후 정보수집 활동이 극대화되면서 TAO도 활발해졌다(Loleski. 2019, 119). 오늘날 TAO는 소속 해커들에게 최고 수준의 교육을 제공한다. 취약점을 찾아 활용하면서 축적된 성공사례와 경험에 기반한 지식을 체계화해 제공하고 있다(Joyce. 2016).

중국이나 러시아, 북한, 이란의 해킹 역량도 세계적 수준이다. 조사에 따르면 해킹에 성공하기까지 러시아는 약 18분 49초, 북한은 2시간 20분, 중국이 4시간, 이란은 5시간 9분의 시간이 소요된 것으로 파악된다(Crowd Strike. 2019, 14). 2020년 10월 NSA는 중국 정부의 해커그룹들이 주로 활용하는 취약점 목록을 공개하기도 했다(NSA. 2020). 이에 따르면 중국은 윈도우 OS의 원격 서비스를 통해 코드를 실행할 수 있는 취약점, 모바일아이언(MobileIron)의 기기 관리 솔루션을 통해 서버를 장악할 수 있는 취약점, 드레이텍(Draytek)의 라우터 장비에 요청을 전송해 원격 코드를 실행할 수 있는 취약점 등 대부분 내부망에 직접 접속하거나 관문을 뚫을 수 있는 취약점들을 활용하고 있다. 또한 2021년 4월 러시아 해외정보국(SVR)이 펄스 시큐어(Pulse Secure)와 포티넷(Fortinet)의 VPN 취약점을 악용하는 정황이 확인되기도 했다(CISA. 2021).

이스라엘도 잘 알려진 해킹 강국이다. 2021년 12월 이스라엘 스파이웨어 제조업체 NSO 그룹의 감시 툴인 페가수스에 의해 미국 국무부 직원 11명의 아이폰이 해킹당해 수개월 간 정보가 유출된 사건이 밝혀졌다. 페가수스는 아이폰의 제로데이 취약점을 활용해 피해자의 아이폰이 문자를 수신하기만 해도 기기를 감염시킬 수 있었다(Kirchgaessner. 2021).

이 외에도 취약점을 활용해 정보를 수집하고 감시하려는 각국의 활동들이 수시로 이루어지고 있다. 이에 따라 취약점 거래시장도 형성되어 있다. 공개적으로 제로데이 취약점을 구매하고 거래하는 업체인 제로디움(Zerodium), 크라우드펜스(Crowdfence) 등이 대표적이다.

2) 자국의 사이버보안 강화

정부가 확보한 취약점을 무조건 공격에만 사용하는 것은 아니다. 예를 들어 2016년 영국 정부통신본부(GCHQ)의 통신전자보안팀이 모질라(Mozilla) 웹 브라우저 Firefox의 특정 버전에 적용되는 원격코드실행 취약점을 찾아 Mozilla에게 보고하여 해당 취약점이 패치되기도 했다(The Register, 2016). 또한 GCHQ는 2016년 이전에도 애플의 iOS를 포함한 여러 소프트웨어에서 24개의 취약점을 찾아 제거하는 데 기여했다(Cox, 2016). 미국의 NSA도 2017년 발견한 취약점의 약 90%를 공개한다고 주장했다(Waterman, 2017). 실제로 2020년 NSA가 Microsoft 윈도우 OS의 중대한 결함을 찾아 무기화하지 않고 Microsoft에게 공유했던 사실이 공개되기도 했다(Nakashima, 2020).

아울러 사이버범죄 수사를 위해서도 취약점을 활용할 수 있어야 한다. 종단 간 암호화 기술이 발전하면서 암호화 메신저나 메일 서비스를 활용한 범죄가 증가하고 있다. 수사기관들이 영장을 들고도 실제 수사를 진행할 수 없는 이른바 ‘암흑화(going dark)’ 현상이다(김창섭·이상진, 2021, 41). 수사기관은 이제 통신을 실시간으로 감청하기도 어렵고 단말기를 확보하더라도 강력한 사용자 인증체거나 디스크 암호화라는 장벽을 마주하게 된다. 위커(Wickr)나 스냅챗(Snapchat)은 수신자가 메시지를 수신하면 클라이언트와 서버에서 메시지가 완전히 소멸되는 기능을 제공한다. 기존의 범죄자는 아무리 강해도 국가의 공권력에 대항할 수 없었다(이원상, 2017, 88). 그러나 사이버범죄는 다르다. 해커 한 명이 한 국가를 마비시킬 수 있는 환경이 조성됐기 때문이다. 결국 국가도 무기의 평등 관점에서 취약점을 활용할 수 있어야 한다.

3) 디지털 미래 대비

더욱 중요한 문제는 전 세계가 디지털 전환을 서두르고 있다는 점이다. 기술중심 사회에서 기술을 통제할 수 있는 능력은 강력한 권력이다(Winner, 1978, 139). 2003년 이라크전쟁에서 벌어진 지휘통제체계 교란 작전, 2008년 조지아를 마비시키고 지상전에 돌입했던 러시아의 전쟁방식, 2010년 이란 핵 시설을 파괴한 스텝스넷 공격, 2013년 3.20 사이버테러, 2016년 국방 전산망 해킹 사건 등을

돌아보라. 오늘날 국가지원 해킹조직들은 피싱메일을 통해 우리나라 외교, 통일, 국방 분야 데이터를 탈취하고 IT 제품의 취약점을 이용한 공급망 공격으로 기관 내부에 침투하고 있다(국가정보원, 2021, 16). 이러한 작전들의 진짜 효과는 최악의 상황에서 최대로 발휘될 것이다. 각국 정부가 오래전부터 사이버를 국가안보의 우선순위로 다루고 있는 이유다(Agresti, 2010, 101-104). 이제는 사실상 전 세계의 정부들이 취약점을 활용해 정보를 수집하고 무기화하고 있다(Starks, 2021).

이 때문에 뛰어난 디지털 인프라는 위협이기도 하다. 디지털 환경은 근본적으로 불완전하다(Matwysbyn and Cui et al. 2010, 67). 규제는 커녕 보안에 대한 인식도 없던 시절부터 연결성만을 추구해왔는데 이제는 그런 기술의 결과들이 얽혀 있는 상태다. 스마트시티와 자율주행자동차, 드론 택시들이 등장하고 있다. 근본적인 위협 요소인 취약점 문제를 제대로 다루지 못하면 디지털 전환에 성공할 수 없고 경제와 안보도 뒤쳐질 수밖에 없다. 무엇보다 국민의 생명과 신체는 침해되면 복구할 수 없는 절대적 권리다. 디지털과 현실 공간이 밀접하게 연결될수록 국가는 생명과 신체에 관한 위협을 사전에 식별하고 예방할 수 있어야만 한다. 이제 정부는 안전을 보장할 의무를 이행하기 위해 필요한 역량과 권한을 갖춰야 한다(Williams, 2011, 1199).

3. Vulnerabilities Equities Process(VEP)의 법적 이해와 개념 수용

자유민주주의 법치국가에서 취약점 문제를 다루는 일은 더욱 어렵다. 국가사회의 안전을 보장하고 시민을 보호하려면 일단 피해가 발생하지 않도록 해야 한다는 점에서 예방하는 것이 효율적이다(Heyman, 1991, 545). 따라서 국가안보와 재난안전의 관점에서 취약점을 수집할 수 있어야 한다. 그러나 정부의 행위를 허용하는 법적 권한이 필요하다. 근대국가의 이념과 법치주의에 따라 정부는 국민이 제정한 법률을 준수하고 국제사회의 관계를 고려해야 하기 때문이다. 무엇보다 정보수사기관의 활동이 개인의 자유를 제한하는 경우 법률이 부여하는 권한과 절차에 따라야 하는 것이 원칙이다. 감시나 감청, 압수수색 등의 직접적인 공권력 행사는 법률에 근거해야 한다(박광민·박웅신, 2019, 201).

그러나 법률로 요건과 대상, 절차 등을 엄격히 정해두면 현장의 유연한 대응이

어려울 수밖에 없다(한희원, 2017, 281-282). 이에 따라 자칫 법치주의의 준수를 요구하는 것이 마치 정보활동을 저해한다고 인식될 여지가 있는데 이는 잘못된 접근이다. 먼저 예외로서 허용되던 정보활동의 영역이 크게 줄어들고 있다는 점을 인식해야 한다. 이제 정보활동 또한 국제질서가 형성되면서 마련된 국제인도법과 인권 존중의 원칙을 준수해야 한다(Deeks, 2016, 685). 각국은 국제법 규범과 다른 국가들의 법률을 살펴보지 않을 수 없게 되었다. 수사를 위한 정보활동 또한 마찬가지다. 정보를 수집, 가공하는 기능 자체가 권력작용이기 때문이다(김한균, 2019, 166). 둘째, 정보수사기관의 오남용 문제들이 불거지면서 법적 통제장치가 요구되고 있다. 미국의 워터게이트 사건이나 COINTELPRO와 같은 FBI의 불법 감시 활동은 미국 내 인식과 법체계를 뒤바꿨다. 법적 제한으로 인해 설령 첩보활동의 효과가 줄더라도 오남용으로 인한 피해보다는 낫다는 인식이 자리한 것이다(Civiletti, 1980, 903-904). 우리나라 또한 최근 국가정보원법을 개정하면서 국내정치 개입을 원천 차단하고 해외 정보활동과 사이버 및 과학기술 분야 권한을 강화했다. 셋째, 이러한 변화들은 오히려 우리 정보수사기관이 필요한 자원을 적법하게 동원하고 관련 기능을 실질적으로 행사할 수 있도록 하는 기틀이 될 수 있다. 핵심은 결국 공동체의 합의다. 적법한 기준을 정하고 필요한 기능을 수행할 수 있도록 지원해야 한다.

따라서 우리 정보수사기관이 보안취약점을 활용해 활동할 수 있도록 권한을 부여하는 법률을 제정해야 한다. 보안취약점을 악용한 안보위협 및 범죄 행위들을 감시하고 예방하도록 힘을 실어줄 수 있어야 한다(Williams, 2011, 1200). 이를 위해 고려해야 하는 구체적인 기준과 절차도 설계해야 한다. 즉, 취약점을 공개하는 이익이 더 크지, 보관해두고 작전이나 수사에 활용하는 것이 더 크지 판단할 수 있는 체제가 필요하다. 보안취약점의 공개 여부를 심의, 판단할 수 있는 법적 절차는 결국 보안취약점을 국가 차원에서 관리하기 위한 기본 전제로서 정당성을 확보하고 취약점 공개 문제를 합리적으로 다룰 수 있는 틀이 된다. 이미 미국, 영국, 캐나다 등 주요 선진국들이 관련 정책을 운영하고 있다. 직역하자면 ‘취약점 지분 절차(VEP: Vulnerabilities Equities Process)’라고 불리는 정책이다. VEP 정책의 핵심은 취약점의 공개 또는 보관 여부를 판단함으로써 두 경우 간의 지분을 나누는 행위다. 즉, 공개와 보관의 이익을 비교 형량하고 합리적인 균형점을

정하는 절차로 이해할 수 있다. 따라서 우리가 수용하는 때에는 취약점의 공개 여부를 심의하여 결정하는 ‘취약점 공개심의절차’라고 표현할 수 있을 것이다. 아래에서는 그러한 정책의 기원과 발전과정을 살피고 핵심 쟁점들을 탐색한다.

III. 보안취약점 공개심의정책의 발전과 주요 쟁점

1. 보안취약점 공개심의정책의 연혁

취약점 공개심의정책의 기원은 2008년 부시 행정부의 국가안보정책지침 제54호(NSPD-54)다. 동 지침에 따라 국가 차원의 사이버보안이니셔티브(CNCI)가 추진됐는데 그중 미국의 정보시스템을 보호하기 위해 공격적 역량을 적용할 수 있는 계획을 개발하라는 내용이 있었다. 동 계획은 취약점을 활용한 공격과 방어에 이익을 비교衡量할 수 있는 VEP 절차를 마련해야 한다고 권고했다(ODNI, 2010, 2). 이에 따라 국가정보국장실(ODNI)이 이끌고 국가안전보장회의(NSC), 중앙정보국(CIA), 국방정보국(DIA), 연방수사국(FBI), 국방부, 법무부, 국무부, 에너지부, 국토안보부가 참여하는 워킹그룹이 구성됐다. 해당 워킹그룹은 2008년부터 2년에 걸친 작업을 통해 2010년 2월 첫 취약점 공개심의정책인 이른바 ‘VEP 문서(Commercial and Government Information Technology and Industrial Control Product or System Vulnerability Equities Policy and Process)’를 수립했다.

초기 VEP 문서는 비공개였다. 그러나 2013년 에드워드 스노든의 폭로로 정부가 제로데이 취약점을 약 2,500만 달러에 구매했던 사실이 드러났다(Fung, 2013). 이와 함께 정부가 취약점을 정보활동이나 공격 목적으로 활용한 사실이 알려지면서 문제가 커졌다(Schwartz and Knake, 2016, 7). 관련 사실관계를 식별하고 개선하기 위해 수립된 대통령 특별조사위원회는 2013년 12월 조사결과를 발표하면서 30번 권고를 통해 취약점 문제를 언급했다. 이에 따라 미국 정부가 정보활동을 위해 예외적으로 취약점을 활용하려면 상위 범정부 검토 그룹을 구성하고 적정 절차를 거쳐야 했다(Clarke and Morell et al. 2013, 219).

이와 함께 2014년 4월 블룸버그 통신이 NSA가 하트블리드(Heartbleed) 취약

점을 이미 알고 있었음에도 이를 은밀히 활용해왔다고 폭로했다(Riley, 2014). 이에 따라 2014년 5월 전자프론티어재단(Electronic Frontiers Foundation)이 정보자유법(Freedom of Information Act)에 근거해 VEP 정책의 기록 공개를 요청했다. 오바마 행정부는 NSA가 취약점을 활용하고 있었음을 인정하고 2014년 12월부터 VEP 정책을 일부 공개했다. 공식 공개된 것은 2015년 3월이었으나 자료는 상당 부분 비닉 처리되어 상세 내용을 파악하기 어렵다.

이에 대해 행정절차에 불과한 VEP 정책을 법제화해야 한다는 의견, VEP 정책에 민간 관계자를 참여시키고 투명성과 감독을 강화해야 한다는 의견, 국토안보부가 해당 정책을 주관해야 한다는 의견들이 제기됐다(Jaikaran, 2017, 6-9). 그러던 중 2016년 샌 버나디노 총격 사건에서 FBI가 아이폰의 취약점 공개 여부를 VEP 절차에 부치지 않겠다고 밝히자 VEP 정책의 실효성에 관한 문제들이 불거졌다. 이어서 2017년 5월 워너크라이(WannaCry) 랜섬웨어 사태가 발생하고 해킹 대응이 요구되자 상원과 하원에서 취약점 공개심의검토위원회(ERB: Equities Review Board)를 공식화하고 의회와 프라이버시 및 시민자유 감독위원회(PCLOB: Privacy and Civil Liberties Oversight Board)에 대한 보고의무를 부여하며 국토안보부가 VEP 절차를 전담하도록 하는 해킹대응역량보호법안(PATCH Act: Protecting our Ability to Counter Hacking Act)을 발의했다. 이에 대응하여 2017년 11월 트럼프 행정부의 사이버안보조정관 Rob Joyce는 동 법안의 주요 내용들을 도입해 신속히 새로운 VEP 헌장(VEP Charter)을 발표했다.

2. 보안취약점 공개심의정책의 동향

미국이 2017년 새로운 공개심의정책을 마련한 이후 Five Eyes 국가들이 뒤따랐고 독일과 중국도 유사한 움직임을 보이고 있다. 영국은 2018년 11월 외무부 산하 정부통신본부(GCHQ: Government Communications Headquarters) 차원에서 공개심의절차를 발표했다. 2019년 3월 호주 신호정보국(ASD: Australian Signals Directorate)이 사이버보안 취약점 공개원칙을 수립했다. 같은 기간 캐나다 신호정보기관인 통신보안국(CSE: Communications Security Establishment)도 공개심의관리체계를 마련했다. 이어서 독일은 2021년 8월 사이버보안전략을

통해 취약점 관리 절차를 수립하겠다고 밝혔다(Bundesministerium des Innern, für Bau und Heimat. 2021, 103-104). 중국도 2021년 9월 네트워크 제품 보안 취약점 관리규정(网络安全产品安全漏洞管理规定)을 시행하면서 국가 차원에서 취약점을 공식 관리하기 시작했다(工业和信息化部, 国家互联网信息办公室, 公安部. 2021). 이 규정 제3조에 따라 취약점 관리 계획과 조정은 국가인터넷정보실이 담당한다. 특히 문제가 되는 부분은 제9조다. 취약점을 발견한 주체는 취약점 정보를 공개하지 않아야 하며 사전에 공개할 필요가 있다고 판단하는 경우 관련 취약점이 적용되는 사업자와 협의하여 공업정보화부 및公安부에 보고해야 한다. 또한 동조 제7항에 따르면 제로데이 취약점은 해당 사업자를 제외하고는 해외의 기관이나 개인에게 제공할 수 없다. 정부가 모든 제로데이 취약점을 수집하고 중국 이외의 주체에게 취약점이 공유되지 못하도록 함으로써 통제를 강화한 것이다.

〈표 1〉 국가별 취약점 국가관리 정책의 수립

| 국가명 | 정책명 | 발표일 |
|-----|---|---|
| 미국 | 취약점 공개심의절차 (VEP: Vulnerability Equities Process) | 2010년 2월 최초 수립(비공개) 2015년 3월 공식 공개 2017년 11월 수정 |
| 영국 | 공개심의절차(The Equities Process) | 2018년 11월 |
| 호주 | 사이버보안 취약점의 책임있는 공개원칙 (Responsible Release Principles for Cyber Security Vulnerabilities) | 2019년 03월 |
| 캐나다 | 공개심의관리체계 (Equities Management Framework) | 2019년 03월 |
| 독일 | 2021 사이버보안전략 (Cybersicherheitsstrategie für Deutschland 2021) | 2021년 08월 취약점 관리 절차 수립 계획 |
| 중국 | 네트워크 제품 보안취약점 관리규정 (网络安全产品安全漏洞管理规定) | 2021년 09월 국가 차원의 취약점 종합 관리 |

3. 보안취약점 공개심의정책의 핵심 쟁점

1) 법제화 이슈

정보기관이나 수사기관의 취약점 활용 행위는 보안을 침해한다. 이를 정당화하려면 보안을 침해하도록 허용하는 법적 근거가 있어야 한다. 현재 취약점 공개심

의정책을 운영하는 국가들 모두 법적 근거를 두고 있지 않다. 다만 미국에서 2017년 취약점 공개심의정책을 법제화하기 위한 시도가 있었다. 현재 미국의 VEP 현장은 법률이나 행정명령이 아닌 내부 문서다. 따라서 정부기관들은 취약점을 공개하거나 평가절차에 부의해야 할 의무를 지지 않는다. 이 때문에 2017년 해킹대응 역량보호법안(PATCH Act: Protecting our Ability to Counter Hacking Act)이 발의됐다. 의회를 통과하진 못했지만 공개심의절차의 법적 근거를 마련하기 위한 시도였다는 점에서 큰 의미를 갖는다(Williams. 2018, 126).

2) 운영 주체의 문제

취약점 공개심의정책을 어떤 기관이 운영하고 최종 판단은 어디서 내릴 것인지의 문제도 중요하다. 미국은 의사결정기관인 공개심의검토위원회(ERB)를 두고 국가안전보장회의의 사이버보안 전문가를 위원장으로 두고 있다. 아울러 실무는 NSA가 전담하도록 하고 있다. 이에 따라 NSA는 취약점 공개심의절차 관련 정보 교류, 문서화 및 사후 검토를 위한 기록관리 등을 수행한다. 관련하여 NSA가 취약점을 보관하는 결정을 선호하기 때문에 국토안보부와 민간 전문가들을 참여시켜 균형을 유지할 필요가 있다는 비판도 있다(Rosenblum. 2021). 이 때문에 2017년 PATCH 법안은 국토안보부 장관이 ERB의 위원장을 담당하도록 하기도 했다. 관련하여 민간의 이익이 실질적으로 고려될 수 있는지도 검토해야 한다. 현재 ERB는 관리예산처(OMB), NSA, CIA, ODNI, 재무부, 국무부, 법무부, 국토안보부, 에너지부, 사이버사령부, 상무부의 장이 정한 대표부로 구성된다. 상무부가 참여하고 있긴 하지만 사실상 국가안보의 관점에서 연방기관들이 모인 기구다. 민간의 이익이 실질적으로 고려되지 않을 수 있는 것이다. 따라서 민간 주체들이 관련 절차에 관여할 수 있도록 하는 방안도 고려해야 한다(Zhang. 2019). 영국은 GCHQ 공개심의위원회를 통해 의사결정을 수행한다. 동 위원회의 위원장은 GCHQ 산하 국가사이버안보센터(NCSC) 소속 책임자로 한다. 실무는 정보공동체의 전문가들로 구성된 공개심의실무진(ETP)이 담당하고 있다. 호주는 ASD가 취약점 공개심의절차를 운영하고 있다. 고위 관리단으로 구성된 공개심의위원회에서 의사결정을 수행하고 실무 단위의 판단은 현장 및 기술 전문가로 구성된 공개심의실무진이 전담한다. 캐나다도 공개심의검토위원회를 두고 있다. 사이버보안센터(CCCS)와

신호정보수집 기관의 국장급 임원이 공동으로 의장을 맡는다. 실무진은 CCCS의 장과 신호정보수집 기관의 전문가로 구성된다.

〈표 2〉 국가별 취약점 공개심의정책 전담기관

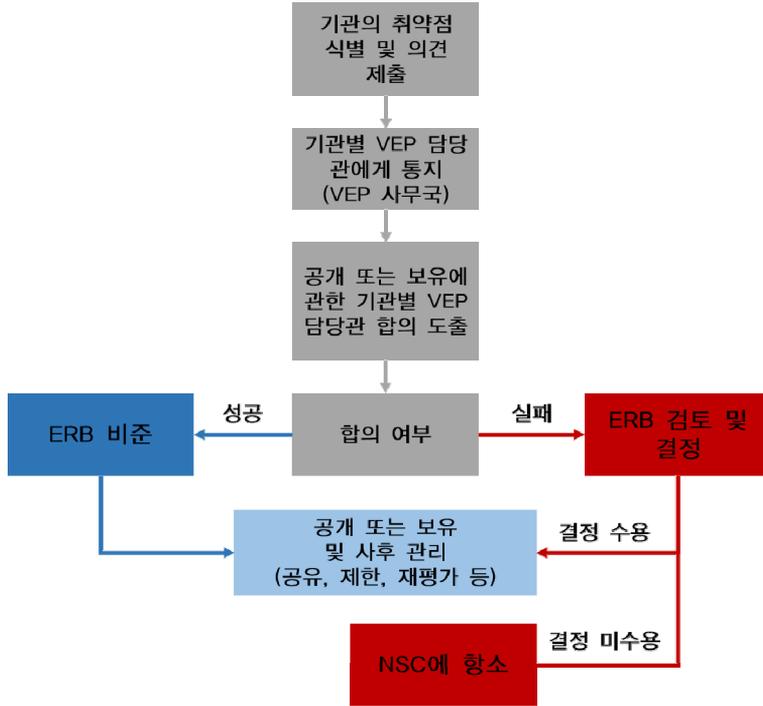
| 국가명 | 의사결정기관 | 실무 |
|-----|---|--|
| 미국 | 공개심의검토위원회 (ERB: Equities Review Board) | VEP 사무국: NSA 전담 |
| | 위원장: 대통령실 국가안전보장회의(NSC)에서 선임 | |
| 영국 | GCHQ 공개심의위원회 (EB: GCHQ Equity Board) | 공개심의실무진 (ETP: Equities Technical Panel) |
| | 위원장: GCHQ 산하 NCSC에서 선임 | 구성: 정보공동체 전문가 |
| 호주 | ASD 공개심의위원회 (EB: Equity Board) | ASD 공개심의조정그룹 (Equity Steering Group) |
| 캐나다 | 공개심의검토위원회 (ERB: Equities Review Board) | 실무진 (Technical Panel) |
| | 공동위원장: 캐나다 사이버보안센터 및 신호정보기관의 장 | 구성: 캐나다 사이버보안센터 및 신호정보기관의 전문가 |

3) 절차 통제의 문제

(1) 공개심의절차

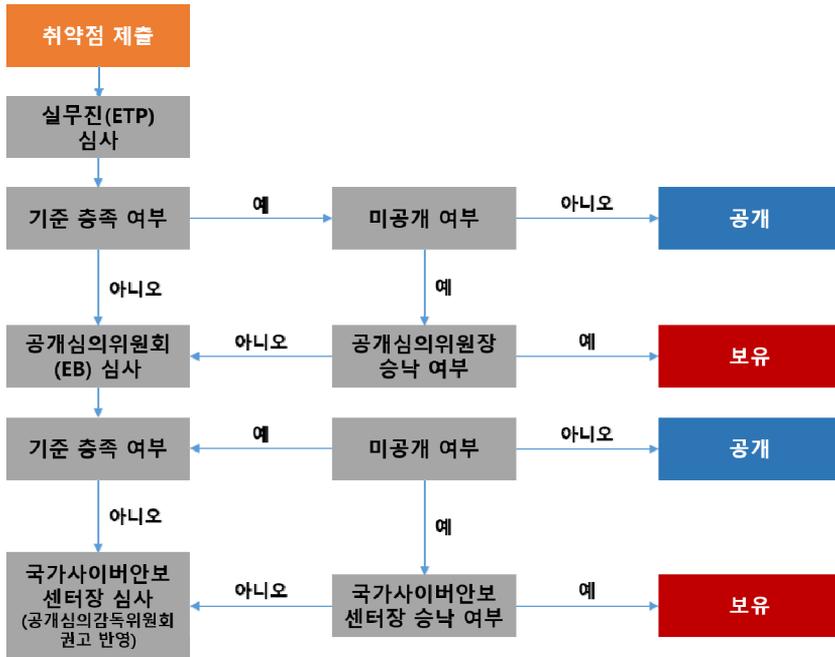
취약점을 어떤 절차로 평가해 공개 또는 보관 여부를 결정할 것인지 논의해야 한다. 미국은 새로운 취약점을 획득한 경우 보관 또는 공개 의견과 함께 VEP 사무국인 NSA에 제출한다. 제출서에는 취약점 정보, 취약점의 영향을 받는 제품 또는 시스템, 해당 취약점 정보의 취급에 관한 기관의 권고를 포함해야 한다. VEP 사무국은 제출서를 수령한 날로부터 1일 이내에 기관별 VEP 담당관들에게 통지하고 해당 취약점에 관한 이해관계 의견을 요청한다. 취약점에 관한 이해관계를 주장하는 기관은 5일 이내에 보관 또는 공개 권고에 대한 동의 여부를 제출한다. 권고에 동의하지 않는 기관은 관계 기관 및 VEP 사무국과 협의하여 7일 이내에 합의에 도달해야 한다. 그렇지 못한 경우 권한은 ERB에 넘어간다. 합의가 있는 경우 ERB는 최종 검토하여 비준하고 그렇지 못한 경우에는 직권으로 결정할 수 있다. ERB의 결정을 수용하지 않는 경우 기관들은 NSC에 항소할 수 있다.

〈그림 1〉 미국의 취약점 공개심의절차



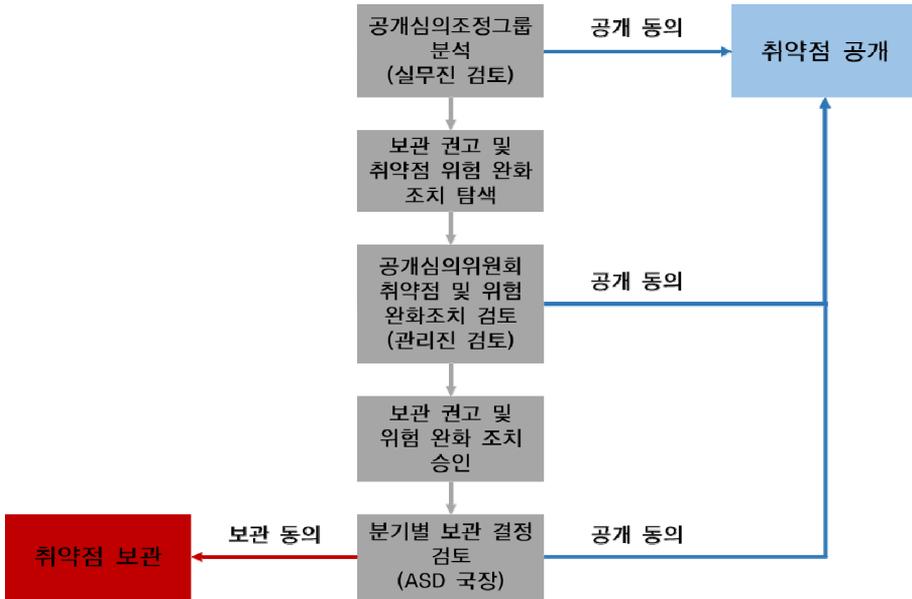
영국은 미국과 달리 실무진 차원의 결정만으로도 취약점을 공개할 수 있다. 즉, 취약점을 보관하려는 경우에만 EB의 승인을 받는다. 기관이 취약점을 제출하면 정보기관의 전문가들로 구성된 실무진에서 검토하여 취약점을 보관할 필요가 없는 경우 공개할 수 있다. 보관이 필요한 경우에는 EB 위원장의 승인을 받아야 한다. 공개 또는 보관에 관한 실무진의 합의가 도출되지 않는 경우 EB에 안전을 상정해야 한다. EB는 취약점 공개를 직권으로 결정할 수 있으나 보관 결정을 내리는 경우 최종적으로 NCSC장의 승인을 받아야 한다. 만약 EB 차원에서도 합의가 이루어지지 않거나 NCSC장이 승인하지 않는 경우 공개심의감독위원회의 권고를 받아 다시 NCSC 차원에서 최종결정한다.

〈그림 2〉 영국의 취약점 공개심의절차



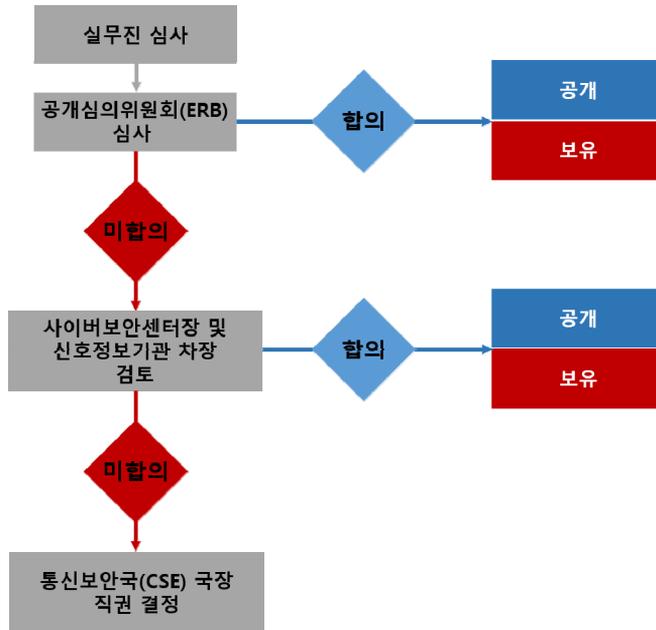
호주 ASD는 발견한 취약점을 실무진인 공개심의조정그룹에 제출한다. 호주 또한 실무진의 결정만으로도 취약점을 공개할 수 있다. 단, 보관을 결정한 경우 보관함으로써 발생할 수 있는 위험을 완화할 수 있는 조치를 마련해야 한다. 관련 보관 결정과 위험 완화 조치는 EB에서 다시 검토하여 공개 또는 보관 결정을 내릴 수 있다. 보관에 관한 최종 결정은 ASD 국장이 내리며 국장은 분기별로 취약점 공개 또는 보관 여부를 재검토한다.

〈그림 3〉 호주의 취약점 공개심의절차



캐나다는 CCCS와 신호정보기관의 전문가로 구성된 실무진이 식별된 취약점을 절차에 부의하고 위협과 영향 식별 및 완화를 위해 전문가 평가를 수행한다. 이에 따른 평가결과와 공개 또는 보관 권고를 문서화하고 ERB에 제공한다. ERB는 실무진의 평가 및 권고사항을 검토하고 필요한 경우 추가 설명을 요구할 수 있다. 또한 공개심의를 위한 합의 결정에 도달할 수 없는 경우 관련 결정을 CCCS의 장과 신호정보기관의 차장에게 회부하며 ERB에서 내린 결정에 관하여 CCCS의 장과 신호정보기관의 차장에게 정기 보고한다. CCCS의 장과 신호정보기관의 차장은 여러 정보를 고려해 ERB에서 합의가 이루어지지 않은 사항에 관한 최종 협의를 수행한다. 이 단계에서도 합의에 도달하지 못할 경우 최종 결정권은 CSE의 장에게 넘어간다. 이에 따라 CSE의 장은 CCCS의 장과 신호정보기관의 차장이 제안한 공개심의 결정을 검토하고 최종 결정을 내린다.

〈그림 4〉 캐나다의 취약점 공개심의절차



(2) 사후 감독절차

취약점 공개심의정책의 신뢰성도 확보할 수 있어야 한다. 이미 취약점 공개심의 정책을 두고 있는 국가들조차 불투명하다는 비판을 받고 있다. 관련하여 미국은 2020년 국방수권법(National Defense Authorization Act for Fiscal Year 2020) 제6720조를 통해 연방정부의 보안취약점 공개심의 절차에 관한 정보공동체의 보고의무를 부여했다. 구체적으로 살펴보면 동조 (b)항을 통해 취약점 공개심의절차의 절차나 기준에 중대한 변화가 있는 경우 30일 이내에 변동사항을 의회 정보위원회에 보고하도록 했다. 연간 보고의무도 부여했다. (c)항을 통해 매년 1회 이상 국가정보보국장(DNI)으로 하여금 정보위원회에 전년도 취약점 평가절차에 부의한 취약점의 개수, 이 중 대중에 공개하거나 특정 사업자에게 제공한 취약점의 수, 취약점 평가절차에서 배제된 취약점의 유형별 총 개수를 기밀 보고서로 제출하도록 했다. 아울러 특정 정보는 공개하도록 했는데 그러한 정보에는 공개심의절차에 따라 사업자나 대중에 공개된 취약점의 총 개수와 그러한 취약점 중 패치

된 취약점의 총 개수가 포함된다. 영국은 NCSC장을 위원장으로 하는 공개심의감독위원회를 설치했다. 동 위원회는 공개심의절차가 적절하게 수행되는지 검토하는 역할을 수행한다. 호주 ASD의 취약점 공개심의정책은 최종적으로 정보안보감사관의 독립적인 검토를 받는다. ASD는 모든 결정을 다루는 연간보고서를 작성해 정보안보감사관에게 제출하며 해당 보고서의 사본은 국방부 장관에게도 제공된다. 캐나다 CSE 또한 CSE 감독관과 의회 국가안보 및 정보위원회의 감독을 받는다.

4) 내용적 판단 기준

취약점 공개심의를 통해 고려해야 하는 기준과 요소를 설정해야 한다. 미국은 방어 및 활용적 관점과 함께 상업 및 국제관계를 고려하고 있다. 기본적으로 취약점의 영향 범위, 취약점의 식별 및 악용 가능성, 취약점의 위험성, 취약점의 위험 완화 가능성을 종합적으로 검토하고 있다. 활용적 관점에서는 취약점의 정보 내지는 작전상의 가치와 효과를 식별하고 해당 취약점 외에도 이를 대체할 수 있는 수단이 존재하는지 보충성을 검토하고 있다. 아울러 취약점 관련 사실이 드러날 경우 미국 정부와 산업계의 관계, 미국 정부와 국제관계에의 영향을 사전 검토하도록 하고 있다.

〈표 3〉 미국 취약점 공개심의정책의 내용

| 구분 | | 내용 |
|-------------|-------------|---|
| 방어적 고려사항 | 위험 (1A) | <ul style="list-style-type: none"> • 대상 제품의 사용처와 범용성 • 취약점에 영향을 받는 제품 또는 버전의 범위 • 해당 취약점이 알려질 경우 악용될 가능성 |
| | 취약점 (1B) | <ul style="list-style-type: none"> • 해당 취약점을 악용하기 위해 확보해야 하는 접근 루트 • 해당 취약점의 악용만으로 충분히 피해를 발생시킬 수 있는지 여부 • 위협행위자들이 해당 취약점을 발견하거나 획득할 가능성 |
| | 영향 (1C) | <ul style="list-style-type: none"> • 해당 제품의 보안에 의존하고 있는 이용자들의 수 • 해당 취약점의 심각성과 활용의 잠재적 결과 • 해당 취약점을 악용함으로써 위협행위자들이 얻을 수 있는 접근 루트나 이익 • 적들이 패치를 역공학하고 취약점을 찾아내 패치되지 않은 시스템에 악용할 가능성 • 정부, 기업 및 소비자들이 해당 보안취약점의 악용으로 인해 발생하는 보안 피해를 상쇄할 수 있는 정도로 패치를 설치할 가능성 |

| 구분 | | 내용 |
|------------------------------|--------------|---|
| | 완화 (1D) | <ul style="list-style-type: none"> • 제품이 해당 취약점을 완화할 수 있도록 설계되었는지 여부 및 해당 취약점에 의한 위험을 완화할 수 있는 다른 방법의 존재 가능성 • 기존의 모범 사례, 지침, 표준, 보안 관행을 통해 취약점의 영향을 완화할 수 있는 가능성 • 해당 취약점이 공개될 경우 업체 등이 해당 취약점의 영향을 효과적으로 완화하는 패치와 업데이트를 개발, 배포할 가능성 • 패치와 업데이트가 배포될 경우 취약한 시스템에 얼마나 빠르게 적용될 것인지 여부 및 얼마나 많은 시스템들이 영원히 또는 1년 이상 패치되지 않은 상태로 남아있을 것인지의 비율 • 위협행위자에 의한 취약점 악용이 정부기관 또는 다른 보안 공동체에 의해 탐지될 수 있는 가능성 |
| 정보활동 /법집행 /작전시 고려사항 | 작전가치 (2A) | <ul style="list-style-type: none"> • 해당 취약점의 활용이 정보수집, 사이버작전 또는 법집행 목적의 증거수집에 도움이 되는지 여부 • 정보수집, 사이버작전 또는 법집행 목적의 증거수집에 관한 해당 취약점의 증명된 가치 • 해당 취약점의 잠재적 가치 • 해당 취약점의 작전상 효과성 |
| | 작전영향 (2B) | <ul style="list-style-type: none"> • 해당 취약점의 활용이 사이버 위협행위자 및 관련 작전, 국가정보우선 순위체계 또는 군사적 표적, 군인 또는 민간인의 보호 등을 위해 우월한 작전적 가치를 제공할 수 있는지 여부 • 해당 취약점을 활용해 얻는 작전상 이익을 실현하기 위해 다른 대체적 수단이 존재하는지 여부 • 해당 취약점을 공개할 경우 정보원, 정보출처나 정보수집의 방법 등이 드러날 가능성 |
| 상업적 고려사항 | | <ul style="list-style-type: none"> • 미국 정부가 해당 취약점 정보를 보관하고 있는 사실이 밝혀질 경우 미국 정부와 산업계의 관계에 미칠 수 있는 영향 |
| 국제적 고려사항 | | <ul style="list-style-type: none"> • 미국 정부가 해당 취약점 정보를 보관하고 있는 사실이 밝혀질 경우 국제관계에서 미국 정부의 지위에 미칠 수 있는 영향 |

영국은 취약점의 완화 가능성, 취약점 활용의 필요성, 보안상 위험성을 검토하고 있다. 이에 따라 완화 가능성 측면에서는 취약점의 영향을 완화할 수 있는 방법과 함께 그러한 방법이 공개될 경우 영국의 국가안보에 미칠 수 있는 부정적 영향을 고려하고 있다. 취약점 활용의 필요성 관점에서는 주로 정보나 작전상의 가치와 기회, 다른 작전이나 협력국 등에 미칠 수 있는 영향을 검토한다. 보안상 위험성 관점에서는 취약점을 공개하지 않을 경우 발생할 수 있는 영향과 위험, 제3자가 발견하거나 악용할 가능성, 패치되지 않을 경우 발생할 수 있는 영향과 위험 등을 고려해야 한다.

〈표 4〉 영국 취약점 공개심의정책의 기준

| 구분 | 내용 |
|-----------------------------------|---|
| 완화 가능성 (Possible Remediation) | <ul style="list-style-type: none"> 취약점의 영향을 완화할 수 있는 방법 취약점의 영향을 완화할 수 있는 방법이 배포될 경우 영국의 국가안보에 미칠 수 있는 부정적 영향 |
| 운영 필요성 (Operational Necessity) | <ul style="list-style-type: none"> 해당 취약점을 보관함으로써 얻을 수 있는 정보 가치 해당 취약점 정보를 통해 얻을 수 있는 작전 가치 해당 정보를 통해 얻을 수 있는 정보 기회 해당 취약점에 대한 정보력 실현 의존성 해당 정보를 공개할 경우 다른 작전 능력이나 협력자에게 미칠 영향 |
| 방어적 위험성 (Defensive Risk) | <ul style="list-style-type: none"> 해당 취약점을 공개하지 않을 경우 영국 및 동맹국과 기업, 시민에게 발생할 수 있는 영향의 평가 해당 취약점이 타인에 의해 발견될 가능성 해당 취약점이 타인에 의해 악용될 가능성 해당 취약점이 패치되지 않는 경우 노출되는 기술 또는 분야 해당 취약점이 악용되는 경우 발생할 수 있는 잠재적 피해 취약점 패치가 없는 경우 구성 변경 등 다른 기술적 위협의 완화 가능성 존재 여부 |

호주는 〈표 5〉와 같은 8가지 원칙을 제시하고 있을 뿐 공개심의절차를 진행하면서 고려해야 하는 세부 요소와 기준들을 공개하고 있지 않다.

〈표 5〉 호주 취약점 공개심의정책의 원칙

| 구분 | 내용 |
|----|---|
| 원칙 | <ol style="list-style-type: none"> ① 보안을 우선으로 할 것 ② 국가 이익을 위할 것 ③ 위험을 평가: ASD는 악의적 행위자가 취약점을 이용할 수 있는 가능성을 신중하게 고려. 그러한 가능성이 있다고 판단되는 경우에는 취약점을 공개하여 패치가 이루어지도록 함 ④ 결과 고려: ASD는 악의적 행위자가 취약점을 악용할 경우 발생할 수 있는 잠재적 영향을 고려. 여기에는 영향을 받는 대상과 피해 규모 등이 포함 ⑤ 위협의 완화: 취약점을 보관하는 경우 ASD는 취약점을 패치하기 위한 보안 권고를 발표하는 등 호주의 시스템이 악용되지 않도록 보호하는데 최선을 다함 ⑥ 책임있는 공개: ASD는 사업자들과 긴밀히 협의하여 취약점을 대중에 공개하기 전 패치나 기타 완화 조치들이 이루어지도록 조치 ⑦ 정기적인 검토: ASD는 모든 취약점 보관 결정을 검토함. 국가안보상의 긴급성 등이 인정되지 않는 경우 취약점을 공개하여 제거 ⑧ 엄격한 감독: ASD의 모든 취약점 결정은 정보안보감사관의 독립적인 검토를 받으며 관련 연간보고서를 제출 |

캐나다는 5개 원칙과 10개 세부 기준을 공개하고 있다. 이에 따르면 캐나다는 정부 및 주요기반시설과 관련된 취약점인지, 캐나다에서 널리 사용되는 정보시스템이나 기술의 취약점인지, 예상되는 공격자의 식별 및 공격을 위해 필요한 전문성, 공격으로 인해 예상되는 피해, 해당 취약점의 정보적 가치, 다른 방법은 없는지에 관한 보충성, 취약점 완화 조치 등을 검토하고 있다.

〈표 6〉 캐나다 취약점 공개심의정책의 원칙 및 기준

| 구분 | 내용 |
|----|---|
| 원칙 | <ul style="list-style-type: none"> • CSE가 작전 또는 연구를 통해 발견하거나 획득한 취약점은 공개심의절차에 따름 • 공개된 취약점은 이 절차의 대상이 아님 • 공개 결정이 내려지면 CSE는 영향을 받는 업체와 협력하여 시스템 소유자와 운영자가 공개적으로 취약점을 알리기 전에 패치를 적용할 수 있도록 지원 • 보관한 취약점은 캐나다 정부의 최우선 정보 요구사항과 관련된 것이어야 함 • 외국 기업이 독점하여 사용하는 정보시스템 및 기술에 관한 고유의 취약점은 캐나다 및 캐나다인에게 위험을 미칠 우려가 없으므로 이 절차의 대상이 아님 <p>※ 개별 취약점을 보관하기 위한 결정은 최초 결정이 승인된 날로부터 최소 12개월마다 재검토</p> |
| 기준 | <ol style="list-style-type: none"> ① 취약점이 캐나다 정부 및 주요기반시설과 관련된 정보시스템 또는 기술과 관련되는지 여부 ② 취약점이 캐나다 정부 및 주요기반시설과 관련은 없지만 캐나다에서 널리 사용하는 정보시스템이나 기술에서 발견되는지 여부 ③ 캐나다 네트워크를 대상으로 해당 취약점을 사용할 수 있는 공격자의 식별 ④ 캐나다 네트워크를 대상으로 취약점을 사용하는 데 필요한 기술적 전문성 또는 복잡성 ⑤ 공격자가 취약점을 성공적으로 악용할 경우 발생할 수 있는 피해의 심각성 ⑥ 캐나다의 안보 관점에서 취약점을 보관함으로써 예상되는 정보적 가치 평가 ⑦ 보관한 취약점을 사용해 얻을 것으로 예상되는 결과를 달성하기 위해 다른 유사한 기능을 CSE에서 사용할 수 있는지 여부 ⑧ 캐나다 정부 및 주요기반시설의 정보시스템 및 기술과 캐나다에서 널리 사용되는 정보시스템 및 기술에 대한 취약점의 영향을 줄일 수 있는 완화 조치가 있는지 여부 ⑨ 해당 제품에서 식별된 취약점을 책임감 있게 완화하려는 민간 부문의 역량 및 의지 및 이를 위한 CSE의 지원 필요성과 CSE의 역량 및 권한 평가 ⑩ 취약점이 동맹국 등에 의해 제공되었는지 여부와 유사한 공개심의 절차에 따라 이미 평가되었는지 여부 |

IV. 보안취약점 공개심의정책의 설계

1. 취약점 공개심의정책의 운영 주체

보안취약점 공개심의정책은 국가의 대외 및 안보전략과 깊게 연관된다. 이러한 점에서 우리나라 또한 정보활동을 전담하는 국가정보원이 실무를 전담해야 한다는 관점도 있다(장노순, 2022, 64). 미국의 경우 사이버보안 전반은 국토안보부가 전담하지만 사이버 정보수집이나 취약점 공개심의절차 등은 NSA가 담당하고 있다. 이에 대하여 심의절차의 중립성 문제 등을 고려해 NSA 정보보증부의 사무국 기능을 국토안보부로 이관해야 한다는 주장도 있다(Schwartz and Knake, 2016, 15). 그러나 현재 영국도 정보기관인 GCHQ가 NCSC를 운영하며 취약점 공개심의절차를 다루고 있다. 캐나다와 호주 또한 각각 신호정보기관인 CSE와 ASD가 취약점 공개심의 실무를 맡고 있다. 아울러 독일 내무부는 2021년 사이버보안전략을 통해 취약점 공개심의정책을 설계 중이라고 밝혔으나 사무국 업무를 수행할 기관이나 의사결정기구 등을 구체적으로 공개하고 있지는 않다(Federal Ministry of the Interior, Building and Community, 2021, 96). 관련 공개적 논의를 수행하면서 추진한 연구에서는 군사기관이나 안보기관보다는 사무국 자체의 기능 또한 부처 간 의견을 조정할 수 있도록 대통령실이나 총리실에서 담당할 수 있어야 한다고 권고한 사례도 확인된다(Herpig, 2018, 15).

취약점 문제는 국가사회 전반과 민간 부문에도 영향을 미친다. 따라서 취약점 공개 문제는 범부처 및 전문가들이 참여한 의사결정체계를 통해 논의해야 한다(Clarke and Morell et al. 2013, 219-220). 특히 조정 기능은 그러한 상위 의사결정기구에 부여될 수 있어야 한다. 다만 적어도 지금과 같은 상황에서 실무지원 기능은 안보적 관점에서 접근하는 것이 타당하다고 생각된다. 현재 취약점이 민간에도 영향을 미치면서 각국 정보기관의 정보활동 수단으로 활용되고 있는 점, 우리나라의 안보 특성을 고려할 때 북한, 중국, 러시아가 고도의 해킹 역량을 갖춘 국가라는 점, 국가정보원이 사이버안보 역량을 갖추고 관련 기능을 수행하고 있다는 점을 고려해야 하기 때문이다. 결국 최소한 취약점에 대한 세계적 접근이 안보 활동에서 벗어나 일반적인 보안 관점에서 수행되지 않는 이상 취약점은 국가적 정

보이의 경쟁과 시민 보호의 수단이 될 수밖에 없는 것이다. 글로벌 차원의 접근이 필수적인 이유이기도 하다. 국내에서는 오히려 그러한 인식을 공유하고 권한을 부여하되 오남용이 없도록 실질적인 법적 통제장치를 마련하는 것이 중요하다.

따라서 연락 관리, 기록관리, 정보공유, 보고서 작성 등 의사결정기구의 실무와 심의절차를 지원하는 사무국의 역할은 국가정보원 국가사이버안보센터에서 수행하되 심의의 최종 결정은 다양한 이해관계 주체들이 참여하는 의사결정기구에서 수행해야 한다. 그러한 의사결정기구의 의장은 미국이 NSC 내 사이버보안 전문가를 지명하고 있는 것과 같이 상위 조직에서 담당하는 것이 선진적이다. 보다 포괄적이고 중립적인 관점에서 안건을 검토하고 부처 간 의견을 조율할 수 있어야 하기 때문이다. 예를 들어 청와대 국가안보실 신기술사이버안보비서관이 주재하고 국가정보원 국가사이버안보센터 및 부문별 정보기관의 담당자들이 참여하는 국가취약점관리회의를 운영해 볼 수 있을 것이다. 국가취약점관리회의에는 공공뿐만 아니라 민간 전문가들도 참여하도록 할 수 있다. 이제 민간 보안업체들과 협력하지 않고서는 원하는 수준의 사이버안보 활동을 수행하기 어려운 상황이다(장노순, 2022, 68). 민간 보안업체들은 국제규범이나 정치 외교적 관계로부터 비교적 자유롭고 기술 역량이나 전문성 등이 뛰어나 다수의 위협정보를 빠르게 수집할 수 있다. 따라서 취약점 공개심의정책에 민간위원의 형태로 민간 부문의 참여를 보장하는 것이 타당하다고 생각된다. 나아가 법적 타당성과 기술적 전문성 또한 요구된다는 점에서 학계 전문가를 참여하도록 함으로써 전문성과 함께 객관성도 확보할 수 있다.

2. 명확한 법적 근거의 마련

현재 상황에서 취약점 공개심의정책은 결국 사이버안보에 관한 법률로 다뤄야 하는 문제다. 그러나 현재 국가 차원의 사이버안보 활동을 다루는 법률이 없는 상황이다. 국가사이버안보법안이 국회에 계류 중이지만 취약점의 국가적 관리나 공개심의정책에 관한 내용은 없다.

국가 차원에서의 취약점 관리 필요성과 역할 및 책임, 기준과 절차를 규정하는 근거법이 필요하다. 특히 취약점 문제는 민간 부문에도 영향을 미칠 수 있고 민간의 참여도 요구된다는 점에서 반드시 명확한 법적 근거가 필요하다. 아울러 취약점을

활용해 수사를 진행하는 등 사법 절차를 추진하려면 취약점 활용의 최초 판단 기준이 되는 취약점 공개심의정책 또한 법률로 규율해야 한다. 우리 헌법 제12조제1항 후문과 제3항이 천명하는 적법절차의 원칙과 형사소송법 제308조의2에 따른 위법수집증거의 배제 원칙을 준수해야 하기 때문이다.

따라서 국가사이버안보법을 제정하면서 취약점의 국가관리 원칙과 취약점 공개심의정책의 운영 주체, 의사결정기구와 해당 기구의 구성 및 구성방안, 평가절차와 기준 요건, 오남용 통제 및 보고의무에 관한 사항들을 함께 규정할 수 있어야 한다.

3. 취약점 공개심의정책 제안

취약점 공개심의정책의 핵심은 정부가 취약점을 저장하고 활용하기보다 사업자에게 알려주는 것을 우선으로 하자는 데 있다. 호주가 보안을 우선으로 한다는 원칙을 세우고 있는 점, 영국과 호주가 실무진 결정만으로도 취약점을 공개할 수 있도록 하는 점 등을 고려하면 취약점은 보안을 우선으로 공개하는 것이 원칙이어야 한다. 각국의 정부들이 보안을 우선으로 하지 않고 공격에 취약점을 우선 활용한다면 보안은 계속 약해질 수밖에 없다(윤상필, 2021, 225).

따라서 취약점을 확보하게 되면 실무를 전담하는 국가정보원에서 판단해 관련 사업자에게 취약점의 존재를 알려줄 수 있어야 한다. 공개 판단을 한 경우 사업자와 함께 패치를 개발할 수도 있을 것이다. 아울러 보관 결정을 했더라도 우리 기업이나 기관에 영향을 미칠 수 있는 취약점이라면 패치를 개발해두는 것이 안전할 수 있다. 작전 목적을 달성했거나 해당 취약점이 다른 제3자에 의해 발견됐다면 수행했거나 수행 중인 작전이 드러나지 않는 시점에 미리 개발해 둔 패치를 즉시 배포함으로써 우리 기업과 기관들의 피해를 예방하는 것이 타당하다. 아울러 우리 기관이나 기업의 취약점을 구매해서 보안을 강화하는데 쓸 수도 있다(Li and Liao, 2018, 8-9).

반면 취약점을 공개하지 않고 보관, 활용하려는 경우 일련의 요건들을 검토해 적정 절차에 따른 승인을 받아야 한다. 또한 정부가 보관하는 취약점이 유출되지 않도록 강력하게 보호해야 함은 물론이다. 요건을 설계하는 때에는 주요국의 공통 사항들을 고려하면서 우리 자체의 특성이나 자체 기준을 반영할 수 있어야 한다. 관련하여 <표 7>과 같은 기준을 고려할 수 있을 것이다.

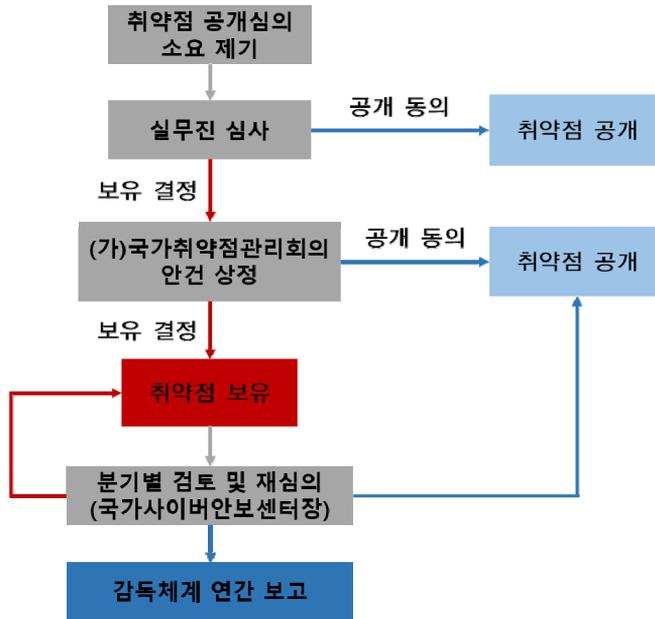
〈표 7〉 취약점 공개심의 결정의 기준안

| 내용 |
|--|
| ① 해당 취약점의 영향을 받는 제품과 제품의 속성, 버전 및 범용성 |
| ② 해당 취약점이 공개되면 악용될 가능성 |
| ③ 해당 취약점의 심각성 |
| ④ 취약점 공개 후 패치의 개발 및 배포 실효성 |
| ⑤ 해당 취약점을 다른 기관이나 단체, 개인이 찾아낼 가능성 |
| ⑥ 해당 취약점의 활용이 정보활동이나 수사 등의 목적에 도움이 되는지 여부 |
| ⑦ 대체할 다른 수단이 없는지에 관한 보충성 여부 |
| ⑧ 해당 취약점이 공개될 경우 정보의 출처나 수단, 방법 등이 드러날 가능성 |
| ⑨ 해당 취약점이 공개될 경우 우리나라 정부의 대외 관계 및 산업계 등 외부 관계에 관한 영향 |
| ⑩ 해당 취약점의 활용으로 인해 침해되는 권리 및 이익형량 결과 |

무엇보다 취약점을 활용하는 행위는 침익성이 매우 높다는 점에서 목적을 달성하기 위해 다른 방법이 없는 경우에만 취약점을 활용해야 한다. ⑦번 요건과 같이 보충성을 면밀히 판단해 취약점을 활용함으로써 얻게 되는 이익과 침해되는 이익을 비교 형량하여 전자의 이익이 월등한 경우에만 허용되어야 한다.

기본적인 절차는 ① 취약점 공개심의의 소요 제기 → ② 실무진 검토 및 권고 → ③-1 권고 결과가 ‘공개’인 경우 해당 업체에게 취약점 제보, ③-2 권고 결과가 ‘보관’인 경우 상위 의사결정기구에 안건 상정, ④ 상위 의사결정기구의 공개 또는 보관 결정, ⑤ 실무기관인 국가사이버안보센터장의 분기별 검토 및 재평가에 따른 취약점 공개 또는 보관 재결정, ⑥ 외부 감독체계와의 연간 보고로 구성해 볼 수 있다. 특히 내국인을 대상으로 보안취약점을 활용하려는 경우 법관의 영장을 받아야 한다. 그 외의 경우에는 자체 검토와 대통령의 승인만으로도 절차를 진행할 수 있을 것이다. 아울러 국가사이버안보센터장은 취약점 보관 결정을 분기별로 검토하여 목적을 달성했거나 공개하는 이익이 더 큰 경우 재평가하여 공개할 수 있어야 한다. 이러한 전반의 합의 및 결정 내용은 연간 보고 형태로 감독체계에 보고해야 한다.

〈그림 5〉 우리나라 취약점 공개심의절차 제안



4. 감독체계 설계

필요한 권한을 부여하려면 오남용을 방지하고 신뢰를 보장할 수 있는 감독체계를 마련해야 한다. 적정 수준의 통제와 감독을 통해 정당성을 부여하고 국민의 신뢰와 지지를 받음으로써 강력하고 확실한 권한과 자원을 받을 수 있기 때문이다(전웅, 2015, 567). 따라서 정부의 오남용 행위를 효과적으로 통제할 수 있는 환경을 조성해야 한다(Garcha, 2018, 863). 영국은 공개심의감독위원회를 두고 있으며 호주의 경우 정보안보감사관이 독립적인 지위와 권한으로 취약점 공개심의정책을 검토한다. 이에 따라 ASD로 하여금 취약점 공개심의정책에 관한 연간 보고서를 작성해 제출하도록 하고 있다. 캐나다 또한 CSE 커미셔너와 의회 국가안보 및 정보위원회의 사후 감독을 받고 있다.

이러한 감독체계는 기관의 내부와 외부 모두에 마련되어야 한다. 기관 스스로 문제점을 식별하고 개선할 수 있으면 가장 효과적이다(이원우, 2011, 116). 현장의 신속한 대응과 감독 등은 내부 감독체계를 통해 효율적으로 확보할 수 있기

때문이다. 역량있는 감독관을 두는 것도 중요하다. 전문적인 활동을 효과적으로 통제하려면 감독관의 역량이 보장되어야 한다(Lowenthal, 2012, 217). 기술적 현상을 이해할 수 있는 지식과 함께 그 문제의 위법성을 판단할 수 있어야 한다. 그러나 내부 차원의 감독체계는 조직의 보호나 동료애 등을 이유로 제대로 기능하지 않을 우려가 있다(전웅, 2015, 571-572). 또한 오남용 행위는 실무자나 중간 관리자보다는 기관의 최고 관리자층에서 결정되는 경향이 있다는 점도 고려해야 한다(Posner, 2008, 258). 이러한 차원에서 외부의 독립적인 감독체계가 요구된다. 실질적인 감독과 통제가 이루어지려면 독립성과 지위가 보장되어야 한다. 국가정보원, 검찰, 경찰, 군사안보지원사령부 등의 권력기관들을 관장할 수 있어야 하기 때문이다(이재일, 2015, 34).

따라서 외부 감독체계는 대통령 직속의 독립된 행정조직으로 두는 것이 타당하다. 효과적인 감독을 수행하기 위해 감독기구에는 반드시 고도의 기술을 활용한 정보활동을 이해하고 검토할 수 있는 전문인력을 뒤야 한다(Franklin and King, 2018, 40). 관련 인원들은 민주적 통제절차를 이해하고 법적, 기술적 전문성뿐만 아니라 국가안보 관념과 정보활동의 중요성 등을 이해할 수 있어야 한다(Jasutis and Fuior et al. 2020, 78-80). 감독조직의 권한도 명확한 법률로 보장해야 한다. 미국은 CIA 감사관(Inspector General)을 신설하는 과정에서 기밀정보에 접근하는 등 본연의 감독 기능을 적절하고 효과적으로 수행할 수 있도록 명확한 법적 권한을 줘야 한다고 판단했다(Bowsher, 1988, 7-8).

아울러 취약점 결정에 관한 통계는 공개할 필요도 있다. 시민의 입장에서는 정보기관이 취약점을 활용해 어떤 활동을 수행한다는 사실만으로도 우려의 시선을 가질 수밖에 없다(Black, Jr. 1997, 2). 따라서 정부는 시민의 신뢰와 승인을 얻기 위해 투명성을 보장할 수 있는 합리적인 소통방법을 모색해야 한다(Reddick and Chatfield et al. 2015, 138). 다만 과도한 투명성은 오히려 취약점을 활용해 얻고자 하는 목적을 저해하고 외교적 마찰 등 예상하지 못한 문제를 낳을 수 있다. 이러한 점을 고려해 구체적인 취약점 정보의 출처나 활용처, 활용 방법과 결과 등은 국가안보의 목적상 공개하지 않는 것이 타당하다. 반면, 취약점 공개심의정책으로 다룬 건수, 취약점 공개 및 사업자 제공 건수, 이를 통해 취약점이 제거된 횟수와 같은 통계들은 공개할 수 있어야 한다.

V. 결론

이중적일 수밖에 없는 기술적 속성을 가진 보안취약점은 각국 정부의 이해관계에 얽히면서 전략 우위를 확보하기 위한 자원경쟁의 대상으로 변모했다. 취약점을 가진 국가는 그것이 다른 누군가에 의해 드러나 제거되지 않는 이상 원하는 이익을 얻을 수 있다. 정보활동이나 수사 등을 위해 사용할 수도 있고 자국 기업이나 기관의 보안을 강화하기 위해 공유할 수도 있다. 특히 취약점의 문제는 디지털 전환이 고도화될수록 안전과 직결된다는 점도 중요하다.

안전과 관련된 문제라면 조금 더 앞선 미래를 생각하고 대비해보자. 취약점은 국가안보의 관점에서 다뤄야 하는 자원이자 재난안전의 관점에서 처리해야 하는 결함이다. 이 필요성을 강조하고 사회의 인식과 공감을 얻는 데까지 오랜 시간이 걸릴 수 있다. 그러나 이미 주요 선진국들이 그러한 절차를 두고 정당성을 확보하고 있는 점에 비해 국내에서는 취약점의 정책적 관리 필요성에 관한 논의가 턱없이 부족한 상황이다. 이에 본 연구는 취약점의 국가적 관리 필요성을 제기하고 이를 위한 절차의 법적 의의와 고려사항들을 검토하여 구체적인 설계방안을 제안했다.

먼저 취약점의 공개 또는 보관 여부를 판단하는 절차인 취약점 공개심의정책의 법적 근거를 마련해야 한다. 사이버안보와 관련되는 문제이기 때문에 사이버안보에 관한 법률을 먼저 제정하고 취약점의 국가적 관리와 공개심의절차에 관한 사항, 오남용 통제에 관한 사항들을 명시해야 한다. 또한 국가정보원의 국가사이버안보센터가 운영을 전담하되 의사결정기구로 가칭 ‘국가취약점관리회의’를 둘 수 있을 것이다. 동 회의는 청와대 국가안보실 신기술사이버안보비서관이 주재하고 국가정보원 사이버안보센터 및 국방, 경찰 등 사안에 따른 관계 기관의 담당자들과 함께 민간 보안업체와 법적, 기술적 전문성을 갖춘 학계 전문가 등이 참여하는 것이 타당하다. 취약점 문제는 특정 기관이나 공공 부문에만 한정되지 않기 때문이다.

아울러 권한이 부여되는 만큼 정부는 책임성을 강화하고 불필요한 권리침해를 최소화하면서 신뢰를 확보하기 위한 노력을 다해야 한다. 이를 위해 취약점 활용 관행을 감독할 수 있는 감독체계를 기관의 내부와 외부 모두에 뒤야 한다. 특히 내부의 감독체계만으로는 신뢰성과 객관성을 온전히 담보하기 어렵다는 점에서 외부의 독립 감독체계로서 대통령 직속의 독립된 감독조직을 제안하였다. 무엇보다

다 감독체계의 핵심은 기술적 문제들을 식별하고 쟁점을 이해할 수 있는 최고 수준의 전문성이라고 할 수 있다. 또한 국민의 알 권리 차원에서 국회 정보위원회의 역량도 강화하고 최근 헌법재판소의 결정에 따라 정보위원회 회의의 공개 문제에 대응할 수 있도록 비공개 요건을 법적으로 확립하되 합리적인 수준에서 통계적인 내용들은 공개할 수 있어야 한다.

투 고 일 : 2022. 02. 05.

심사완료일 : 2022. 03. 29.

계 재 일 : 2022. 05. 30.

참고문헌

1. 국내 자료

- 국가정보원. 2021. 『2021 연례보고서: 국가사이버안보센터』.
- 김창섭·이상진. 2021. “안보 목적의 해외정보 온라인 수집을 위한 법제도 연구”. 『국가정보 연구』 제14권 제1호. 한국국가정보학회.
- 김한균. 2019. “수사기관의 정보 수집·생산 기능 합리화-영국 국가범죄수사청 정보기능 분장 및 통제 사례를 중심으로-”. 『형사소송 이론과 실무』 제11권 제2호. 한국형사소송법학회.
- 박광민·박용신. 2019. “글로벌 정보환경에서의 방첩업무 개선방안”. 『외법논집』 제43권 제2호. 한국외국어대학교 법학연구소.
- 오일석. 2019. “미국 정보기관 제로데이 취약성 대응 활동의 법정책적 시사점”. 『미국헌법 연구』 제30권 제2호. 미국헌법학회.
- 윤상필. 2021. “보안취약점의 사회적 인식과 법·기술적 대응전략”. 고려대학교 박사학위논문.
- 이원상. 2017. “형사법적 관점에서의 랜섬웨어 대응방안”. 『범죄수사학연구』 제3권 제1호. 경찰대학 수사과학연구센터.
- 이원우. 2011. “현대적 민주법치국가에 있어서 행정통제의 구조적 특징과 쟁점”, 『행정법 연구』 제29호. 행정법이론실무학회.
- 이재일. 2015. 『통신감청제도의 문제점과 개선방향』. 국회입법조사처.
- 장노순. 2022. “정보기관과 비국가 행위자의 이중관계: 사이버 위협의 공개지목과 사이버 공작을 중심으로”. 『국가안보와 전략』 제21권 제4호. 국가안보전략연구원.
- 전웅. 2015. 『현대 국가정보학』. 박영사.
- 한희원. 2017. “국가안보 패러다임의 변화와 정보 수사 융합에 대한 법규범적 연구: 전쟁에서 국가안보사법과의 전투로”. 『법학연구』 제17권 제2호. 한국법학회.

2. 국외 자료

- Ablon, Lillian and Bogart, Andy. 2017. *Zero Days, Thousands of Nights: The Life and Times of Zero-day Vulnerabilities and Their Exploits*. RAND Corporation.
- Agresti, William W. 2010. “The Four Forces Shaping Cybersecurity”. *Computer* 43(2). IEEE.

- Arora, Ashish, Krishnan, Ramayya, Telang, Rahul and Yang, Yubao. 2004. "Impact of Vulnerability Disclosure and Patch Availability - An Empirical Analysis". in *the 3rd Workshop on the Economics of Information Security*.
- ASD. 2019. "Responsible Release Principles for Cyber Security Vulnerabilities".
- Black, Jr., William B. 1997. "Thinking Out Loud about Cyberspace", *Cryptolog*, National Security Agency.
- Bowsher, Charles A. 1988. "Testimony on the Establishment of an Inspector General at the Central Intelligence Agency". Government Accountability Office.
- Buchanan, Ben. 2020. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*, Cambridge. MA: Harvard University Press.
- Bundesministerium des Innern, für Bau und Heimat. 2021. *Cybersicherheitsstrategie für Deutschland 2021*.
- Civiletti, Benjamin R. 1980. "Intelligence Gathering and the Law: Conflict or Compatibility?". *Fordham Law Review* 48(6).
- CISA. 2021. "NSA-CISA-FBI Joint Advisory on Russian SVR Targeting U.S. and Allied Networks".
- CISA, FBI, NSA, ACSC, CCCS, CERT-NZ, NZ-NCSC, and NCSC-UK. 2021. "Mitigating Log4Shell and Other Log4j-Related Vulnerabilities". Joint Cybersecurity Advisory.
- Clarke, Richard A., Morell, Michale J., Stone, Geoffrey R., Sunstein, Cass R. and Swire, Peter. 2013. *Liberty and Security in a Changing World*. The President's Review Group on Intelligence and Communications Technologies.
- Crowd Strike. 2019. *Global Threat Report 2019: Adversary Tradecraft and the Importance of Speed*.
- Crowd Strike. 2021. "OverWatch Exposes AQUATIC PANDA in Possession of Log4Shell Exploit Tools During Hands-on Intrusion Attempt".
- CSE. 2019. "CSE's Equities Management Framework".
- Deeks, Ashley S. 2016. "Confronting and Adapting: Intelligence Agencies and International Law". *Virginia Law Review* 102(3).

- Desai, Deven R. and Kroll, Josua A. 2017. "Trust but Verify: A Guide to Algorithms and the Law". *Harvard Journal of Law & Technology* 31(1).
- Federal Ministry of the Interior, Building and Community. 2021. Cyber Security Strategy for Germany 2021.
- Franklin, Sharon B. and King, Eric. 2018. *Strategies for Engagement Between Civil Society and Intelligence Oversight Bodies*. New America.
- Garcha, Rupinder K. 2018. "NITs a No-Go: Disclosing Exploits and Technological Vulnerabilities in Criminal Cases". *New York University Law Review* 93(4).
- GCHQ. 2018. "The Equities Process".
- Herpig, Sven. 2018. *Governmental Vulnerability Assessment and Management*, Stiftung Neue Verantwortung.
- Heyman, Steven J. 1991. "The First Duty of Government: Protection, Liberty and the Fourteenth Amendment", *Duke Law Journal* 41.
- Jaikaran, Chris. 2017. "Vulnerabilities Equities Process". Congressional Research Service.
- Jasutis, Grazvydas, Fuor, Teodora and Vashakmadze, Mindia. 2020. *Parliamentary Oversight of Military Intelligence*, NATO Parliamentary Assembly, DCAF.
- Joyce, Rob. 2016. "Disrupting Nation State Hackers", *USENIX Enigma* 2016.
- Kaplan, Fred. 2016. *Dark Territory: The Secret History of Cyber War*, New York: Simon & Schuster.
- Li, Zhen and Liao, Qi. 2018. "Harnessing Uncertainty in Vulnerability Market", in *the Proceeding of the 2018 27th International Conference on Computer Communication and Networks(ICCCN)*, IEEE.
- Loleski, Steve. 2019. "From cold to cyber warriors: the origins and expansion of NSA's Tailored Access Operations(TAO) to Shadow Brokers". *Intelligence and National Security* 34(1).
- Lowenthal, Mark M. 2012. *Intelligence: From Secret to Policy(5th ed)*. California: CQ Press.
- NSA. 2020. "Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities".

- NSA/CSS. 2000. *Transition 2001(declassified)*.
- Matwyshyn, Andrea M., Cui, Ang, Keromytis, Angelos D., and Stolfo, Salvatore J. 2010. "Ethics in Security Vulnerability Research". *IEEE Security & Privacy* 8(2).
- ODNI. 2010. "Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process".
- Posner, Richard A. 2008. "Privacy, Surveillance, and Law", *The University of Chicago Law Review* 75(1).
- Reddick, Christopher G., Chatfield, Akemi Takeoka and Jaramillo, Patricia A. 2015. "Public Opinion on National Security Agency Surveillance Programs: A Multi-Method Approach", *Government Information Quarterly* 32(2).
- Saltzman, Ilai. 2013. "Cyber Posturing and the Offense-Defense Balance", *Contemporary Security Policy* 34(1).
- Schneier, Bruce. 2017. "Class Breaks". Schneier on Security.
- Schwartz, Ari and Knake, Rob. 2016. *Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process*, Harvard Kennedy School Belfer Center.
- Shirey, Rob. 2000. "Vulnerability". Internet Security Glossary(RFC 2828). Internet Engineering Task Force(IETF), Internet Society(ISOC).
- Tasheva, Iva. 2017. "DIGITAL EUROPE position paper on vulnerability stockpiling". DIGITAL EUROPE.
- U.S. President's Commission on Critical Infrastructure Protection. 1997. *Critical Foundations: Protecting America's Infrastructures*.
- Williams, Ian. 2018. "The Secrets We Keep...: Encryption and the Struggle for Software Vulnerability Disclosure Reform". *Michigan Technology Law Review* 25(1).
- Williams, Robert D. 2011. "(Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action". *The George Washington Law Review* 79(4).
- Winner, Langdon. 1978. *Autonomous Technology: Technics-out-of-Control as*

a Theme in Political Thought. Cambridge: The MIT Press.

Wu, Weimi. 2015. "Hacking Team Flash Zero-Day Tied To Attacks In Korea and Japan... on July 1". Trend Micro.

Zhang, Daniel. 2019. "Vulnerabilities Equities Process Revisited". Georgetown Security Studies Review.

工业和信息化部, 国家互联网信息办公室, 公安部. 2021. "网络产品安全漏洞管理规定".

3. 인터넷 자료

Cox, Joseph. 2016. "GCHQ Has Disclosed Over 20 Vulnerabilities This Year, Including Ones in iOS(2016.04.30)". VICE. <https://www.vice.com/en/article/yp3w3j/gchq-vulnerabilities-mozilla-apple> (검색일: 2022년 1월 10일).

De Standaard. 2021. "Defensie slachtoffer van ernstige cyberaanval(2021.12.20)". https://www.standaard.be/cnt/dmf20211220_92316559 (검색일: 2022년 1월 4일).

Fung, Brian. 2013. "The NSA hacks other countries by buying millions of dollars' worth of computer vulnerabilities(2013.08.31)". The Washing Post. <https://www.washingtonpost.com/news/the-switch/wp/2013/08/31/the-nsa-hacks-other-countries-by-buying-millions-of-dollars-worth-of-computer-vulnerabilities/> (검색일: 2022년 1월 8일).

Hern, Alex. 2015. "Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim(2015.07.06)". The Guardian. <https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim> (검색일: 2022.01.13).

Kirchgaessner, Stephanie. 2021. "NSO Group spyware used to hack at least nine US officials' phones(2021.12.03)". The Guardian. <https://www.theguardian.com/world/2021/dec/03/us-state-department-officials-iphones-hacked-nso-group-spyware> (검색일: 2022년 1월 7일).

Nakashima, Ellen. 2020. "NSA found a dangerous Microsoft software flaw and alerted the firm-rather than weaponizing it(2020.01.14)". The Washington Post. <https://www.washingtonpost.com/national-security/nsa-found-a->

dangerous-microsoft-software-flaw-and-alerted-the-firm—rather-than-weaponize-it/2020/01/14/f024c926-3679-11ea-bb7b-265f4554af6d_story.html (검색일: 2022년 1월 8일).

Rosenblum, Todd. 2021. “What to do with cyber vulnerabilities?(2021.07.08.)”. The Hill. <https://thehill.com/blogs/congress-blog/technology/562116-what-to-do-with-cyber-vulnerabilities> (검색일: 2022년 1월 13일).

Riley, Michael. 2014. “NSA Said to Have Used Heartbleed Bug, Exposing Consumers(2014.04.11.)”. Bloomberg News. <http://www.bloomberg.com/news/articles/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers> (검색일: 2022년 1월 12일).

Starks, Tim. 2021. “‘Almost every nation’ now has cyber vulnerability exploitation program, NSA official says(2021.09.29.)”. CYBERSCOOP. <https://www.cyberscoop.com/rob-joyce-nsa-cyber-exploitation-program/> (검색일: 2022년 1월 11일).

The Register. 2016. “Mozilla slings Firefox patches at flaw found by GCHQ’s infosec arm(2016.04.28.)”. https://www.theregister.com/2016/04/28/firefox_patch/ (검색일: 2022년 1월 10일).

Waterman, Shaun. 2017. “Should the government stockpile zero-day software vulnerabilities?(2017.05.19.)”. CYBERSCOOP. <https://www.cyberscoop.com/should-the-government-stockpile-zero-day-software-vulnerabilities/> (검색일: 2022년 1월 8일).

Legal Understanding and Institutional Design of Vulnerabilities Equities Process

Sang-pil, Yoon · Hun-yeong, Kwon

Security vulnerabilities are strategic resources that must be managed at the national level. Therefore, it is necessary to establish a procedure to determine whether it is profitable to disclose or retain vulnerabilities from the national strategic point of view. To this end, this paper proposed to accept the concept of the Vulnerabilities Equities Process(VEP) and its specific design framework. First, the National Intelligence Service should be in charge of the executive secretariat in that vulnerability issues are directly related to national cybersecurity. However, as a decision-making body for VEP, a so-called ‘National Vulnerability Management Meeting’ should be set up and presided over by the New Technology and Cyber Security Secretary at the Blue House National Security Office, allowing related agencies, private security firms and academic experts to participate. In addition to these matters regarding the operating entity and decision-making body, a law is needed that comprehensively deals with detailed standards and requirements for VEP, with matters on oversight system.

Keywords: Vulnerability, Security Vulnerability, Vulnerability Disclosure, Vulnerability Equities Process, National Cybersecurity