

## A Study on Priorities of Cyber Security Policy and Governance

Hyeon Suk Lyu<sup>1+</sup>, Hee Jung Cho<sup>2</sup>, Hun A Lee<sup>1</sup>

<sup>1</sup> The Korea Institute of Public Administration, 235 Jinheung-ro, Eunpyeong-gu, Seoul, Korea

<sup>2</sup> Institute of Social Science, Dasan 432, Sogang University, 35, Baekbeom-ro, Mapo-gu, Seoul, Korea

### Abstract

Cyber-attacks and crimes are currently the fastest growing threats to almost every aspect of modern life. Yet, the Korean government and its policies do not seem to properly address the cyber-security issues and challenges. The aim of this study is to cover all aspects of cyber-security issues by taking a holistic approach. It first explores the notions and main tenets of cyber vulnerabilities and cyber resilience and develops the analytical framework based upon the concept of cyber resilience.

**Key words:** cyber threats, cyber security, cyber vulnerability, cyber resilience

### 1. 서론

2016년 7월 11일 인터파크에서 총 1,030만 명의 개인정보가 유출되는 사고를 비롯<sup>1)</sup>, 2014년 1월 초 국내 대표 카드 3사에서 총 1억 580명의 개인정보가 유출되는 등<sup>2)</sup> 최근 카드사, 이동통신사, 소셜커머스는 물론 정부부처 등 공공기관에서 연일 대규모 개인정보 유출 및 도난 사고가 발생하여 범사회적 불안을 초래하고 있다. 개인정보 유출 및 사이버침해 사고는 여러 분야에

서 다양한 방식으로 일어나고 있으며, 대규모 동시 다발성 DDoS(디도스) 공격 역시 증가하고 있다.

한편, 최근 액티브X와 공인인증서가 국내 모바일 금융시장 및 전자상거래 분야의 대표적 걸림돌로 인식되어 거센 비난을 받고 있다. 스마트폰 이용 활성화에 따른 모바일 사이버침해 위협 역시 매해 증가하고 있다. 악성 앱(App) 탐지건수는 2013년 2,351건에서 2014년 4,048건으로 전년대비 72%로 증가했고, 피싱<sup>3)</sup>, 파밍<sup>4)</sup>, 스미싱<sup>5)</sup> 차단건수는 2013년 10,311건에서 2014

<sup>+</sup> Corresponding author: Hyeon Suk Lyu, Tel. +82-2-2007-0685, Fax. +82-2-564-1046, e-mail. [hslyu@kipa.re.kr](mailto:hslyu@kipa.re.kr)

1) “‘개인정보 유출’ 인터파크, 행정기관 신고 의무도 안 따랐다.” 2016.07.27. 「한겨레」 (<http://goo.gl/sTI5k2>)

2) 2014.01.19. 금융감독원 보도자료

3) 피싱(Phishing): 개인정보(Private data)와 낚시(Fishing)의 합성어로, 금융기관 또는 공공기관을 가장해 전화나 이메일로 인터넷 사이트에서 보안카드 일련번호와 코드번호 일부 또는 전체를 입력하도록 요구해 금융 정보를 몰래 빼가는 수법(출처: 사이버경찰청)

4) 파밍(Pharming): 악성코드에 감염된 PC를 조작해 이용자가 은행, 금융회사 등 정상적인 홈페이지 주소로 접속하여도 가짜 사이트로 유도되어 범죄자가 개인 금융 정보 등을 몰래 빼가는 수법(출처: 사이버경찰청)

5) 스미싱(Smishing)은 문자메시지(SMS)와 피싱(Phishing)의 합성어로 문자메시지내 인터넷주소 클릭하면 악성코드가 설치되어 피해자가 모르는 사이에 소셜결제 피해 발생 또는 개인·금융정보를 탈취한다(출처: 사이버경찰청). 스미싱 문자의 경우, 공공기관(법원, 민원24 등) 사칭 스미싱(26.2%)이 가장 많고, 지인(23.9%), 택배(22.2%) 등의 순으로 나타났고, 브라질 월드컵(2014년 6월 6,002건),

년 15,470건으로 증가했다. 악성 앱 유포방식은 스마트폰 SMS를 통한 URL 링크에서 공유기 DNS 변조, 공식 앱마켓 이용 등 다변화되고 있으며, 캡차코드<sup>6)</sup>와 같은 새로운 방식이 출현하는 등 스미싱 위협이 한층 교묘해지고 있다.

사이버침해 사고의 사회적 피해는 엄청나다. 개인의 경우에는 개인 신원 정보의 도난, 사기, 위조지폐 및 저작권 침해 등의 피해자가 될 확률이 크다. 기업의 경우는 지적재산이나 기업기밀정보, 가치, 평판 등이 위협받을 수 있고 기업스파이 및 정보시스템 침해로 인해 막대한 재정적 손해를 입을 수 있다. 기업 및 개인의 손해는 곧 GDP 감소와 경제성장의 저하로 이어지기 때문에 장기적으로는 국가적 차원에서의 손실이라고도 할 수 있다. 정부차원에서는 스파이 및 사이버공격 등으로 인해 국가안보 및 국제외교 관계에 있어 불리한 상황에 처할 수도 있다. 수도, 전력, 식량공급, 국민보건 등을 제공하는 국가 핵심 기관 인프라가 공격을 받을 경우에는 엄청난 사회적 혼돈과 불안정을 초래해 국가 기능이 마비될 수도 있다(Wright & Schaetzel, 2013).

최근 사물인터넷, 클라우드, 빅데이터, 모바일 환경 등 새로운 기술 이용이 확대되면서 예측할 수 없는 사이버침해 사고는 더욱 증가할 전망이다. 보안 연구가 결여되어 있는 핀테크(FinTech) 등 복합 기술 등장과 급속한 확산으로 인해 국내 사이버보안 환경은 그 어느 때보다도 불안하고 위태롭다. 이러한 새로운 기술환경 및 금융시장의 변화는 정부의 사이버 보안 정책에 대한 심각한 도전이기 때문에 새로운 범정부적 사이버보안 체계 및 정책마련이 시급하다.

그러나 현행 사이버보안 법제도 및 거버넌스 체계가 이러한 변화를 반영하지 못하는 문화·제도적 지체현상(cultural lag)이 발생하고 있다. 급변하고 있는 국내외 사이버보안 환경 연구 역시 한계점을 지닌다. 기술적 대안에만 집중한 '기술 중심적' 접근 및 사이버 보안과 관련된 법제도적 고찰 등 특정 분야에만 초점을 맞춘

'단선적 접근'에 그치면서 국내 사이버 보안환경의 전체적인 수준이나 문제점을 규명하는 데 한계가 있다. 인종보안에 대한 연구도 마찬가지로 급변하는 외부환경 변화를 반영하고 있지 못한 채 공인인증 중심적 담론에서 크게 벗어나지 못하고 있다.

이에 본 연구는 급증하는 사이버 침해사고 유형과 특징을 파악하고 새로운 기술 환경 변화, 법제도, 조직문화, 사용자 인식 등을 아우르는 종합적 고찰을 토대로 정책적, 기술적 방안을 구체적으로 제시하고자 한다.

연구 방법론적으로 분석적 계층화 방법인 AHP(Analytic Hierarchy Process)분석을 이용한다. AHP조사는 각 계층 전문가의 의견을 동시에 수렴하여 합의된 내용을 토대로 정책적 우선순위를 도출하는 데 매우 적합하다(Kang, 2015). 보다 객관적인 정책 선정을 위하여 사이버보안 취약성, 복원력 강화 방안, 현 인증보안체계의 취약성, 향후 인증보안 복원력 강화 요인 등을 중심으로 총 네 개의 AHP 모델을 개발하고, 개발 모델 및 선정된 요인을 대상으로 1차적으로 전문가 브레인스토밍을 통해 수정보완 작업을 하였으며, 'ExpertChoice'라는 소프트웨어를 사용하였다.

## II. 이론연구 및 연구모형

### 1. 사이버침해와 사이버보안

사이버침해는 온라인에서 범죄로 규정되고 있는 행위 이외에도 법적으로 침해하는 모든 행위를 포함한다. 사이버침해는 컴퓨터와 인터넷을 이용하기 때문에 단적으로 정의하기가 어려우나, 사이버공간에서 발생하는 모든 범죄현상을 뜻하는 것으로(Cho & Shin, 2009), 사이버공격(cyber attacks) 또는 사이버 위협(cyber threats)을 포괄한다.

사이버침해 유형은 대체로 공격자의 공격의도(intention or motivation)에 따라 구분된다. Gallaher, et. al.(2014: 49)에서는 사이버공격 유형을 조직화된

추석(2014년 9월 6,135건) 등 사회적 이슈를 악용한 사례도 다수이다.

6) 캡차코드(Captcha Code): 문자, 숫자를 직접 입력하도록 하여 자동회원가입 등을 방지하는 방식



국내에서 가장 대표적인 인증 수단은 ‘공인인증서’이다. 공인인증서는 1990년 초 모든 데이터를 오프라인에서의 확인과정을 거치지 않고 온라인으로 처리하는 소위 ‘이음새 없는(seamless) 전자정부 및 전자상거래’를 실현하고자 탄생하였다. 온라인상 구현된 전자정부서비스나 전자금융거래서비스는 개인을 직접 대면할 수 없기 때문에 기존의 주민등록증, 인감도장 등의 역할을 대신할 수 있는 인증수단이 필요했다. 이를 해결하기 위해 공개키 기반의 전자서명 기술이 도입되었으며, 공인인증서는 온라인 비대면 환경에서 인증 수단으로 온라인상 인감증명서로 사용되기 시작했다.

기술적으로 공인인증서는 행위자에 대한 전자서명 기술을 사용하여 부인방지 기능을 구현할 수 있는 유일한 수단이다. 공인인증서는 국가공인인증기관(CA)에서 발급·관리하기 때문에 다른 인증 수단에 비해 신뢰성이 매우 높으며, 「전자서명법」을 통해 법적 효력을 지니는 강력한 인증 수단이다. 「전자서명법」은 공인인증서를 이용한 공인전자서명이 서명, 서명날인, 기명날인과 동일한 효력을 갖고 있으며, 전자거래에서의 법적 근거가 된다는 사실을 보장한다(National Information Society Agency, 2010). 공인인증서는 사이버공간에서 가장 확실한 신원확인수단이자 높은 보안성을 충족하기 때문에 기존 인증 수단 분류(what you know, what you have, what you are)에 공인인증서를 더하여 ‘신뢰성 있는 제3자(Trusted Third Party)’로 표현하기도 한다(Lee, 2013).

현재 국내 인터넷 환경은 외국에 비해 엄격한 본인확인 체계에 기반하고 있다. 현재 관련 법령에는 「전자서명법」, 「전자정부법」 등이 있고, 정보통신망과 정보시스템의 보호추진에 관한 법령은 「국가정보화기본법」, 「정보통신기반보호법」, 「정보통신망이용촉진및정보보호등에관한법률」, 「전자정부법」, 「전자거래기본법」, 「국

가사이버안전관리규정」 등이 있다(Korea Communications Commission, 2011).<sup>9)</sup> 최근 전자정부 사이트는 공인인증서를 통한 본인확인의 보안성을 높이기 위한 수단으로 ‘복합 인증’이라는 것을 도입하고 있지만, 이러한 수단도 결국에는 공인인증서를 통한 본인확인에 초점을 맞추고 있는 것이기 때문에 법적 문제가 남아 있다. 또한 최근 주민등록번호 수집이 금지되었으나, 여전히 많은 법조항에 광범위하게 본인확인 절차가 남아있다. 「개인정보보호법」 및 「정보통신망이용 촉진 및 정보보호 등에 관한 법률」상 주민등록번호 수집 및 이용의 법령상 예외로 허용되는 경우의 상당수가 이에 해당하며, 예외 규정들은 개인 식별이 전제된 정보 이용을 허용하기 때문에 실질적인 본인확인 체계로 기능한다(Shim, 2014: 214).

액티브X도 해결해야 할 과제이다. 공인인증서 기술이 기본적으로 마이크로소프트의 표준 기술인 액티브X를 기반으로 설계되었다는 점과 이로 인하여 보안상 취약성을 갖고 있으며,<sup>10)</sup> 그리고 보다 궁극적으로는 이용자의 편의성이 떨어진다는 점 등을 어떻게 해소해 나갈 것인지의 문제는 시급히 해소해야 할 사항이다.

결과적으로 공인인증서를 전자정부의 본인확인 수단으로 지속적으로 활용하고자 하는 경우, 공공영역 활용에 한정되는 공인인증서 체계 및 관리 거버넌스 구축 방법과 전자정부 본인확인 수단의 보안성 문제가 반드시 해결되어야 한다.

### 3. 사이버취약성과 사이버복원력

사이버취약성(cyber vulnerability)은 사이버공간에서 직접적으로 일어나는 물리적 피해에 초점이 맞춰져 있다. Ernst & Young(2014)에서는 취약성을 ‘공격 받거나 피해를 받을 가능성에 노출된 경우(as exposure to the possibility of being attacked or harmed)’로

9) 공인인증서와 관련 있는 「전자서명법」은 미래창조과학부, 민원 분야와 관련 있는 「전자정부법」은 행정자치부, 결제나 금융 서비스 이용 시 적용되는 「전자금융법」은 금융위원회 소관이다. 이 밖의 국가 사이버안보와 관련된 「국가사이버안전관리규정」은 국가정보원 소관이다.

10) 물론 HTML5 기술의 활용을 통해 액티브X의 기술·보안상의 한계를 뛰어넘을 수 있다는 주장이 있지만, 아직까지 이러한 기술은 실용화단계에 있지 않은 것으로 평가되고 있다.

정의했다. 그간 사이버취약성의 구성요소 관련 연구 역시 사이버공간의 물리적 피해에 초점을 맞춘 기술 부분에 편중되어 있다. Homeland Security(2011)는 보편적 사이버취약성 요소를 승인, 접근권한 제어, 인증서관리, ICS 보안설정 및 유지관리, 네트워크 설계의 취약성, 모니터링 문제 등으로 제시했다. 그러나 사이버취약성은 단순한 기술 문제뿐 아니라 개인 차원의 문제도 포함한다. 실제로 많은 사람들이 온라인 활동으로 인한 개인의 취약성을 잘 알지 못한다. 스마트폰에 내재된 GPS기능이나 손쉽게 저장하는 건강 관련 디지털 정보 등에 대해서는 보안을 생각하지 않는 경우가 많고, 클라우드 서비스에 개인정보를 저장해 발생할 수 있는 위험에 대해 인지하는 경우는 드물다(Gay, 2011).<sup>11)</sup>

이러한 취약성에 대응하는 개념으로 ‘복원력(resilience)’을 들 수 있다. 어원학적으로 복원력은 ‘다시 뛰어오른다(to jump back)’란 뜻의 라틴어 ‘리실리오(resilio)’에서 비롯되었다(Klein, *et. al.*, 2003; Manyena, 2006; Lyu, *et. al.*, 2009 재인용). 사전적 정의의 경우, 메리엄-웹스터 사전에서는 복원력을 ‘스트레스로 인해 압박감을 받은 개체가 크기와 모양을 회복하는 능력 또는 예기치 못한 불의의 사고 또는 변화 등에 쉽게 적응하거나 회복하는 능력’으로 정의한다. 이러한 특징에 따라 복원력 개념은 사이버보안 취약성의 대안이 된다. 다만, 사이버복원력은 보편적으로 이용되는 정의가 없기 때문에 다음 <Table 1>과 같이 다양하게 정의된다.

복원력을 구성하는 요소로는 시스템 견고성, 가외성, 자원동원성, 신속성, 적응성 및 흡수력 등이 포함된다. 특히, 복원력의 구성 요소는 개념정의와 마찬가지로 재난 분야에서 활발히 연구되었다. Bruneau, *et. al.*(2003)은 복원력을 견고성(robustness), 중복성(redundancy), 자원

Table 1. Various definitions of cyber resilience

Author	Definitions
Merriam-Webster	<ul style="list-style-type: none"> <li>The capability of a strained body to recover its size and shape after deformation caused especially by compressive stress</li> <li>An ability to recover from or adjust easily to misfortune or change</li> </ul>
NIAC, 2010	<ul style="list-style-type: none"> <li>Infrastructure resilience is the ability to reduce the magnitude and/or duration of disruptive events.<sup>12)</sup></li> </ul>
Presidential Policy Directive, 2013	<ul style="list-style-type: none"> <li>The term ‘resilience’ means the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruption. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.</li> </ul>
NAS(National Academy of Science), 2012	<ul style="list-style-type: none"> <li>The ability to prepare and plan for, absorb, recover from and more successfully adapt to adverse events.</li> </ul>
Marc Werfs, 2013	<ul style="list-style-type: none"> <li>The essence of resilience is to build a decisive advantage by being prepared for disruptive events.</li> </ul>
Caitríona, H., 2014	<ul style="list-style-type: none"> <li>The ability of the nation or region(e.g. ASEAN region) and its citizens to be prepared, to be able to adapt, and to make quick process post-events.</li> </ul>
EY, 2014: 1	<ul style="list-style-type: none"> <li>Cyber resilience is the ability to powerfully resist, react to and recover from potentially catastrophic cyber-security threats, and reshape their environments for increasingly secure, sustainable cyber operations.</li> </ul>

동원성(resourcefulness), 신속성(rapidity) 네 가지로 구분하였다. Maguire & Hagan(2007)은 저항력(resistance), 회복력(recovery), 창조력(creativity)을 제시한다(Kang, *et. al.*, 2013).

Tiernery & Bruneau(2007)는 4R모델, 견고성, 가외성(여유), 자원동원성, 신속성을 네 가지 차원으로 구분하였다. 이 모델을 바탕으로 복원력의 영역을 <Table 2>와 같이 기술영역, 조직영역, 사회영역, 경제영역 총 네 가지로 구분하였다.

11) Ernst & Young(2014) 조사결과, 사이버취약성에서 가장 많이 나타나는 항목은 내부 직원의 부주의 및 접근권한이 없는 직원의 임의접근(38%)으로, 이는 낡은 정보보안 컨트롤(시스템)이나 구조의 문제(35%)보다 더 많이 발생하는 것으로 알려졌다. 클라우드 서비스 이용, 모바일 이용, 외부 무단 접근 등은 15% 내외로 비등하게 나타났는데, 클라우드 서비스나 모바일 이용과 같은 분야에서는 사이버취약성을 인지하기 어렵다. 소셜미디어 이용(7%) 역시 취약성의 한 종류로 나타났는데, 소셜 미디어를 통해 자신의 위치 정보, 개인 정보(휴가 날짜 및 장소, 출장지 등) 등이 노출될 경우 사이버취약성을 유발할 가능성이 높다.

12) Infrastructure protection은 위협적 사건의 영향을 줄이거나 막는 것, Infrastructure resilience는 붕괴의 중요도, 영향, 지속기간을 줄이는 능력을 가리킨다(NIAC, 2009).

Table 2. Four domains of resilience

Domains	Contents
Technology	System's physical characteristics of reducing damages and functional errors
Organization	Organization or institution that manage physical elements of system
Society	Characteristics of social groups or individuals
Economics	Characteristics of local economy or companies

Lyu, *et. al.*(2009)은 <Table 3>과 같이 제시하였다.

Tiernery & Bruneau(2007)의 차원 구분은 사회 전반을 포괄하고 있기 때문에 사이버복원력의 차원을 설명하는 데에 무리가 없지만, Lyu, *et. al.*(2009)의 논의를 참고하여 선택한 시스템견고성, 자원동원성, 신속성, 적응성은 왜 기존 논의와 다른지 설명이 필요하다. Lyu, *et. al.*(2009)이 '여유'로 명명한 가외성은 만약 사이버침해 등으로 시스템이 작동을 멈출 경우 바로 대체할 수 있는 자원을 가리킨다. 즉, 시스템 문제와 대체 자원의 유무를 동시에 포괄하고 있는데, 사이버복원력에서는 보다 시스템과 인적 자원 문제가 구분되어야 한다고 보았다. 따라서 본 연구에서는 시스템 대체 요소와 인력 대체 요소를 구분하여 향후 사이버복원력의 정책적 순위를 탐구할 때 명확한 결과를 얻기 위하여 가외성을 제외하고, 시스템견고성과 자원동원성을 포함하였다. 또한 Lyu, *et. al.*(2009)이 정의한 사회 전체 복원력의 수준을 결정짓는 기술적, 조직적, 사회적, 경제적 역량을 '정부'라는 특정 조직단위에서의 복원력 영역인 기술·인력, 제도·거버넌스, 리더십과 인식, 예산

으로 재구성하였다. 이를 정리한 것이 다음 <Table 4>이다.

첫째, '시스템견고성'은 침해상황에서도 작동하는 시스템 역량을 가리킨다. 따라서 기술적으로는 강한 보안 시스템과 사이버침해를 예측할 수 있는 능력이 필요하며, 취약성 및 복원성 정의, 취약성 관리에 대한 법적 절차가 제도적으로 마련되어야 한다. 보안시스템 구축과 개선을 위한 투자는 사이버보안 정책을 담당하는 조직의 유무와 연결된다. 조직은 체계적으로 사이버복원력 관련 정책을 확대해 나가야 한다. 한편, 인증은 시스템견고성을 위한 제도정책에 포함된다. 그러나 국내 인증의 경우 장기간 특정 보안기술 기반인 공인인증서에만 지나치게 의존해왔다는 취약성이 있다. 특히 전자상거래 및 금융시장에서 간편 결제 및 핀테크가 점차 확산되고 있는 이 시점에서 공인인증서를 대체할 수 있는 범정부 차원의 다양한 인증보안 기술에 대한 투자와 개발 노력이 시급하다. 이 같은 맥락에서 마이핀, 아이핀 등의 대체 인증기술과 더불어 최근에는 다중요인인증(Multi Factor Authentication)등의 도입을 통한 사이버 침해 감소 및 사이버복원력 강화 방안이 모색되고 있다.

둘째, '자원동원성'은 보안 취약성 관리 및 이를 담당하는 사람들에 대한 역량이다. 따라서 보안기술을 갖고 있는 전문 인력이 중요하며, 이러한 보안 전문가를 양성 및 지원하기 위한 예산이 필요하다. 또한 보안 전문 인력의 자격, 의무 및 역할을 정의하여 효율적인 인력

Table 3. Aspects of resilience & their exemplifications

Aspects / Areas	Technology Aspect	Organization Aspect	Social Aspect	Economic Aspect
Robustness	New Structure, Code Unity, Remodeling	Comprehensiveness of Contingency Plans	Social Vulnerabilities, Index of Vulnerability	Extent of Economic Diversity
Redundancy	Possibility of technology replacement	Replacement Are for Disaster Management	Existence of Disaster Victims' choice	Capacity of replacing input elements or preserving elements
Resources	Presence of Resources for recovery and repair	Capacity for improvement, innovation, expansion	Capacity of corresponding human needs	Innovative Capacity
Rapidity	Time duration for recovery of system failure	Time duration for the initial recovery right after attack	Time spent for recovering houses and works	Time duration for recovering production or finances

Table 4. Dimensions and areas of cyber-resilience

area dimension	Technology	Governance	Insights	Finance
	Technology & HR	Institution · Governance	Leadership · Awareness	Budget
Robustness	The latest security system and capacity for sensing potential cyber risks	Making security system mandatory and providing clear cyber response procedures, role & responsibility & expanding the comprehensiveness of cyber resilience policies	Security Leadership and High Awareness of CSO in each organization	Security Incident Prevention System Building and Investment
Resourcefulness	Expertise of security Personnel for system recovery	Ensuring of security experts and necessary resources & institutionalizing cooperative network with related organizations	Raising the status of cyber security agencies and organizations	Increasing investment in security personnel's training and support
Rapidity	Time duration for the initial recovery right after attack	Consistent order and control from cyber risk control tower & providing manual for saving time. Fast information sharing and communication amongst related agencies and experts	Organization-level approach(not IT division approach) for cyber security and shared responsibilities amongst related agencies	Investment for rapid recovery <sup>13)</sup>
Adoptability	Objective evaluation of consequences of cyber attacks and applying the findings to security system and new technology development	Establishing institutions and organizational system for preparing for new threats and strengthening cyber resilience	Elevating the security awareness and sharing the necessity of cyber security among the public officials across the government	Investment for increasing system robustness, resources & rapidity

관리가 가능하도록 한다. 조직적으로는 이들의 혁신과 능력을 이끌어낼 수 있는 거버넌스 체계가 마련되어야 한다.

셋째, '신속성'은 가능한 빨리 정상 또는 원래 상태로 돌아가는 능력이다. 기술적으로는 최초복구까지 걸린 시간의 단축이 중요하며, 생산이나 예산을 복구하는 데 드는 시간의 단축도 수반되어야 한다. 조직적으로 신속성을 관리할 수 있는 '컨트롤 타워'가 필요하며, 제도적으로는 복구과정에 대한 절차나 매뉴얼로 시간을 단축할 수 있어야 한다.

넷째, '적응성'은 사이버침해를 극복하고, 침해의 경험으로부터 학습하고, 시스템건고성, 자원동원성, 신속성을 확장하는 능력이다. 기술적으로 더 나은 보안 시스템을 구축해야 하며, 이를 위한 새로운 수단과 기술 소개 및 투자가 필요하다. 신종 사이버침해에 대비하여 제도가 개선되어야 하며, 이에 따른 미래 위협에 대비하기 위한 조직체계를 마련해야 한다.

#### 4. 선행연구

기존 사이버보안 관련 연구는 법·제도 연구 및 기술 연구가 가장 많다. 법·제도는 국내 사이버보안 형태의 특이성을 다루고 있으며, 기술 연구는 이를 극복할 수 있는 새로운 기술적 대안에 대해 주로 논의한다.

법제도를 다룬 연구는 주로 국가적 추진체계와 법 개정 방향에 대한 내용을 담고 있다. Kim(2011)은 정보통신기반보호법, 정보통신망이용촉진 및 정보보호 등에 관한 법률 등 관련법을 다루는 주체가 위원회 조직인 것이 취약한 사이버보안 환경을 만들고 있다고 주장한다. 또한 해킹(5종류), 컴퓨터바이러스(3종류), 정보통신망 침입행위, 정보손괴행위(3종류), 정보변조행위, 정보유출행위(2종류) 등과 관련된 법안을 살펴봄으로써 사이버보안에도 형사정책적 대응방안이 아닌, 형사사법적 대응방안이 필요하다고 강조한다. Kwon(2011)은 사이버보안 관련 법제는 통신망의 안전성을 위한 내용으로는 볼 수 없으며, 사고 대응을 위한 조직체계 및 운영이 대통령 훈령(국가사이버안전관리규정)으로 되

13) 현재 ISO22301 내 재난 초동대응부터 전사적 업무복귀까지 전체 인증체계를 시행하고 있으며, 구체적으로 복구목표시간(Recovery Time Objective)과 복구목표시점(Recovery Point Objective)을 두고 있다.

어 있다는 한계를 지적하며, 2011년 발표한 국가 사이버안보 마스터플랜이 컨트롤타워 부재를 보완한 것은 바람직하지만, 법적 근거가 부족하다는 한계를 갖고 있다고 주장한다. 따라서 사이버보안 기본 법률을 제정하여 국가적 추진체계를 마련하고, 민간 보안전문가, 방송·통신사업자, 포털 사업자 등 관련 사업자를 반드시 포함시켜 제도와 현실의 괴리를 최대한 줄여야 한다고 강조한다. Oh & Seoung(2014)의 연구는 외국 사례를 비교하여 국경이 없는 사이버공간의 특성을 이해하여 2013년 발의된 법률의 허점을 보완해야 한다고 본다. 공공기관에만 적용되는 국가사이버안전관리규정 이외에 민간 기업이나 이용자에게도 적용되는 제도가 필요하고, 민주적인 감시와 견제 장치까지 확보된 기관이 법제도를 정비해야 한다고 보았다. Bae(2014)는 해외 사례 중 내각부와 함께 정보인증중앙기구, 사이버보안청, 민간비상대비사무처 등의 구조로 이루어진 영국의 사이버보안 전략을 소개하였다. 특히, 사이버범죄 억제, 사이버 공격에 대한 복원력 강화 및 권익 보호, 안정적인 사이버 공간 구현, 사이버보안 지식, 기술, 능력 구축 등과 같이 구체적인 목표를 두고 사이버보안 전략 계획(2013)을 세워 실행 중인 영국의 사례는 향후 국제기구 또는 외국과의 협력이 절실한 국내 사이버 보안 정책에도 시사하는 바가 크다. Bae, *et. al.*(2015)의 연구는 국가 사이버보안 평가를 위한 평가항목을 제시하고 있다. 사이버보안 관리 프로세스를 체계화하고 역량 강화를 목적으로 하는 사이버보안 역량 성숙도 모델(Capacity Maturity Model: CMM)을 이론으로 하여 미국 헤리티지 재단의 '2015 군사력지수', 유럽 소프트웨어 연합(The Software Alliance: BSA)의 '사이버보안 대시보드', 호주 전략정책연구소(Australian Strategic Policy Institute: ASPI)의 '아태지역 사이버 성숙도' 등의 평가 항목을 통해 국내 사이버보안 역량 평가항목을 제안하였다. 특히, 세부 평가항목 중 법제도는 사이버보안 기본법과 정보보호에 관한 법률의 수준 정도를 평가 항목으로 지정하여 사이버공간의 기본적인 신뢰 구축이 가능 여부에 중점을 두었다.

기술연구는 주로 현재 사이버보안 체계의 문제점을 해결할 방안을 제시하는 데 초점을 두고 있다. Choung & Bae(2014)는 해킹에 대비한 보안패치 설치 및 정보화 교육, 다중 정보보호를 위한 네트워크 보안요소 강화, 신규 보안 취약점에 대한 연구와 투자, 대응체계 정비, 전자정부 기본 인프라에 대한 지속적 투자 강화 등을 통해 보다 안전한 전자정부 보안대책의 필요성과 방안을 제시하고 있다. 그러나 기술연구의 한계는 널리 사용되고 있는 공인인증의 포괄성 등을 고려한 연구는 적다는 점이다. 기존 연구들이 대체로 사후약방문의 관점에서 보안문제에 접근하거나 보안의 대상을 실물(physical objects)에만 집중하고 있다. 즉, 공인인증의 장점을 살리면서도 인증 체계 안정성을 높이는 시각은 적어, 현실화하기에는 제약이 있는 것으로 나타났다.

### III. 연구방법: AHP조사

AHP조사는 계층분석적 의사결정방법으로 복잡한 의사결정 상황에서 경제적 이해득실과 같은 수치화가 가능한 정량적 요소 뿐 아니라 수량화가 어려운 정성적 요소를 측정할 수 있는 조사방법이며, 이를 통해 합리적이고 체계적인 결과 도출이 가능하다. AHP조사에 참여하는 이해 당사자 혹은 의사결정 참여자가 다수인 경우, 그룹의 의사를 도출할 수 있도록 지원하는 의사결정방법이다(Kang, 2015).

AHP조사의 핵심은 쌍대비교를 통한 우선순위 도출이다. 목표, 판단기준, 대안 등 여러 항목에 대해 1:1 쌍대비교를 진행하고, 각 응답자의 우선순위를 도출한다. 이 과정에서 각 응답은 자동적으로 논리적 일관성을 검증받고, 이에 따라 비일관적인 답변은 보정되어 결과의 객관성은 높아진다. AHP조사는 설계과정에서 많은 문제의식과 시각을 포용하기 때문에 지식을 자산화하여 측정하는 방법이 가능하고, 의사결정의 실행력을 높여준다는 장점이 있다.

2015년 5월 29일 민간 및 보안 실무자 5명, 정부 실

무자 3명, 학계 전문가 2명 등 총 10명의 전문가와 함께 1차 전문가 브레인스토밍을 진행하였고, 6월 30일부터 8월 3일까지 보안 및 ICT 전문가와 함께 총 세 차례 워크숍을 진행하였다. 학계 5명, 정부·공공기관 7명, 민간 5명 등 총 17명의 전문가가 참여하였으며, 방법론적으로 워크숍 내 현장 의견수렴과 웹 솔루션을 활용한 설문조사를 병행하였다.

이 과정을 통하여 취약성 및 복원력 정의와 선행연구 등을 참고하여 사이버취약성과 복원력, 인증 취약성과 복원력 등 총 4가지 분야를 구성하는 핵심 요소를 먼저 선정하였고, 전문가 의견을 참고하여 중요도와 일관성, 타당성 등을 검증하였다.

조사결과는 ‘배분방식(Distributive Mode)’을 활용한다. 배분방식은 비교대상의 가중치의 합이 1이 되도록 비교대상간 중요도의 상대적 비율에 따라 가중치(중요도)를 부여하는 방식으로, 비교 대상간 중요도를 도출하는 데 활용된다.

국내 인증보안 취약성 및 복원력 요소들 간 요인은 <Table 5>~<Table 8>과 같다.

Table 5. Cyber-security vulnerability factors

1 <sup>st</sup> Criteria	2 <sup>nd</sup> Criteria
Technology (HR)	Outdated Security Technology
	Shortage of Cyber Security Experts
Institution · Governance	Absence of Governance amongst security-related agencies
	Lack of legal responsibilities and penalty regulations for holding the agencies responsible for cyber incidents
	Low compatibility of security technology and system
Insight: Leadership · Awareness	Absence of awareness and understanding of government CSOs
	Low organizational status of cyber security division
	Lack of understanding the significance of cyber security across the government
Fiances	Limited investment on cyber-security due to uncertainty of investment effect
	Insufficiency of finance for post-event recovery, due to prevention-centered budget allocation

Table 6. Factors for enhancing cybersecurity

1 <sup>st</sup> Criteria	2 <sup>nd</sup> Criteria
Robustness	Applying the cutting-edge security technology
	Excluding the dependence of specific security technology
Resources	Training cyber security experts
	Raising the organizational status of cybersecurity agencies or divisions
	Increasing investment in cybersecurity
Rapidly	Balanced budget allocation between prevention at pre-event and recovery at post-event
	Building policy collaborations amongst security-related agencies
	Clarifying the legal responsibilities and roles of government cyber security agencies
Adoptability	Assuring government CSOs taking cyber-security as organizational strategy, not IT approach
	Maximizing the learning effect from cyber incident recovery & enhancing the security awareness of government officials

Table 7. Authentication vulnerability factors

1 <sup>st</sup> Criteria	2 <sup>nd</sup> Criteria
Technology (HR)	Potential risk of reproduction of authentication tools without permission
	All levels of authentication procedure is processed in a same terminal
	Check only password
	Dependence on a specific security means
Institution · Governance	Excessive demand of individual identification & use resident residential number for authentication key
	Uniformity of authentication tools via enforcement of a specific authentication mechanism
	Implementation of new authentication tools without legal readiness and deployment in relation to new technologies (e.g. Fintech)
Insight: Leadership · Awareness	Diversified electronic signature governance and thereby difficulties of implementing consistent policies
	Absence of government principles of issuing authentication tools and procedure
Insight: Leadership · Awareness	Lack of policy considerations of diverse authentication methods reflecting technology environment change
Fiances	Insufficient investment on electronic finance and payment

Table 8. Factors for enhancing authentication resilience

1 <sup>st</sup> Criteria	2 <sup>nd</sup> Criteria
Robustness	Applying additional technologies for preventing authentication replica
	Introducing diverse and multiple authentication tools (e.g. Tokens, MFA)
	Strengthening security via diversification of authentication elements
	Developing systems for figuring out users' intentions (e.g. Detecting system for impersonation)
Resources	Research and investment on current authentication security technology & alternative technologies that could replace the public key authentication
Rapidity	Two-tier or multi-tier electronic signature & consistent cyber security policy
	Enforcing service provider's responsibility for identifying the causes of cyber incidents
Adoptability	Disuse of resident registration number & apply legal rules to identification mechanisms
	Diversification of new alternative authentication technologies
	Change of legal system in tune with the introduction of new ways of authentication
	Government policy and technology leadership in relation to authentication security (e.g. CSO)

#### IV. 분석결과 및 논의

##### 1. 사이버보안 취약성

###### 1) 문항별 분석결과

1차 기준 4개의 범주에 대하여 전문가들은 ‘예산’(0.3009)을 가장 중요하게 생각하는 것으로 나타났으며, 이어서 ‘리더십·인식’(0.2926), ‘기술(인력)’(0.2232), ‘제도·거버넌스’(0.1834) 순으로 나타났다. ‘기술(인력)’의 세부항목 2개의 2차 기준에 대하여 전문가들은 ‘사이버보안 전문 인력 부족’(0.7521)을 가장 중요하게 생각하는 것으로 나타났으며, 이어서 ‘적시에 적용되지 못하는 보안기술’(0.2479) 순으로 나타났다. ‘제도·거버넌스’의 세부항목 3개의 2차 기준에 대하여 전문가들은 ‘사이버보안 유관기관 간 거버넌스 부재’(0.4723)를 가장 중요하게 생각하는 것으로 나타났으며, 이어서 ‘사이버침해 시 유관기관의 법적 책임 및 처벌규정 미흡’(0.3457), ‘호환성이 낮은 보안기술과

체계’(0.1820) 순으로 나타났다. ‘리더십·인식’ 세부항목 3개의 2차 기준에 대하여 전문가들은 ‘정부 사이버보안 담당 부처 최고관리자의 관심 및 이해 부족’(0.5247)을 가장 중요하게 생각하는 것으로 나타났으며, 이어서 ‘사이버보안 담당 부처 및 조직 위상 낮음’(0.2773), ‘법정부 공무원 차원에서의 사이버보안의 중요성 인식 부족’(0.1980) 순으로 나타났다. ‘예산’의 세부항목 2개의 2차 기준에 대하여 전문가들은 ‘사이버보안의 투자효과 불확실성으로 인한 최소한의 투자’(0.7077)를 가장 중요하게 생각하는 것으로 나타났으며, 이어서 ‘사전대비 중심의 예산 배정으로 인해 예측 탐지 및 복구와 같은 사후처리 예산 부족’(0.2923) 순으로 나타났다.

###### 2) 종합 상대적 중요도

사이버보안 취약성요인의 1차 기준 4개, 2차 기준 10개를 종합적으로 고려하여 종합중요도를 도출한 결과, 전문가들은 ‘사이버보안의 투자효과 불확실성으로 인한 최소한의 투자’(0.2129)를 가장 중요하게 생각하는 것으로 나타났다. 이어서 ‘사이버보안 전문 인력 부족’(0.1678), ‘정부 사이버보안 담당 부처 최고관리자의 관심 및 이해 부족’(0.1535) 순으로 나타났다. 반면, ‘호환성이 낮은 보안기술과 체계’(0.0334) 등은 상대적으로 덜 중요한 것으로 나타났다.

###### 3) 그룹별 비교

1차 평가기준의 4개 범주에 대하여 학계, 민간 기업, 정부·공공기관의 의견을 분석한 결과, 학계의 경우 ‘리더십·인식’(0.3830)을 가장 중요하게 생각하였고, 민간 기업은 ‘기술(인력)’(0.4098)을 가장 중요하게 고려하였다. 반면, 정부·공공기관의 경우 ‘예산’(0.3492)을 가장 중요하게 생각하였다. 가장 큰 중요도 차이를 보이는 기준은 ‘기술(인력)’이다. 민간은 0.4098로 가장 중요하다고 본 반면, 학계는 0.1483만큼 중요하게 생각하여 0.2615 만큼 차이가 발생하였다.

‘기술(인력)’ 하위 2차 평가기준 2개에 대하여 학계,

민간 기업, 정부·공공기관의 의견을 비교한 결과, 세 그룹의 평가기준에 대한 우선순위는 학계, 민간 기업, 정부·공공기관 모두 '사이버보안 전문 인력 부족'을 가장 중요하게 생각하였다. 학계, 민간 기업, 정부·공공기관 그룹 사이에는 0.0913 만큼의 중요도 차이가 나타났다.

'제도·거버넌스' 하위 2차 평가기준 3개에 대하여 학계, 민간 기업, 정부·공공기관의 의견을 비교한 결과, 학계, 민간 기업, 정부·공공기관 모두 '사이버보안 유관기관 간 거버넌스 부재'를 가장 중요하게 생각하는 것으로 나타났다. 가장 큰 중요도 차이를 보이는 기준은 '호환성이 낮은 보안기술과 체계'로 학계, 민간 기업, 정부·공공기관 그룹 사이에는 0.1046 만큼의 중요도 차이가 나타났다.

'리더십·인식' 하위 2차 평가기준 3개에 대하여 학계, 민간 기업, 정부·공공기관의 의견을 비교한 결과, 학계, 민간 기업, 정부·공공기관 모두 '정부 사이버보안 담당 부처 최고관리자의 관심 및 이해 부족'을 가장 중요하게 생각하였다. 가장 큰 중요도 차이를 보이는 기준은 '사이버보안 담당 부처 및 조직 위상 낮음'으로 학계, 민간 기업, 정부·공공기관 그룹 사이에는 0.2673만큼의 중요도 차이가 나타났다.

'예산' 하위 2차 평가기준 2개에 대하여 학계, 민간 기업, 정부·공공기관의 의견을 비교한 결과, 학계, 민간 기업, 정부·공공기관 모두 '사이버보안의 투자효과 불확실성으로 인한 최소한의 투자'를 가장 심각한 사이버보안 취약성으로 생각하였다. 학계, 민간 기업, 정부·공공기관 그룹 사이에는 0.2279의 중요도 차이가 나타났다.

## 2. 사이버보안 복원력

### 1) 문항별 분석결과

1차 기준 4개에 대하여 전문가들은 '신속성'(0.4363)을 가장 중요하게 생각하는 것으로 나타났으며, 이어서 '자원동원성'(0.2887), '시스템견고성'(0.1821), '적응성'(0.0929) 순으로 나타났다.

'시스템견고성'의 세부항목 2개의 2차 기준에 대하여 전문가들은 '최신보안기술 적용'(0.6133)을 가장 중요하게 생각하는 것으로 나타났으며, 이어서 '특정보안기술 종속성 배제'(0.3867) 순으로 나타났다. '자원동원성'의 세부항목 4개의 2차 기준에 대하여 전문가들은 '사이버보안에 대한 예산 투자 확대'(0.3113)를 가장 중요하게 생각하는 것으로 나타났으며, 이어서 '사이버보안 담당 부처 및 조직의 위상 제고'(0.2721), '사이버보안 전문 인력 양성'(0.2264) '사전대비와 사후처리의 균형 있는 예산 배정'(0.1902) 순으로 나타났다. '신속성'의 세부항목 3개의 2차 기준에 대하여 전문가들은 '부처 최고관리자가 보안을 IT기술접근이 아닌 조직차원의 전략적 접근'(0.3847)을 복원력 강화의 가장 중요한 요인으로 생각하는 것으로 나타났으며, 이어서 '유관기관의 법적 책임과 역할 명확화'(0.3495), '유관기관 간 정책 협력체계 구축'(0.2659) 순으로 나타났다.

### 2) 종합 상대적 중요도

사이버보안 복원력 제고 정책 우선순위 선정을 위해 1차 기준 4개, 2차 기준 10개를 종합적으로 고려하여 종합중요도를 도출한 결과, 전문가들은 '부처 최고관리자가 보안을 IT기술접근이 아닌 조직차원의 전략적 접근'(0.1678)을 가장 중요하게 생각하는 것으로 나타났으며, 이어서 '유관기관의 법적 책임과 역할 명확화'(0.1525), '유관기관 간 정책 협력체계 구축'(0.1160), '최신보안기술 적용'(0.1117) 순으로 나타났다.

### 3) 그룹별 비교

1차 4개의 평가기준에 대하여 학계, 민간 기업, 정부·공공기관의 의견을 비교한 결과, 학계와 민간 기업의 경우 사이버보안 침해사고 대응의 시스템 자체 복구에 필요한 '신속성'(0.5008, 0.4866)을 복원력 강화의 가장 중요한 요인으로 응답한 반면, 정부·공공기관의 경우 복구 작업에 필요한 인적·물적 자원 및 협력과 같은 '자원동원성'(0.4077)을 가장 중요하게 생각하였다. 가장 큰 중요도 차이를 보이는 기준은 '자원동원성'으로

정부·공공기관은 0.4077로 가장 중요하게 생각한 한편, 학계는 0.1959만큼 중요하게 생각하여 0.2118의 중요도 차이가 나타났다.

‘시스템견고성’ 하위 2차 평가기준 2개에 대하여 학계, 민간 기업, 정부·공공기관의 의견을 비교한 결과, 학계는 공인인증서와 같은 ‘특정보안기술 종속성 배제’(0.5495)를 가장 중요하게 생각한 반면, 민간 기업, 정부·공공기관은 ‘최신보안기술 적용’을 가장 중요하게 생각하였다. 또한 학계, 민간 기업, 정부·공공기관 그룹 사이에는 0.2738만큼 중요도 차이가 있었다.

‘자원동원성’ 하위 2차 평가기준 4개에 대하여 학계, 민간 기업, 정부·공공기관의 의견을 비교한 결과, 학계는 ‘사이버보안 담당 부처 및 조직의 위상 제고’(0.3471)를 가장 중요하게 생각한 반면, 민간 기업, 정부·공공기관은 ‘사이버보안에 대한 예산 투자 확대’를 가장 중요하게 생각하였다. 가장 큰 중요도 차이를 보이는 기준은 ‘사이버보안에 대한 예산 투자 확대’로 민간 기업은 0.3606으로 가장 중요하게 생각한 반면 학계는 0.2266만큼 중요하게 생각하여 0.1340만큼의 중요도 차이가 나타났다.

‘신속성’ 하위 2차 평가기준 3개에 대하여 학계, 민간 기업, 정부·공공기관의 의견을 비교한 결과, 학계와 정부·공공기관은 ‘부처 최고관리자가 보안을 IT기술 접근이 아닌 조직차원의 전략적 접근으로 취급’을 가장 중요하게 생각한 반면, 민간 기업은 ‘유관기관의 법적 책임과 역할 명확화’(0.5366)를 가장 중요하게 생각하였다. 가장 큰 중요도 차이를 보이는 기준은 ‘부처 최고관리자가 보안을 IT기술접근이 아닌 조직차원의 전략적 접근’으로 학계는 0.5838로 가장 중요하게 생각한 반면 민간 기업은 0.2193만큼 중요하게 생각하여 0.3645의 중요도 차이가 나타났다.

적응성의 경우 ‘범정부 공무원들의 보안인식’ 및 형태변화 단일항목만 포함하고 있어 비교 내용이 없다.

### 3. 인증 취약성

#### 1) 문항별 분석결과

인증취약성 평가 1차 기준 4개에 대하여 전문가들은 ‘제도·거버넌스’(0.3151)를 가장 중요하게 생각하는 것으로 나타났으며, 이어서 ‘기술(인력)’(0.2792), ‘리더십·인식’(0.2198), ‘예산’(0.1859) 순으로 나타났다.

‘기술(인력)’의 세부항목 4개의 2차 기준에 대하여 전문가들은 ‘인증수단의 무단 복제 사용 가능’(0.3558)을 가장 심각한 취약요인으로 생각하는 것으로 나타났으며, 이어서 ‘특정 보안 수단에만 의존’(0.3026), ‘인증단계가 모두 한 단말기에서 처리’(0.1821), ‘비밀번호 일치 여부만 확인’(0.1594) 순으로 나타났다. ‘제도·거버넌스’의 세부항목 5개의 2차 기준에 대하여 전문가들은 ‘과도한 개인인증 요구 및 주민등록번호를 인증키로 활용’(0.3315)을 가장 심각한 취약요인으로 인식했으며, 이어서 ‘특정 인증수단의 강제화로 인한 인증수단의 획일성’(0.2603), ‘법제도적 보완 및 준비 없이 사용되는 인증방식(예: 핀테크, 간편결제)’(0.1419), ‘분산된 전자서명 거버넌스 체계 및 일관된 정책추진 어려움’(0.1400), ‘법정부 차원에서의 인증수단 발급 및 이용절차의 원칙 부재’(0.1263) 순으로 나타났다.

#### 2) 종합 상대적 중요도

인증 취약성 요인 우선순위 선정을 위해 1차 기준 4개, 2차 기준 11개를 종합적으로 고려하여 종합중요도를 도출한 결과, 전문가들은 ‘외부환경 변화를 반영한 다양한 인증방식 인지 및 정책적 고민 미흡’(0.2198)을 가장 심각한 인증 취약요인으로 생각하는 것으로 나타났으며, 이어서 ‘전자금융 및 전자결제에서의 인증보안 투자 미흡’(0.1859), ‘과도한 개인인증 요구 및 주민등록번호를 인증키로 활용’(0.1044) 순으로 나타났다.

#### 3) 그룹별 비교

인증취약성 1차 4개 평가기준에 대하여 학계, 민간 기업, 정부·공공기관의 의견을 비교한 결과, 학계, 민간 기업, 정부·공공기관 모두 ‘제도·거버넌스’를 가

장 중요하게 생각하였다. 가장 큰 중요도 차이를 보이는 기준은 ‘예산’으로, 정부·공공기관은 0.2191 만큼 중요하게 생각했고, 학계는 0.1504 만큼 중요하게 생각하여 0.0687 만큼의 중요도 차이가 나타났다.

‘기술(인력)’ 하위 2차 평가기준 4개에 대하여 학계, 민간 기업, 정부·공공기관의 의견을 비교한 결과, 학계와 민간 기업은 ‘인증수단의 무단 복제 사용 가능’을 가장 심각하게 생각한 반면, 정부·공공기관은 ‘특정 보안 수단에만 의존’(0.3517)을 가장 심각한 문제로 생각하였다. 가장 큰 중요도 차이를 보이는 기준은 ‘인증수단의 무단 복제 사용 가능’로 민간 기업은 0.3996으로 가장 중요하게 생각한 반면, 정부·공공기관은 0.3506 만큼 중요하게 생각하여 0.0865 만큼의 중요도 차이가 나타났다.

‘제도·거버넌스’ 하위 2차 평가기준 5개에 대하여 학계, 민간 기업, 정부·공공기관의 의견을 비교한 결과, 학계와 정부·공공기관은 ‘과도한 개인인증 요구 및 주민등록번호를 인증키로 활용’을 가장 심각하게 생각한 반면, 민간 기업은 ‘특정 인증수단의 강제화로 인한 인증수단의 획일성’(0.3437)을 가장 심각한 인증 취약성으로 생각하였다. 가장 큰 중요도 차이를 보이는 기준은 ‘과도한 개인인증 요구 및 주민등록번호를 인증키로 활용’으로 정부·공공기관은 0.4087로 가장 심각한 결핍도로 생각한 반면 민간 기업은 0.2146 만큼 중요하게 생각하여 0.1940 만큼의 중요도 차이가 나타났다.

#### 4. 인증 복원력

##### 1) 문항별 분석결과

인증복원력 제고 요인 평가 1차 기준 4개 항목에 대하여 전문가들은 ‘시스템견고성’(0.3755)을 가장 중요하게 생각하는 것으로 나타났으며, 이어서 ‘적응성’(0.2470), ‘자원동원성’(0.1888), ‘신속성’(0.1887) 순으로 나타났다. ‘시스템견고성’의 세부항목 4개의 2차 기준에 대하여 전문가들은 ‘다양한 인증기술 개발 및 적용(예: 토큰화, MFA)’(0.3289)을 가장 중요하게 생

각하는 것으로 나타났으며, 이어서 ‘인증요소 다양화를 통한 보안강화’(0.2813), ‘인증수단 복제 방지 기술 추가 적용’(0.1995), ‘사용자 의도 파악 시스템 개발(예: 도용탐지시스템)’(0.1903) 순으로 나타났다. ‘신속성’의 세부항목 2개의 2차 기준에 대하여 전문가들은 ‘서비스제공자의 원인규명 및 책임확보’(0.6533)를 가장 중요하게 생각하는 것으로 나타났으며, 이어서 ‘이원·다원화된 전자서명충위 및 일관된 정책추진’(0.3467) 순으로 나타났다. ‘적응성’ 하위 세부항목 4개의 2차 기준에 대하여 전문가들은 ‘새로운 인증방식 기술의 다양화’(0.3148)를 가장 중요하게 생각하는 것으로 나타났으며, 이어서 ‘범정부 차원의 인증보안에 대한 정책·기술적 리더십(예: CSO)’(0.2343), ‘새로운 인증방식에 대한 법제도 개선’(0.2311), ‘주민번호 사용 폐지 및 본인확인수단에 대한 법치원리 반영’(0.2198) 순으로 선호도가 나타났다.

##### 2) 종합 상대적 중요도

인증 복원력 정책 우선순위 선정을 위해 1차 기준 4개, 2차 기준 11개를 종합적으로 고려하여 종합중요도를 도출해본 결과, 전문가들은 ‘현 인증보안 취약성 연구 및 공인인증서 대체기술 개발에 대한 예산투자 필요’(0.1888)를 가장 중요하게 생각하는 것으로 나타났으며, 이어서 ‘다양한 인증기술 개발 및 적용(예: 토큰화, MFA)’(0.1235), ‘서비스제공자의 원인규명 및 책임확보’(0.1233), ‘인증요소 다양화를 통한 보안강화’(0.1056) 순으로 나타났다.

##### 3) 그룹별 비교

인증복원력 1차 4개 평가기준에 대하여 학계, 민간 기업, 정부·공공기관의 의견을 비교한 결과, 학계, 민간 기업, 정부·공공기관 모두 ‘시스템견고성’을 가장 중요하게 생각하였다. 가장 큰 중요도 차이를 보이는 기준은 ‘시스템견고성’으로 학계는 0.4186만큼 중요하게 생각하고, 정부·공공기관은 0.3485만큼 중요하게 생각하여 0.0701만큼의 중요도 차이가 나타났다.

‘시스템견고성’ 하위 2차 평가기준 4개에 대하여 학계, 민간 기업, 정부·공공기관의 의견을 비교한 결과, 학계, 민간 기업, 정부·공공기관 모두 ‘다양한 인증기술 개발 및 적용(예: 토큰화, MFA)’을 가장 중요하게 생각하였다. 가장 큰 중요도 차이를 보이는 기준은 ‘인증수단 복제 방지 기술 추가 적용’으로 정부·공공기관은 0.2414 만큼 중요하게 생각하고, 민간 기업은 0.1445 만큼 중요하게 생각하여 0.0970 만큼의 중요도 차이가 나타났다.

‘신속성’ 하위 2차 평가기준 2개에 대하여 학계, 민간 기업, 정부·공공기관의 의견을 비교한 결과, 학계, 민간 기업, 정부·공공기관 모두 ‘서비스제공자의 원인규명 및 책임확보’를 가장 중요하게 생각하였다. 학계, 민간 기업, 정부·공공기관 그룹 사이에는 0.1023 만큼의 중요도 차이가 나타났다.

‘적응성’ 하위 2차 평가기준 4개에 대하여 학계, 민간

기업, 정부·공공기관의 의견을 비교해본 결과, 학계는 ‘새로운 인증방식에 대한 법제도 개선’(0.3168)을 가장 중요하게 생각한 반면, 민간 기업, 정부·공공기관은 ‘새로운 인증방식 기술의 다양화’를 가장 중요하게 생각하였다. 가장 큰 중요도 차이를 보이는 기준은 ‘새로운 인증방식에 대한 법제도 개선’으로 학계는 0.3168 로 가장 중요하게 생각한 반면, 민간 기업은 0.1800 만큼 중요하게 생각하여 0.1368 만큼의 중요도 차이가 나타났다.

## V. 결론

### 1. 조사결과

17명의 민간, 정부, 학계 전문가를 대상으로 국내 사이버보안 및 인증 취약성과 복원력에 대한 세 차례 AHP 조사 결과는 <Table 9> 및 <Table 10>과 같다.

Table 9. Synthesized significances according to categories (1)

Criteria		Rank	Cybersecurity Vulnerability	Authentication Vulnerability
1st Criteria		1st	Finance	Institution · Governance
		2nd	Insight: Leadership & Awareness	Technology(HR)
		3rd	Technology(HR)	Insight: Leadership & Awareness
2nd Criteria	Tech	1st	Shortage of Cyber Security Experts	Potential risk of reproduction of authentication tools without permission
		2nd	Outdated Security Technology	Over-dependence on a specific security means
		3rd	※N/A (No sub-criteria)	All levels of authentication processed in a same terminal.
	Institution · Governance	1st	Absence of governance amongst security responsible agencies	Excessive demand of identification & overuse of residential number as an authentication key
		2nd	Lack of legal responsibilities and penalty regulations for holding the agencies responsible for cyber incidents	Uniformity of authentication tools via enforcement of a specific authentication mechanism
		3rd	Low compatibility of security technology and system	Implementation of new authentications tools without legal readiness and deployment
	Insights	1st	Absence of government CSO's awareness and understanding of cyber security	Lack of policy considerations of diverse authentication methods reflecting technological changes
		2nd	Low organizational status of cyber security divisions	
		3rd	Lack of understanding the significance of cyber security across the government	
	Finance	1st	Limited investment on cybersecurity due to uncertainty of investment effect	Insufficient investment on electronic finance and payment
		2nd	Insufficient finance for post-event recovery due to prevention-centered budget allocation	
		3rd	N/A	

Table 10. Synthesized significances according to categories (2)

Criteria		Rank	Cybersecurity Resilience	Authentication Resilience
1st Criteria		1st	Rapidity	Robustness
		2nd	Resources	Adoptability
		3rd	Robustness	Resources
2nd Criteria	Robustness	1st	Applying the cutting-edge security technology	Introducing diverse and multiple authentication tools
		2nd	Excluding the dependence of specific security technology	Strengthening security via diversification of authentication elements
		3rd	N/A	Applying additional technologies for preventing authentication replica
	Resources	1st	Increasing investment in cyber-security	Research and investment on current authentication security technology & alternative technologies that could replace the public key authentication
		2nd	Raising the organizational status of cyber-security agencies or divisions	
		3rd	Training cyber security experts	
	Rapidity	1st	Assuring government CSOs taking cyber-security as organizational strategy	Enforcing service providers' legal responsibility for identifying the causes of cyber incidents
		2nd	Clarifying the legal responsibilities and roles of government cyber-security agencies	Two-tier or multi-tier electronic signature & consistent cyber security policy
		3rd	Building policy collaboration amongst agencies responsible for cyber-security	N/A
	Adoptability	1st	Maximizing the learning effect from cyber incident recovery & enhancing the security awareness of government officials	Diversification of new alternative authentication technologies
				Government policy and technology leadership in relation to authentication security
				Change of legal system in tune with the introduction of new ways of authentication

우선 사이버보안 취약성 결과를 보면, ‘사이버보안 취약성’ 요인 우선순위 선정을 위한 1차 기준의 경우, 상대적 중요도는 ‘예산’(0.3009)의 상대적 중요도가 가장 높았으며, 이어서 ‘리더십·인식’(0.2926), ‘기술(인력)’(0.2232), ‘제도·거버넌스’(0.1834) 순으로 나타났다. 즉, 기술이나 제도보다 사이버보안에 대한 예산 확보가 최우선적으로 해결해야 할 과제였다. 사이버보안 취약성에 대해 가장 요구되는 우선과제는 1) 사이버보안 예산 확보, 2) 사이버보안 자체의 중요성을 인지하고 인식변화를 촉구하는 것이다. 즉, 투자와 인식을 모두 고려한 답변이라 할 수 있다.

또한 사이버보안 취약성 요인 종합중요도를 도출한 결과, 전문가들은 ‘사이버보안의 투자효과 불확실성’으로 인한 최소한의 투자’(0.2129)를 심각한 문제로 생각하고 있었으며, 이어서 ‘사이버보안 전문 인력 부족’(0.1678), ‘정부 사이버보안 담당 부처 최고관리자의

관심 및 이해 부족’(0.1535) 순으로 나타났다. 또한 상대적 중요도 측정 결과, 1순위와 3순위 모두 사이버보안 관련 리더십 및 인식 제고에 관련된 것이었으며, 사이버보안 전문인력 부족 역시 정책적 장려를 필요로 하고 있음을 알 수 있다. 상대적 중요도를 공통적으로 고려했을 때, 사이버보안의 투자효과 불확실성으로 인한 최소한의 투자와 사이버보안 전문 인력 부족이 정책적 우선순위 상위권을 차지한 것 역시 투자와 인식 개선이 시급하다는 의견을 반영하고 있다. 또한 예산이 부족하면 인력 수급이 어렵다는 점도 예산과 리더십·인식의 높은 응답률을 대변한다.

사이버보안 복원력 정책 우선순위 검증 결과, 첫째, 1차 기준 중에서는 ‘신속성’(0.4363)이 가장 높게 나타났다. 이어서 ‘자원동원성’(0.2887), ‘시스템견고성’(0.1821), ‘적응성’(0.0929) 순으로 나타났다. 둘째, 전문가들은 ‘부처 최고관리자가 보안을 IT기술접근이

아닌 조직차원에서 전략적으로 접근하는 것'(0.1678)을 가장 중요하게 생각하는 것으로 나타났으며, 이는 전체 종합 순위에서도 1순위를 기록하였다. 이어서 '유관기관의 법적 책임과 역할 명확화'(0.1525), '유관기관 간 정책 협력체계 구축'(0.1160), '최신보안기술 적용'(0.1117) 순으로 나타났다. 종합 상대적 중요도 상위 3개는 모두 신속성으로, 사이버보안 복원력을 제고하기 위한 가장 시급한 사항은 신속성 강화인 것으로 밝혀졌다. 사이버보안 취약성과 마찬가지로 사이버보안 담당인력의 인식 문제가 복원력에 가장 필요한 요소로 지적되었다. 셋째, 민간과 학계 전문가 모두 '신속성'을 사이버보안 복원력에 가장 필요한 차원이라 보았다. 위에서 보았듯, 종합중요도 상위권 3개 모두 신속성의 하위 항목인 것으로 나타나 많은 전문가들이 신속성 향상을 가장 중요하게 고려하고 있음을 알 수 있었다. 이와 같은 결과는 사이버보안 유관기관 간 정보와 기술 공유가 원활히 진행될 수 있도록 협력적 체계가 구성되어야 한다는 사실을 의미한다. 또한 사이버보안에 대한 현재의 기술적 시각(technological approach)을 보다 조직차원(organizational approach)의 전략으로 확대할 필요성이 있다. 단순한 IT접근이 아니라 사이버보안 복원력을 향상하는 여러 가지 정책을 최고관리자의 지휘 아래 조직·기관 차원에서 접근해야함을 의미한다.

인증취약성의 1차 기준에서는 '제도·거버넌스'(0.3151)를 가장 중요하게 생각하는 것으로 나타났으며, 이어서 '기술(인력)'(0.2792), '리더십·인식'(0.2198), '예산'(0.1859) 순으로 나타났다. '인증 취약성' 종합중요도를 도출한 결과, 전문가들은 '외부환경 변화를 반영한 다양한 인증방식 인지 및 정책적 고민 미흡'(0.2198)을 가장 중요하게 생각하는 것으로 나타났다. 이는 현재 인증 보안과 관련해 책임운영기관이 이원화되어 일관된 정책 추진이 어려운 현실을 반영한 것으로 풀이된다. 그러나 차원과 세부 항목의 중요도 간에는 차이를 보였다. 인증 관련 즉각적 정책 및 법제도적 변화가 요구되고 있다는 점에서 제도·거버넌스의 응답이 집중된 것이라 짐작된다. 이와 같이 제도·거버

넌스가 인증 취약성에 즉시 대처하기 위해서는 여러 가지 인증 방법에 대한 발빠른 연구와 이를 정책에 어떻게 반영할 것인지와 같은 선행 작업이 필요하다. 이는 리더십·인식과 예산이 동시에 필요한 부분이므로 실질적으로 제도·거버넌스가 변화하기 위해서는 이 두 가지 차원에 해당하는 2차 기준이 만족되어야 할 것이다. 이처럼 취약성 관련한 예산의 문제는 사이버보안 취약성에서도 찾아볼 수 있다. 최소한의 투자가 사이버보안 취약성을 초래한다고 지적된 것처럼 취약성은 예산과 직접적인 연관성을 갖고 있는 것으로 해석할 수 있다.

인증 복원력 1차 기준 4개 영역에 대하여 전문가들은 '시스템견고성'(0.3755)을 가장 중요하게 생각하는 것으로 나타났다. 개별 보안시스템 자체의 견고성이 필요하다고 본 것이다. 종합 상대적 중요도에서는 자원동원성의 '현 인증보안 취약성 연구 및 공인인증서 대체기술 개발에 대한 예산 투자 필요'(0.1888)가 1순위를 차지하였으며, 시스템견고성의 '다양한 인증기술 개발 및 적용'(0.1235)이 2순위를 차지하였다. 인증 취약성과 마찬가지로 인증 복원력에서도 1차 기준과 종합 상대적 중요도에서 차이가 났다. 이는 시스템견고성을 위해서는 최신보안기술 도입과 적용이 필요하고, 전문인력이 뒷받침되어야 한다는 사실을 의미하며, 1차적으로 예산 확보가 선행되어야 하는, 마치 '닭과 달걀'의 관계처럼 얽혀있는 부분이다.

그룹별로 1차 기준은 사이버보안 복원력이 신속성에 집중되었던 것과는 달리, 인증 복원력은 자원동원성, 시스템견고성, 신속성 등에 골고루 분포되었다. 이는 인증 복원력이 시스템과 기술 등 보안기술에 더욱 집중되는 경향이 있음을 의미한다. 일반적으로 사이버보안 복원력은 다소 포괄적이고 추상적인 개념으로 이해되지만, 인증 복원력은 빈번하게 발생하는 인증 사고 때문에 이해도가 높다. 때문에 인증 복원력은 사이버보안력보다 단기적인 정책적 우선순위를 선호하는 것으로 해석할 수 있다. 특히, 대체기술 개발에 대한 예산 투자와 인증기술 개발 및 적용은 '현 인증기술을 뛰어넘는 새로운 기술'과 '기술의 적용'을 포함한다. 즉, 인증 관

런 시스템 자체를 견고하게 만들어야 한다는데 의견이 모아졌다고 해석할 수 있다. 즉, 인증 복원력과 관련된 정책 우선순위는 사이버보안 복원력 보다 미시적으로 이해되며, 비록 학계, 민간기업, 정부·공공기관 간 두드러지는 차이가 있었으나 다른 차원과 비교했을 때 보안 자체의 안전성, 견고성 등이 가장 높게 나타났다는 사실 역시 이를 뒷받침한다.

AHP 조사 결과의 항목 간 상대적 중요도 종합 결과는 <Table 11>과 같다.

## 2. 시사점

우선 사이버보안 취약성에 관한 요인의 AHP 조사 결과에 의하면, 종합중요도 및 우선순위에서 예산과 리더십·인식, 인력 요인이 공통적으로 강조되고 있다. 즉, 현행 사이버보안 정책에서 가장 큰 문제점은 투자 대비 효과가 불확실하다는 이유로 ‘사후약방문’식의 최소한의 투자만 이루어지고 있다는 점, 이에 따라 사이버보안 전문 인력이 부족하다는 점이다. 그리고 이는 근본적으로 급변하고 있는 ICT 융합 환경에 대한 정부 관계자들 및 정부부처의 관심과 이해 수준이 낮기 때문으로 추정된다.

따라서 이러한 문제점을 극복하기 위하여 단기적으로는 사이버보안 환경에 대해 범정부 차원에서 과감한 예산투자를 시행하는 것이 필요하다. 예컨대 새로운 사

이버보안 취약성에 대한 지속적인 연구와 대응을 위하여 산학연 공동연구센터를 설립하는 방법이나 담당 공무원을 대상으로 보안인식 향상을 위한 정기교육을 실시하는 방안, 최고보안책임자 제도를 도입해 정책적, 기술적 리더십을 제고하는 방안 등이 있을 것이다.

한편 장기적이고 지속가능한 예방책을 마련하기 위해 AHP 조사의 사이버보안 복원력 부문의 조사 결과를 참고해야 할 것이다. 해당 부문에서 전문가들은 지엽적인 기술적 접근법에서 나아가 명확한 책임소재 하에서 신속하고 조직적인 유관기관 협력체계의 대응이 필요함을 공통적으로 지적하고 있다. 즉, AHP 조사결과의 종합 중요도 순위를 보면 ‘부처 최고관리자가 보안을 IT 기술접근이 아닌 조직차원의 전략적 접근’(0.1678), ‘유관기관의 법적 책임과 역할 명확화’(0.1525), ‘유관기관 간 정책 협력체계 구축’(0.116) 등의 사이버보안 복원력의 신속성 항목들이 각각 1위~3위로 우선적으로 강조되었다. 이는 현행 사이버보안의 취약성 중 인력 및 리더십 요인과 연결되는 부분이라 할 수 있다.

이러한 경향성은 인증보안 취약성 부문에서도 나타난다. 인증보안 취약성에 관한 요인의 AHP 조사 결과를 보면, 사이버보안 취약성에서와 마찬가지로 인력과 리더십 및 예산의 문제가 우선과제로 지적되고 있다. 표면적으로는 과도한 개인인증을 요구하는 행태나 주민등록번호를 인증키로 활용하는 방법들이 기술과 인

Table 11. Synthesized comparative significance according to criteria

Significance / Rank	Cybersecurity Vulnerability	Cyber Resilience	Authentication Vulnerability	Authentication Resilience
significance	1st Limited investment on cybersecurity due to uncertainty of investment effect (Finance)	Assuring government CSOs taking cybersecurity as an organizational strategy	Lack of policy considerations of diverse authentication methods reflecting technological change (Leadership & awareness)	Research and investment on current authentication security technology & alternative technologies that could replace the public key authentication (resources)
	2nd Shortage of Cyber Security Experts(Technology & HR)	Clarifying the legal responsibilities and roles of government cyber-security agencies (Rapidity)	Insufficient investment on electronic finance and payment (Finance)	Introducing diverse and multiple authentication tools (Robustness)
	3rd Absence of awareness and understanding of government CSOs (Leadership and awareness)	Building cooperative governance amongst agencies responsible for cyber-security(Rapidity)	Excessive demand of user identification & overuse of residential number as authentication tool (Institution · governance)	Ensuring service providers' responsibility for identifying the causes of cyber incidents (Rapidity)

력의 문제로 지적되고 있지만 실상 근본적으로 이러한 문제들은 외부의 보안환경변화에 빠르게 적응하기 위한 정책적 고민이 부족한 것에서 비롯되며(외부환경 변화를 반영한 다양한 인증방식 인지 및 정책적 고민 미흡, 0.2198), 그에 따른 투자부족(전자금융 및 전자결제에서의 인증보안 투자 미흡, 0.1859)으로 인해 발생한다는 것이다. 결국 이러한 인증 취약성을 개선하고 인증복원력을 향상시키기 위해서는 현재의 인증서를 대체할 수 있는 다양하고 새로운 기술을 개발하는 노력이 필요하다. 동시에 복원력의 자원동원력을 향상시키기 위해 제한적인 투자 관행을 지양하고 사전대비와 사후처리가 모두 가능하도록 과감한 예산투자가 요구된다.

AHP조사의 진행내용상 여러 한계가 있다. 1단계 항목에는 큰 문제가 없으나, 2단계 항목에서 항목이 1개에 불과한 것은 상대가중치가 왜곡될 가능성이 있다. 또한 여건 상 제약으로 모델을 수정하고 판단을 심도 있게 재검토하는 기회를 1인당 한 번으로 제한하였다. AHP 모델 구축을 위한 워크숍 1회와 AHP 평가 워크숍 3회를 실시하였지만, 판단 기준들의 트레이드오프(trade-off)관계를 점검하는 등과 같은 정밀성은 다소 부족하였다. 이는 후속 연구에서 보완해야 할 것으로 보인다.

마지막으로 AHP분석을 통해 도출된 결과는 불변한 것이 아님을 인식할 필요가 있다. 정책 우선순위 변화나 새로운 상황 발생 등 모델 재구성과 새로운 분석이 필요할 경우, 현실을 반영하여 수정될 가능성이 있다.

## 감사의 글

본 논문은 한국행정연구원에서 생산된 자료를 활용하였으며, 한국행정연구원 연구자료관리규칙에 의거 사용허가를 받았음.

## References

- Ahn, Jong Ha. 2013. A Research of Policy Plan for Korea Cyber Security Response System. *Korean Police Studies Review*. 12(3): 125-146.
- Ahn, Jeong Cheol and Hyuk Jin Kwon. 2012. The Development Prospect of Security Strategy Regarding the Types of Cyberwar and Information Technology. *Review of Korean Society for Internet Information*. 13(4): 32-38.
- Bae, Beong Whan. 2014. UK Cybersecurity Strategy Analysis and Implications: Focus on National Cybersecurity Strategy Plan and Its Outcomes. *Institute for Information & Communications Technology Promotion*. 1-14.
- Bae, Sun Ha, Sang Don Park, and So Jeong Kim. 2015. A Study on the Development for the National Cybersecurity Capability Assessment Criteria. *The Korea Institute of Information Security and Cryptology*. 25(5): 1293-1314.
- Bruneau, M., S. Chang, R. Eguchi, G. Lee, T. O'Rourke, A. Reinhorn, M. Shinozuka, K. Tierney, W. Wallace, and D. Von Winterfeldt. 2003. A Framework to Quantitatively Assess and Enhance Seismic Resilience of Communities. *Earthquake Spectra*. 19(4): 733-752.
- Cho, Ho Dae and Dong Il Shin. 2009. Countermeasure by Cyber Infringement Accident Present Condition Analysis of Public and Private Section. *The Korea Contents Society*. 9(1): 331-338.
- Choung, Wan. 2001. A Study on Encryption Policy against Cybercrime. *Korean Institute of Criminology*. 7-131.
- Choung, Young Chul and Yong Guen Bae. 2014. Study on Security Measures of e-Gov with Dynamic ICT Ecosystem. *Journal of Information and Communication Convergence Engineering*. 18(6): 1249-1254.
- Ernst and Young. 2014. Achieving Resilience in the Cyber Ecosystem. *Insight on Governance, Risk and Compliance*. 2014(12): 1-13.
- Gallaher, H., W. MaMahon, and R. Morrow. 2014. Cyber Security: Protecting the Resilience of Canada's Financial System. *Bank of Canada Financed System Review*. 47-53.
- Gay, Gale Horton. 2011. Vulnerabilities in Cyber Security Mean

- Opportunities Too. *U.S. Bank Engineer & Information Technology*. 35(4): 68.
- George, A. Wright and Terrye N. Schaetzel. 2013. *Cyber Security: Designing and Maintaining Resilience*. Georgia Tech Research Institute, Cyber Technology and Information Security Laboratory. 1-14.
- Homeland Security. 2011. *Common Cybersecurity Vulnerabilities in Industrial Control Systems*. 1-88.
- Im, Chae Tae. 2012. The Current Trend of Cyber-attacks and Responses. *Korea Society of IT Services*. 204-222.
- Insights on governance, risk and compliance. (2014.12): 1-13.
- Kang, Hyun Soo. 2014. For the Proper Use of AHP Methods. *The Korea Institute of Public Administration Research Forum*. 64-70.
- Kang, Sang Joon, Sung Han Cho, and Soon Young Hong. 2013. *A Policy Implication for Community Resilience from Natural Disaster*. Gyeonggi Research Institute. 1-102.
- Kim, Seong Cheon. 2011. *Cyber Security Law*. 13(3): 311-336.
- Korea Communications Commission. 2011. *A Study on Solutions for the Advancement of Security Legislation*. 1-386.
- Kwon, Chang Beom. 2011. Management System for a National Cyber Security Review and Development. *Yonsei Journal of Medical and Science Technology Law*. 2(2): 59-80.
- Lee, Jeong Hyun. 2013. Public Authentication Use and Issues in Smart Environment. *Internet & Security Focus*. 2013(3): 23-53.
- Lee, Ki Shik 2008. A Study on Cognition Pattern of Cyber Security and Policy Alternatives in the Internet Age; Based upon Media-Human-Institution-Culture Perspective. *The Journal of Korea Public Management*. 22(4): 99-127.
- Lee, Sang Min. 2011. Current Authentication Methods and Future Prospect. *Korean Payment & Settlement Association*. 1-39.
- Lyu, Hyeon Suk, et. al. 2009. Resilience and Social Capital. In Chung, Ji Beom and Jae Yeol Lee. (eds.). *A Study on Constructing Social System that Offers Strong Resilience to Disasters*. Korea Institute of Public Administration. 13-56.
- Magurie, B. and P. Hagan. 2007. Disasters and Communities: Understanding Social Resilience. *The Australian Journal of Emergency Management*. 22: 16-20.
- Manyena, S. B. 2006. The Concept of Resilience Revisited. *Disasters*. 30(4): 433-450.
- NIAC. 2009. *Critical Infrastructure Resilience Final Report and Recommendations*. 1-54
- National Information Society Agency. 2010. *Developing Public Authentication Use Technology as a Tool for Protecting Residential Number on Internet*.
- Oh, Il Seok. 2014. A Legal Study on Enhancing Security Authority's Cyber Security Activities. *Law of Science & Technology*. 20(3). 41-90.
- Oh, Tae Kon and Gwan Sil Seoung. 2014. Consideration on the Revision Direction of National Cyber Security Management Legislation. *Journal of the Korea Society of Computer and Information*. 19(3): 163-170.
- Shim, Woo Min. 2014. Issues and Alternatives on Internet Identification: Analysis on the Basis of Architectural Regulation Theory. *Korean Law & Society*. 47: 209-237.
- Shin, Jong Hwan. 2013. The Current Status of Cyber Attacks Based upon the Key Domestic Internet Incidents. *Internet & Security Focus*. 2013(9): 36-53.
- Smith, Richard E. 2002. *Authentication: From Password to Public Keys*. Pearson Education, Inc.
- Tierney K. and M. Bruneau. 2007. Conceptualizing and Measuring Resilience: A Key to Disaster Loss Reduction. *Transportation Research Board*. 2007(5): 14-17.
- Tierney, K. 2003. *Conceptualizing and Measuring Organizational and Community Resilience: Lessons from the Emergency Response Following the September 11, 2001 Attack on the World Trade Center*. Preliminary Paper 329. Newark: University of Delaware.
- Timmerman, P. 1981. *Vulnerability, Resilience and the Collapse of Society*. Toronto: Institute of Environmental Studies, University of Toronto.
- U.S. Black Engineer & Information Technology. Winter 2011, 35(4): 68.
- Korean References Translated from the English*
- 강상준, 조성한, 홍순영. 2013. 자연재해로부터의 지역사회 회복탄력성 도입방안. 경기개발연구원. 1-102.
- 강현수. 2015. AHP방법론의 올바른 활용을 위하여. KIPA조사

- 포럼. 64-70.
- 권창범. 2011. 사이버보안을 위한 국가적 추진체계 검토 및 발전방안. 연세 의료·과학기술과 법. 2(2): 59-80.
- 김성천. 2011. 사이버보안 법제에 관한 연구. 중앙법학회. 13(3): 311-336.
- 류현숙, 정재기, 정지범. 2009. 복원력과 사회적자본. 13-56.
- 정지범·이재열 편. 2009. 재난에 강한 사회시스템 구축 방안 연구 -복원력과 사회적 자본. 한국행정연구원.
- 방송통신위원회. 2011. 사이버보안법제 선진화 방안연구. 1-386.
- 배병환. 2014. 영국 사이버보안 전략 분석 및 시사점: 국가 사이버보안 전략 계획과 추진성과를 중심으로. 정보통신기술진흥센터 주간기술동향(2014.10.08.). 1-14.
- 배선하, 박상돈, 김소정. 2015. 국가 사이버보안 역량 평가를 위한 평가항목 연구. 정보보호학회지. 25(5): 1293-1314.
- 신중환. 2013. 국내 주요 인터넷 사고 경험을 통해 본 침해사고 현황. Internet & Security Focus. 2013(9): 36-53.
- 심우민. 2014. 인터넷 본인확인의 쟁점과 대응방향 - 본인확인 방식과 수단에 대한 아키텍처 규제론적 분석. 법과사회. 47: 209-237.
- 안정철, 권혁진. 2012. 정보·사이버전 유형과 정보기술 측면의 보안전략 발전방향. 한국인터넷정보학회. 13(4): 32-38.
- 안중하. 2013. 국내 사이버보안 체계 진단 및 정책적 대응방안 연구. 한국경찰연구. 125-146.
- 오일석. 2014. 보안기관의 사이버보안활동 강화에 대한 법적 고찰. 과학기술법연구. 20(3): 41-90.
- 오태곤, 성관실. 2014. 국가 사이버안전 관리 법제의 개정방향에 관한 소고. 한국컴퓨터정보학회논문지. 19(3): 163-170.
- 이기식. 2008. 인터넷시대 사이버보안(Cyber\_Security)의 인식 양태 및 정책대안. 한국공공관리학보. 22(4): 99-127.
- 이상민. 2011. 인증방법의 현황과 향후 전망. 지급결제와 정보기술. 1-39.
- 이재광, 전태일, 조재신. 2012. 인증시스템. 서울: 도서출판 그린.
- 이정현. 2013. 스마트 환경에서의 공인인증서 활용과 문제점. Internet & Security Focus. 2013(3): 23-53.
- 임채태. 2012. 최근 사이버침해 사고 동향 및 대응방안. 한국IT서비스학회 학술대회논문집. 204-222.
- 정영철, 배용근. 2014. 동적인 ICT 생태계에 따른 전자정부 보안대책 연구. 한국정보통신학회논문지. 18(6): 1249-1254.
- 정완. 2001. 사이버범죄의 보안대책-암호정책을 중심으로. 한국형사정책연구원 학술총서. 7-131.
- 조호대, 신동일. 2009. 공공 및 민간부문의 사이버침해사고 현황분석에 따른 대응방안. 한국콘텐츠학회논문지. 9(1): 331-338.
- 한국정보화진흥원. 2010. 인터넷상의 주민번호 보호수단으로 공인인증서 이용기술 개발.

Received: Aug. 3, 2016 / Revised: Aug. 23, 2016 / Accepted: Aug. 26, 2016

## 국내외 ICT 융합 환경에 적합한 사이버보안 정책우선순위에 관한 연구

**국문초록** 본 연구는 정보통신기술 발전으로 인한 새로운 사이버침해와 같은 변화된 국내외 사이버보안 환경에 주목하여, 사이버복원력 개념을 바탕으로 ICT 융합 환경에 알맞은 법제도 및 거버넌스를 제안하고자 한다. 최근 사물인터넷, 빅데이터, 핀테크 등 다양한 기술이 등장하고 있으나, 법제도 및 거버넌스 체계는 이러한 변화를 따라가지 못하고 있다. 한편, 국내외 사이버보안 환경을 다룬 기존 연구는 기술적 혹은 법제도적 대안 제시 등 단선적 접근에 그쳐 전체적인 실태나 문제점을 도출하는 데 한계가 있다. 인증을 다룬 사이버보안 연구 역시 공인인증 관련 기술 중심적 담론에서 크게 벗어나지 못하고 있다. 따라서 본 연구는 급증하는 사이버침해사고 유형과 특징을 파악하고, 사이버보안 및 인증보안의 취약성과 복원력 요인 도출을 위해 사이버보안 전문가 17인을 대상으로 AHP(Analytic Hierarchy Process)조사를 진행한다. 이러한 실증연구 결과를 토대로 새로운 기술 환경변화와 법제도를 포괄하는 종합적 고찰을 통해 국내 사이버보안에 알맞은 정책적·기술적 방안을 구체적으로 제시한다.

주제어 : 사이버위협, 사이버 보안, 사이버취약성, 사이버복원력

- 
- Profiles
- Hyeon Suk Lyu** : After earning her Ph.D in Public Administration and Management at Manchester University in UK in 2007, She currently works for the Korea Institute of Public Administration as a research fellow. Her research interests are IT policy and e-governance, government reform, organizational behavior and culture, and disaster management(hslyu@kipa.re.kr).
- Hee Jung Cho** : After earning her Ph.D in Politics and e-voting at Sogang University in Korea in 2007. She currently works for the Institute of Social Science, Sogang University. Her research interests are new media politics and e-government (rilla7@naver.com).
- Hun A Lee** : She received her master degree from Sogang University in Korea in 2015. She currently works for the Korea Institute of Public Administration. Her research interests are IT, digital politics, and media(peace.truly.love@gmail.com).