사이버문화신뢰, 정보통신기술 활용수준 그리고 전자부패간의 관계: 공무원의 인식을 중심으로

Cyber-culture, ICT Utilizatition, and eCorruption

최영훈(Choi, Young-Hoon)* · 김석곤(Kim, Suk-kon)**

ABSTRACT

The authors aim at identifying eCorruption vulnerabilities in the connection of embracing eGovernment projects using a 2x2 matrix of ICT utilization ability and cyber-culture. Based upon the results of questionnaire survey of 174 public officials in charge of embracing eGovernment projects at the national and local levels, they found interesting perceptions of eCorruption vulnerabilities. First, major eCorruption vulnerabilities were related to a heavy reliance upon SI contractors or firms and the premature operation of information system. Second, the higher the levels of ICT utilization and cyberculture confidence, the lower the perceived level of eCorruption vulnerabilities. Also, the lower the level of ICT utilization and cyberculture confidence, the lower the perceived level of eCorruption vulnerabilities. Third, the perceived level of eCorruption vulnerabilities is more related to the level of cyberculture confidence than ICT utilization capability.

Key Words : 전자부패(eCorruption), ICT 활용, 사이버문화(Cyberculture)

I. 서론

지난 10년 남짓한 기간 동안 정보통신기술을 이용하여 행정을 변혁하려는 목적으로 시작된 전자정부사업은 다양한 평가(오강탁, 2002; 오강탁, 2005; UN, 2004; Brown University, 2005)에도 불구하고 커다란 진전을 보여 왔다. 그럼에도 학술적으로나 실제적으로 전자정부사업에 대해 공통적으로 지적되는 점은 전자정부에 대한 합리주의적인 사고(Perris, 2001: 19)에 의거하여 전자정부가 그동안의 제반 행정문제들에 대한 만병통치약으로 제안되고 추진되어 왔다는 점이다(김순희 · 김동환, 2001: 741).

전자정부를 문제해결을 위한 순기능적 도구로 인식하면서 사업을 추진하는 동안 정부기관 내외에서 전자정부로 구현된 현실 속에서 역기능적인 편린들이 노출되면서(한세억, 2003: 337), 역기능에 대한 정부대응의 부적절성에 대한 정부내부의 비판과 아울러 정책적 차원에서 역기능에 대한 관심(서진완, 2001)이 커지고 있다. 그러나 이러한

* 광운대학교 행정학과 교수
** 광운대학교 대학원 박사과정 수료

실재적 또는 잠재적 역기능에 대한 정부의 대응방안은 정보보안사고에 대한 대응체계의 강화에 대한 논의 수준에 머물고 있다(지방혁신지방분권위원회, 2003). 이러한 상황에서 전자정부사업과 관련한 다양한 역기능적 측면들이 지적되어 왔다(감사원, 2003). 정부의 차세대 전자정부구현 노력이 가시화되고 있는 상황맥락에서 전략적 우선순위분야로 '깨끗한 정부'가 중요시 되고 이를 위해 '공무원의 청렴성 및 정직성'이 중시되고 있다는 한 연구결과(명승환・최영훈, 2005)가 시사하듯이 전자정부구현에 있어서 부패 등과 같은 역기능적 측면에 대한 보다 적극적인 대응이 필요하다. Marshall(1999)이 시사하듯이 우리의 전자정부구현노력이 공공부문 및 일반국민들에 폭넓게 확산되고 있는 시점에서 이제는 전자정부와 관련된 역기능적 측면을 예방 또는 방지하기 위한 장치의 제도화가 필요하다. 이러한 점에서 Ogburn이 말하는 문화지체(Ogburn, 1966)를 줄여나가는 노력이 지금부터라도 필요하다.

학술적으로도 전자정부와 관련된 많은 문헌들은 주로 전자정부의 한 구성요소인 정보통신기술의 '밝은' 측면에 대한 입증과 반증에 초점을 맞추고 있고, '어두운' 측면은 그에 대한 논의 자체가 수적으로도 제한적이다. 마찬가지로 김영종(1999)에 의해 정보화의 맥락에서 부패문제에 초점을 맞춘 논의들이 전개된 이후 전자정부맥락에서 부패문제를 다룬 문헌들 역시 수적으로 매우 제한적일 뿐 아니라, 소주제로서 다루어져 왔다(송희준・최홍석, 2002; 명승환・최영훈, 2002; 목진휴외, 2002; 최영훈, 2003). 전자정부에 있어서 부패문제를 주된 주제로 한 연구들의 경우도 전자정부를 통한 부패의 통제라는 기능적 측면의 검증에 주로 치우쳐 왔다(남궁근외, 2002; 권해수, 2002; 목진휴외, 2002; 최영훈, 2003). 또한 정보통신기술과 부패간의 관계에 관한 경험적인 연구들(목진휴외, 2002; 최영훈, 2003)[1]은 정보통신기술과 부패감소 간에 명확한 일관성 있는 관계성을 보여주지 못하였다. 그 이유는 양자간의 관계를 파악할 수 있을 정도로 정보통신기술의 확산이 이루어지지 못하였다거나(목진휴외, 2002) 업무분야에 따라 상이한 결과(최영훈, 2003)가 발생할 수 있기 때문이기도 하다. 부패정보통신기술과 부패발생간의 다양한 관련성(최영훈외, 2003; Heeks, 1998)과 전자정부 맥락에서 부패의 발생사례(최영훈외, 2006: 344-354)을 염두에 둔다면, 전자정부맥락에서 부패의 발생잠재성에 대한 경험적 연구가 현재의 시점에서는 보다 축적되어야 할 필요가 있다. 또한 전자정부맥락에서 발생하는 부패를 전자정부시대의 행정윤리로 바라보려는 논의(김영종, 2002; 최영훈외, 2006)가 이루어지고 있다는 점에서 전자정부맥락에서의 부패 잠재성에 대한 논의의 축적은 중요한 작업이 될 것이다.

부패의 문제를 전자적 맥락에 놓고 볼 때, 부패의 잠재성을 객관적으로 파악해 내는 데에는 제약이 따른다. 전자정부사업과 관련된 위험요소들의 관리가 절대적으로 필요하

1) 이 두 문헌은 동일한 설문조사자료를 사용하였을 뿐만 아니라 정보통신기술-레드테이프-부패에 관한 동일한 이론적 토대를 바탕으로 하고 있다. 차이가 있다면 목진휴외(2002)는 응답자들의 전반적인(global) 의견을 토대로 한 데 비해, 최영훈(2003)은 업무분야간의 차이점을 규명하려 하였다는 점이다.

지만(OECD, 2001), 실제로 밝혀지는 전자정부맥락에서의 부패는 금전적 가치나 규모면에서 경미한 수준이라는 점에서 위험요소의 파악 자체에 어려움이 따른다. 이러한 점에서 전자정부맥락에서의 부패의 잠재성은 우선적으로 인식의 차원에서 확인되고 이를 통해 체계적으로 개념화될 필요성이 있다.

전자정부맥락에서 부패 잠재성에 대한 인식은 정보통신기술의 사용과 전자정부가 구현되는 사이버(온라인)문화에 대한 신뢰에 의해 크게 영향을 받을 수 있다. 정보통신기술의 사용의 측면에서 볼 때, 전자정부에 내제된 위험요소는 우연히 발생하는 사건 또는 사고라기보다는 정보통신기술이 가져다주는 편익에 맞물려 불가피하게 공존하는 사회적 비용이기 때문이다(정익재 외, 2000: iii). 사이버문화에 대한 신뢰의 측면에서 볼 때, 정보통신기술로 구현된 사이버공간의 비대면성, 익명성, 개방성 등의 특성들은 부패의 가능성에 커다란 영양을 미친다. 본 연구는 전자정부의 맥락에서 잠재화 된 부패를 전자부패로 개념화 하고, 정보통신기술활용 및 사이버문화신뢰에 따른 전자부패 위험요인을 도출하는데 그 목적이 있다.

II. 전자부패, ICT 활용수준, 그리고 사이버문화신뢰 간의 개념적 관계

1. 전자부패, 정보통신기술과 부패의 관련성

1) 전자부패의 의의

전자부패는 “공공부문에서 컴퓨터시스템을 사용하여 공무원, 계약업자 기타 권한을 부여받은 사람에 의해 범해지는 부조리, 부패 또는 범죄”로 정의된다(최영훈외, 2006: 308; ICAC, 2001: 3).[2] 전자부패를 이렇게 정의할 때 전자부패는 일반적인 부패나 컴퓨터 범죄에 대한 통상의 개념정의 보다 부패의 주체 및 부패의 내용 등의 면에서 더 넓은 의미를 지닌다. 전자부패는 컴퓨터를 수반하는 범죄행위를 의미하는 컴퓨터범죄 또는 전자적 범죄와는 구분되는 개념이다. 전자부패는 공공부문의 업무환경에 있어서 ‘합법적인지만 수용하기 어려운’ (legal but unacceptable) 행위까지도 부패의 범위에 포함시킨다(ICAC, 2001). 이러한 점에서 전자부패 개념은 정보시대의 행정 또는 전자정부에 있어서 공무원 또는 “행정윤리의 새로운 개념”(최영훈외, 2006)[3]으로 간주하기도 한다.

2) 전자부패와 유사한 용어로서 ‘정보부패’(김영종, 1999) 또는 ‘사이버부패’(김영종, 2002)라는 표현을 사용하는 학자도 있다. 정보부패(information corruption)란 “정보관련자가 정보를 누설, 악용하거나 남용하여 시민의 기대가능성을 저버린 일탈행위”(김영종, 1999: 30)로 정의된다. 또 사이버부패는 “컴퓨터범죄를 포함하여 가상공간에서 이루어지는 모든 부패”를 말한다(김영종, 2002: 84). 그러나 정보부패나 사이버부패는 불법적 행위는 물론 비도덕적 행위도 포함한다는 점(김영종, 1999; 2002)에서는 전자부패와 유사한 점을 지니나, 전자의 두 가지 유형의 부패는 공통적으로 ‘특수한 정보관련자의 탐욕의 도모 또는 개인적 이익의 추구’를 전제로 하고 있다는 점에서 정보관련자의 탐욕 등과 같은 개인적인 이익증진 동기 없이도 저질러지는 불법적 또는 비도덕적 행위(예컨대, 자신의 접근 ID나 비밀번호를 부하직원에게 알려주어 일을 대신 처리토록 하는 행위)까지도 포함하는 전자부패와는 다르다.

2) 정보통신기술과 부패의 관계성

아직까지 행정부패와 정보통신기술간의 인과성 등에 대한 경험적인 논의는 존재하지 않으며 단편적으로 이들 간의 상관성의 존재에 대한 논의만 있을 뿐이다. 정보통신기술과 부패의 관계에 관한 논의가 미진한 가운데, 양자의 관계에 대한 다양한 개연성이 제시되고 있다. 정보통신기술이 공공부문의 부패에 미치는 효과에 대해서는 다음의 3가지의 경쟁적인 입장-부패방지·적발효과, 부패유발효과, 무관계-이 가능하다(Heeks, 1998). 로 입장으로 나누어 볼 수 있다.[4)]

부패방지·적발효과는 부패통제에 대한 '원형감옥관념'(Panoptic conception of corruption control)이다(Anechiarico & Jacobs, 1994). 요체는 부패통제의 관건은 어떠한 관리기법을 사용하는가에 달려있다는 것이다. 이에 따르면, 정보통신기술은 관리통제를 가능하게 하는 주된 수단이 될 수 있다. 즉 한 사람의 간수가 재소자들의 일거수일투족을 관찰할 수 있도록 만들어진 원형교도소와 마찬가지로, 정보시대의 조직에 있어서 보이지 않는 곳에서 관리자가 직원들의 제반 행동을 관찰할 수 있게 된다. 이러한 특성을 이용해 부패를 통제할 수 있다는 것이다(Roszak, 1994). 부패방지·적발효과는 두 가지 측면에서 이루어질 수 있다(Heeks, 1998: 6). 하나는 부패유발의 원천이 되는 자원 또는 의사결정과정에 대한 접근을 제한하는 것이다. 접근을 제한하는 방법은 의사결정과정을 자동화(automation)하여 인간의 접근필요성을 제거하거나, 자원에 대한 접근자격을 한정하는 것이다. 또 다른 하나는 상기의 원형감독 메타퍼에서 유추해 볼 수 있듯이 정보통신기술을 통해 업무환경이 투명해 지는 경우 공무원들이 스스로 인지하게 되는 자율성이 낮아지게 되고 이에 따라 부패가 억지될 가능성이 커진다.

부패유발효과는 비록 현재로서는 소수의 견해이지만, 정보통신기술이 일부 공무원들에게는 도리어 새로운 부패의 기회를 제공할 수 있다고 본다(Heeks, 1998). 부패유발효과 역시 크게 두 가지 측면에서 발생할 수 있다. 하나는 정보통신기술의 접근장벽으로 작용하여 정보통신기술에 익숙한 전문가에 의한 부패의 유발가능성이 있다는 점이다(Heeks, 1998: 7). 또 다른 효과는 커넥션효과(connection effect)이다(Bac, 2001). 정보통신기술은 공무원의 신상에 관한 정보를 외부인이 보다 상세히 알 수 있게 하여줌으로써 부패의 목적으로 '커넥션을 구축하기 위한 유인을 증대시켜 줄 수도 있다.

끝으로 정보통신기술(ICT)와 부패간의 무관계성을 주장하는 논거들은 다양하다. 한 가지는 정보시스템의 설계와 관련된다. 전산화가 이루어지더라도 부패관련 자원이나 과정이 전산화되지 않는 경우이다(Heeks, 1998: 7). 이 경우 전산화가 이루어지더라도 여전히 부패의 가능성이 잔존하게 된다.

---

3) 김영종(2002) 역시 전자부패를 행정윤리적 차원에서 접근한다.
4) 여기서는 Heeks(1998)의 3가지 입장에 대한 기술을 중심으로 보완하여 제시하고자 한다.

2. 전자부패 위험요인

전자부패를 유발하는 위험요인에 대해서는 학문적인 측면에서 보다는 실무적 차원에서 논의되어 왔다(ICAC, 2001). 전자정부사업을 통해 구축된 정보통신기술 및 이를 기반으로 이루어지는 사이버공간은 익명성,[5] 네트워크성, 원격성, 접근용이성 등으로 인해 보안 또는 부패와 관련하여 위험도를 증가시키다(Donavan, 1993; 최영훈외, 2005).

1) 행위의 주체에 의한 위험요인

행위자 측면에서 내부자와 외부자에 따라 부패의 양상은 다른 것으로 알려져 있다. Neumann(1999)은 내부자와 외부자를 존재의 양식에 따라 논리적 존재와 물리적 존재로 각각 구분한다. Neumann(1999)은 이에 대해 상술하지 않고 있지만, 의미상 논리적 존재란 해당 정보 또는 정보통신기술에 대한 접근권한을 지니고 있는지에 따라 논리적 내부자와 논리적 외부자, 해당 정보 또는 정보통신기술에 물리적으로 접근(또는 침투)하였는지에 따라 물리적 내부자와 물리적 외부자로 나누어 볼 수 있다.[6] 전자부패의 성격에 따라 고의적인 부패와 우발적인 부패, 그리고 우발적 부패의 성격에 따라 노출성(overt) 부패와 은닉성(covert) 부패 등으로 다시 구분해 볼 수 있다(Neumann, 1999).[7] 이와 같은 행위자별 존재의 기본적인 양식은 <표 1>과 같이 개념화할 수 있다.

<표 1> 행위자별 부패 존재 양식

		논리적 존재	
		내부자	외부자
물리적 존재	내부자	접근권한을 지닌 자(예, 담당공무원이나 계약업체직원 등)가 해당 정보시스템을 이용하여 범하는 부패	접근권한이 없는 자가 해당 정보시스템에 침투하여 범하는 부패
	외부자	접근권한을 지닌 자가 해당 정보시스템에 침투하지 않고 범하는 부패	접근권한이 없는 자가 정보시스템에 침투하지 않고 범하는 부패

출처: Neumann(1999)참고하여 저자가 작성.

2) 기술적 측면에서 본 전자부패 위험요인

Bell & Zipparo(2000)는 정보통신기술이 부패행위에 이용될 잠재성을 보이는 위험요인으로서 일반적 요인과 기술적 요인으로 구분한다. 일반적인 요인으로 자동화(automation), 즉시성(immediacy), 접근성(accessibility), 편재성(Ubiquity), 부수적 정보

5) 사실 전자적 공간에서 익명성은 완전할 수 없다. 이는 전자적 자취들이 사후 또는 사전 또는 접속 중에 기록되고 추적될 수 있기 때문이다.

6) Neumann은 논리적 내부자와 물리적 내부자에 초점을 맞추고 있다.

7) 또한 동기측면에서 금전적 동기와 비금전적 동기로 나누어 볼 수 있다. 전자부패와 관련하여 주목할 것은 직접적 금전이익보다는 보복, 권태, 도전, 탐욕 등이 주요 동기로 지목되기도 한다(Bell & Zipparo, 2001: 12).

의 손실(loss of collateral information), 신사업모형(new business model), 암호화(cryptography)을 들고, 기술적 요인으로 e-mail, 응용서비스 공급자와 IT의 외부수주, 전사적자원기획체계(Enterprise Resource Planning System), 주변기기를 이용한 사기행위, 크래킹 및 해킹 등을 들고 있다.

구체적으로 자동화 및 즉시성과 관련된 부패 발생 가능성은, 업무가 자동화 됨에 따라 간섭이나 감독이 줄어들게 되어 직원들이 범죄자들이나 외부인과 공모하여 시스템상의 거래감시, 수작업 검토, 사용인증 등의 절차에서 허점을 찾아 이를 이용하려 들 수 있다는 것이다. 이 경우 전통적인 감사 방식이나 나 회계 방식도 새로운 환경 하에서는 부적절하게 된다(Bell & Zipparo, 2000).

부수적 정보의 손실과 관련된 부패발생가능성은 공공기관과 전자정부서비스를 이용하는 이들이 미심쩍거나 부자연스럽다든지 혹은 비정상적인 행동을 나타내는 이른바 “사회적 정보(social cues)”를 이용할 여지가 줄어들게 되어, 공급업자, 감독관, 기타 직원의 전자적 비인격화에 의한 희생자가 될 소지가 있다(Bell & Zipparo, 2000).

접근성 및 편재성과 관련하여, Bell and Zipparo(2000)은 직원들이 정보시스템에의 접근이 너무 용이하여 발생하는 문제로서, 많은 경우 패스워드 사용 혹은 패스코드의 보호가 완벽하지 않다는 점으로부터 일어나는 경우가 많다. 직원들이 불법으로 정보시스템에 접근하려 하거나 외부자와 공모하여 그들의 시스템 접근을 도울 수도 있다. 또한 동료들끼리 패스워드를 서로 주고받는 등 보안의식 결여도 전자부패를 유발할 잠재성을 높이는 요인으로 작용한다.

신사업모형과 관련된 부패가능성으로 Bell and Zipparo(2000)는 신기술의 도입에 따라 발생하는 새로운 사업기회에 주목한다. 신기술에 익숙지 못하여 이에 대한 접근이 불가능한 사람들이 존재하는 경우 이들의 행정적 또는 기술적 어려움을 해결하여 주는 대가로 뇌물이 거래되기 쉬운 중간매개산업을 낳을 여지를 남긴다. 아울러 여러 기관의 행정적 기능이나, 아웃소싱 기능의 가상적 통합, 공공부문과 민간부문간 협업 등은 사업수행 및 서비스 공여의 신모형들은 부패의 유발가능성을 안고 있다.

암호화는 정보시스템에 대한 불법적 접근을 방지하는 기능을 하면서도, 부패행위를 입증할 중요한 증거가 부패행위가 의심받을 때 수사를 회피하기 위해 암호화될 수 있다. 특히 Dan Brown의 소설 Digital Fortress(Brown, 2005)에서와 같이 암호화 소프트웨어의 사용이 쉬워지고 일반 OS의 응용프로그램 혹은 워드프로세싱 프로그램의 패키지로 제공되는 추세를 감안하면 암호화는 부패를 조장할 또 다른 가능성을 던지고 있다.

Bell & Zipparo(2000)의 기술적 요인으로서 이메일, 모바일폰 등은 불법적 행위나 부패행위에 자주 사용되는 도구이다. 물론 최근 황우석 사건에서 보았듯이 이메일에 의한 통신은 역으로 부패행위를 적발 및 입증할 수 있는 중요한 근거로도 사용된다. 정보통신기술 및 시스템의 아웃소싱(outsourcing) 및 응용서비스공급자(application service providers) 관련 Bell & Zipparo(2000)은 정부기관들은 아웃소싱한 정보통신기술업자들

에게 포획될 위험에 노출되어 있다고 주장한다. 공공부문의 경우도 사부문과 같이 아웃소싱을 하는 이유는 매우 다양하지만(Bragg, 1998), 공공부문의 경우 기술력 및 전문성 부족이 아웃소싱의 큰 비중을 차지한다(송희준・김은정, 2001). 그러나 이러한 이유로 인해 이루어지는 아웃소싱은 공급자의 계약불이행, 공급업체에 대한 종속가능성, 업체에 대한 통제력 상실, 정보시스템에 대한 보안유지의 어려움 등 다양한 위험요인들을 배태하고 있기도 하다(Ewusi-Mensah, 1997; Keil, Cule, Lyytinen and Schmitt, 1998; Boehm, 1991; Bell & Zipparo, 2000; Tho, 2005; 감사원, 2003). 이와 아울러 전사적 자원관리(Enterprise Resource Planning, ERP)나 전자인증 등도 전자부패의 가능성을 유발하는 요인으로 지목되기도 한다(Bell & Zipparo, 2000; Tho, 2005). 이외에도 스캐너나 프린터를 이용한 위조 또는 ID 위조 등과 같이 정보통신기술을 이용한 사기행위도 잠재성이 높은 요인으로 간주되고 있다(Bell & Zipparo, 2000; Tho, 2005). 또한 크래킹이나 해킹이 이전 보다 훨씬 수월해졌으며, 정부 웹 사이트에 축적되어 있는 데이터와 서비스나 정책에 관련된 정보들이 해킹과 같은 외부의 공격에 의해 파괴될 수 있다. 이러한 해킹은 내부직원의 도움으로 외부인이 컴퓨터 시스템에 침투할 가능성도 커지고 있다(Bell & Zipparo, 2000; Tho, 2005).

3. 전자부패를 보는 인식의 창 : ICT활용수준 및 사이버문화신뢰, 전자부패간의 관계성

전자정부가 작동하는 맥락은 정보통신기술적 요소와 사회문화적 요소가 결합되어 있는 공간이다(Kitchin, 1998). 전자정부는 합리주의적 또는 낙관론적인 전망을 가능하게 함과 아울러, 정보통신기술과 사회문화 또는 사회제도 사이의 '부정적 상승작용'(negative synergies)에 따른 체계적 위험(systemic risks)을 초래하기도 한다(Hellstrom, 2003). 더 나아가 Echeverr(2003)가 주장하듯이, 과학기술(techno-science)[8]은 단순히 진리의 탐구활동이 아니라 선악(good and bad)의 문제와 관련되어 있는 것으로 봄으로써, 과학기술을 인공물이 아닌 세상을 변개시키는 활동으로 간주한다. 전자정부의 맥락을 정보통신기술적 요소와 사회문화적 요소의 결합으로 볼 때, 전자부패는 정보통신기술에 대한 활용능력(capacity to use)에 대한 개인의 인지와 정보통신기술의 활용행위 규제에 대한 믿음(confidence in sanctions)의 결합으로 볼 수 있다(Kuo and Hsu, 2001).

전자정부의 맥락에서 공무원의 요건 중 하나는 정보통신기술의 활용 능력이다. 전자정부의 맥락에서 정보통신기술 활용능력의 중요성은 정보통신기술이 더 이상 행정업무 수행을 위한 외생적 수단으로 존재하는 것이 아니라, 행정업무 자체는 물론 그 수행을

8) Echeverr(2003)은 과학기술(techno-science)을 과학 및 기술과 구분되는 개념으로 정의하고 있다. 이 점에서 일반적인 용어로 사용되는 과학기술(science and technology 또는 scientific and technological) 등의 용어와 혼동해서는 아니 된다.

위해 필수불가결한 내생적이고 통합적인 인프라라는 점이다(최영훈외, 2006). 이러한 정보통신기술의 역할관에서 보면, 공무원들은 업무 수행에 필요한 정보에 접근하고 이를 활용하여 분석 및 의사결정을 행하고 대외적 업무수행 및 서비스 전달 등의 행위를 능률적·효과적으로 그리고 투명하게 수행할 것으로 기대된다. 또한 전자정부의 맥락에서 정보통신기술에 대한 높은 전문성을 지닌 전문가들의 수요도 증대된다. 정보통신기술 활용능력은 전자정부 맥락에서 공무원에게 필수적으로 요구되는 원리인 한편으로 전자정부 맥락에서 공무원의 부패행위에 있어서도 중요한 기제로 작용한다. 정보통신기술의 활용능력이 전자부패 취약성의 높고 낮음에 어떤 영향을 미치는지에 대해서는 경험적으로 명확히 밝혀져 있지 않다. 다만 이러한 관계를 유추해 볼 다소 거리가 있는 경험적 자료를 사용할 수 있을 뿐이다. 먼저, Demchak, Friis and La Porte(1999)는 사회적 차원에서 인터넷 보급율 등이 행정의 투명성 정도와 관계가 있다는 경험적 증거를 보여준다.[9] 다른 한편, 전자부패에 대한 일반적인 인식은 고도의 기술적인 부패행위라고 보고 있다(김영종, 1999). 전자부패를 고도의 기술적인 부패행위로 파악할 때 전자부패의 취약성은 정보통신기술에 대한 전문적인 지식을 지닌 이들 사이에서 나타날 가능성이 더욱 높아진다(Hagque, 2001). 또한 정보통신기술의 활용수준이 증가하면서 고의적으로나 우연적으로나 정보통신기술의 오남용이나 부패가 발생할 가능성도 커진다(Neumann, 1999; Garnham, 1977). 이러한 점에서 Heiddeger(1977: 5)에서 유추해 볼 수 있듯이, 정보통신기술을 숙달해야할 필요가 커질수록 정보통신기술은 인간통제를 벗어날 가능성도 커진다.

정보통신기술 활용능력과 전자부패간의 관계는 직접적이라기보다는 이러한 부패행위가 얼마나 통제될 수 있는지 정보통신기술이 활용되는 맥락과 관련된 문화적 또는 의식적 측면에 의해 영향을 받는 경우가 일반적이다. 정보통신기술의 이용을 규제하는 문화, 즉 사이버 문화는 정보통신기술이 창조해 낸 사이버공간을 새로운 도구이자 장으로 이용하면서 나타나는 문화적 현상을 총칭한다(소흥렬, 1999: 49-50; 홍성태, 1999: 80-86). 이렇게 정의했을 때, 사이버문화는 사이버공간에만 국한되는 현상이 아닌 보다 포괄적인 의미를 지닌다. 사이버공간은 비록 인공으로 만들어지는 공간의 세계이지만 도구주의적 의미를 더하게 되면 누구나 마음대로 만들어 볼 수 있는 무제한적 도구주의의 공간이 될 수도 있다(소흥렬, 1999: 48). 사이버공간은 실제세계를 대체하는 것이 아니라 실제 세계를 다른 자리로 옮겨 놓은 것(소흥렬, 1999: 48)이라는 점에서 사이버문화는 사이버공간 자체의 존재론적 위상과 함께 확장된 세계 속에서 현실세계가 지닌 존재론적 의미를 재고찰하게 한다. 이렇게 보면, 결국 사이버공간은 현실공간의 겨울에 비친 상(mirror image)일 수 있다는 주장이 가능해진다.[10] 사이버공간을 도구이자 장으

9) 행정투명성은 다면적인 가치를 반영하는 것이라는 점에서(명승환·최영훈, 2002) 투명성에 대해 밝혀진 경험적 관계가 모두 전자부패에도 무조건적으로 적용된다고 주장할 수는 없을 것이다.

10) 여명숙(1999: 11)은 사이버공간의 정보들을 처리하는 주체들이 인간 이외에도 에이전트 프로그램일 수 있기 때문에 사이버공간에서의 인간행위의 윤리적 평가가 어려울 수 있다고 주장

로 형성되는 문화는 정보통신기술의 활용과 관련한 개인들의 행위를 규율하는 원리로서 작용한다. 따라서 사이버문화가 개인들의 행위를 규율할 수 있다는 신뢰가 높을수록 전자부패와 같은 정보통신기술의 역기능적인 이용은 감소될 수 있다.

정보통신기술 활용능력 및 사이버문화가 전자부패와 맺는 관계성은 <표 2>와 같이 도식화할 수 있다.

<표 2> 정보통신기술 활용능력, 사이버문화, 전자부패간의 개념적 관계

		정보통신기술의 활용능력	
		높다	낮다
온라인문화 신뢰	높다	I	II
	낮다	III	IV

III. 자료수집방법 및 분석방법

1. 자료수집방법

본 연구를 위한 자료는 중앙부처 및 지방자치단체에서 전자정부사업을 담당한 공무원들을 대상으로 한 설문조사로부터 얻어졌다. 설문조사는 2003년 전국 정보화담당관협의회 회의에 참석한 공무원들을 대상으로 배포되고 회수되었다.[11] 총 250부가 배포되어 204부가 회수되었다. 회수된 204개의 설문지 가운데 174명[12]으로부터 회수된 설문지만을 분석대상으로 하였다.

<표 3>에서 보듯이 분석대상 공무원 중 국가공무원과 지방공무원은 각각 39.1%, 60.9%의 분포를, 직렬별로는 행정직과 전산직이 각각 44.8%, 47.1%로 비교적 균등한 분포(나머지는 무응답 7.5%)를 보였다. 직급별로는 6급이 40.8로 가장 많고 8급과 9급

한다.

11) 설문조사는 2005년 10월부터 이메일조사방식을 통해 공무원을 대상으로 실시되었으나 이메일조사에 대한 응답률이 매우 저조하여 정보화담당관회의 기간 동안 참석자를 대상으로 설문조사를 행하였다. 공무원에 대한 설문조사와 함께 전자정부사업에 참여한 주요 기업을 대상으로도 설문조사를 하였으나 여기서는 기업에 대한 설문조사결과는 포함하지 않았다.

12) 174명의 설문응답만을 분석대상으로 하게 된 이유는 이하에서 언급하듯이, 본연구를 위한 집단분류 변수로 사용된 온라인문화에 대한 신뢰를 묻는 항목 그리고 정보통신기술활용수준을 묻는 항목 모두에 응답한 응답자의 수가 174명이었기 때문이다. 이에 대해서는 이하에서 보다 구체적으로 기술할 것이다.

은 합쳐서 1%에 불과한 분포를 보여주고 있다. 근무연한에 있어서도 거의 70%이상이 10년이상 근속한 공무원들이었다. 일평균 온라인업무시간이 5시간 이상인 비율이 64.3%로 나타나 분석에 포함된 공무원들이 대체로 온라인상의 업무가 많은 집단임을 보여주고 있다.

<표 3> 응답자 배경

(단위: 명, %)

신분		직 렬		직 급		근무연한		일일 평균온라인상 업무시간	
국가 공무원	68(39.1)	행정직	78(44.8)	4급	12 (6.9)	5년미만	26(15.3)	1시간	6 (3.4)
				5급	52(29.9)	10년미만	21(12.0)	2시간	6 (3.4)
				6급	71(40.8)	15년미만	39(28.1)	3시간	17(9.8)
		전산직	83(47.7)	7급	23(13.2)	20년미만	27(15.6)	4시간	32(18.4)
지방 공무원	106(60.9)			8급	1 (0.6)	20년이상	44(26.7)	5시간이상	112(64.3)
		무응답	13(7.5)	9급	1 (0.6)	무응답	4 (2.3)	무응답	1 (0.6)
				무응답	14(8.0)				
합 계	174 (100.0)	합계	174 (100.0)	합 계	174 (100.0)	합 계	174 (100.0)	합 계	174 (100.0)

2. 분석방법

본연구의 분석에 사용된 통계적 방법은 일변량분석방법(One-Way ANOVA)이다. 변량분석방법을 사용하여 응답자의 공무원신분 및 직렬에 의한 차이를 분석하였다. 일변량분석에서 전자부패의 각 차원에 따른 응답자군집간 유사성 및 차별성을 결정하기 위해 Duncan 검정을 행하였다.

Ⅳ. 조사결과의 분석 및 논의

1. 응답자의 군집화와 전자부패 위험요인의 분류

1) 정보통신기술 활용역량, 사이버문화신뢰, 전자부패간 관계의 군집화

정보통신기술활용수준은 응답자가 자신의 정보통신기술 활용수준에 대해 '상' '중' '하' 중 하나로 스스로 평가하도록 하여 측정하였으며, 온라인문화 신뢰수준은 응답자가 '부서내의 온라인 문화 신뢰수준'을 '상' '중' '하' 중 하나로 평가하도록 하여 측정하였다. 응답자 204명 가운데 정보통신기술 활용수준과 온라인문화 신뢰수준 문항 모두 응답한 193명(11명 무응답)의 응답을 토대로 교차분석 하였다. 교차분석 결과 각 항목에 대한 응답이 각각 '상'과 '중'에 집중되어 있어 각 항목에 대해 각각 '하'라고 응답한 응

답자는 총19명으로 의미있는 교차분석에 필요한 최소한의 표본수에 미달하여 이들 19명의 응답을 제외한 174명의 응답을 이용하여 <표 4>에서와 같은 2x2 매트릭스를 구성하였다. 이 과정에서 각 항목에 대한 설문지상의 '상' '중'의 응답항을 각각 '높다' '낮다'로 대치하여 4개의 집단, I, II, III, IV를 구성하였다.

<표 4> 정보통신기술 활용능력과 사이버 문화 신뢰간의 관계

		정보통신기술의 활용수준		
		높다	낮다	합계
사이버문화 신뢰수준	높다	I 37 (21.3)	II 35 (20.1)	72 (41.4)
	낮다	III 31 (17.8)	IV 71 (40.8)	102 (58.6)
	합계	68 (39.1)	106 (60.9)	174 (100.0)

2) 전자부패 위험요인의 분류

전자부패의 위험요인은 Bell & Zipparo(2000) 및 Neumann(1999)의 논의를 바탕으로 하여 다음과 같이 공무원과 민간계약자, 내부자와 외부자 등에 의한 다양한 일반적, 기술적 요인을 바탕으로 하는 전자부패 가능성을 탐색적으로 제시하였다.

- 동료의 패스워드를 알아내어 온라인상에서 불법행위를 저지를 가능성
- 조직 내 중요 자료를 암호화하여 E-mail로 외부의 이해관계인에게 유출할 가능성
- 중요 정보를 담당하는 직원이 휴대폰, PDA, 노트북 등의 무선 통신기능을 이용해 외부에 유통시킬 수 있는 가능성
- 급여를 관리하는 부서에 근무하는 직원이 모든 직원의 급여에서 눈에 띠지 않게 소액을 자신의 계좌로 빼돌릴 가능성
- 시스템에 대한 안정성, 보안테스트 등을 시스템 개발회사에 맡길 가능성
- 최신 소프트웨어나 시스템을 도입함에 있어서 일정이 촉박하여 안정성을 제대로 검증(Beta Test)하지 못한 채 도입할 가능성
- 시스템의 유지, 관리업무를 정부로부터 위임받은 민간회사에 의해 공공 자료가 영리추구에 사용될 가능성
- 시스템의 인가코드나 취약성을 잘 알고 있는 IT 능력이 뛰어난 내부직원이 외부의 해커를 가장해 불법적으로 정보를 유출해 이익을 취할 가능성
- 시스템 공급업체 또는 업체의 직원이 정보시스템 내부에 '자신만이 아는 접근통로'(Back Door)를 만들어 놓고 공공정보를 유출하거나 변환할 수 있는 가능성
- 전자조달부문의 인증절차를 잘 알고 있는 내부직원이 전자조달 시스템에 허위사업

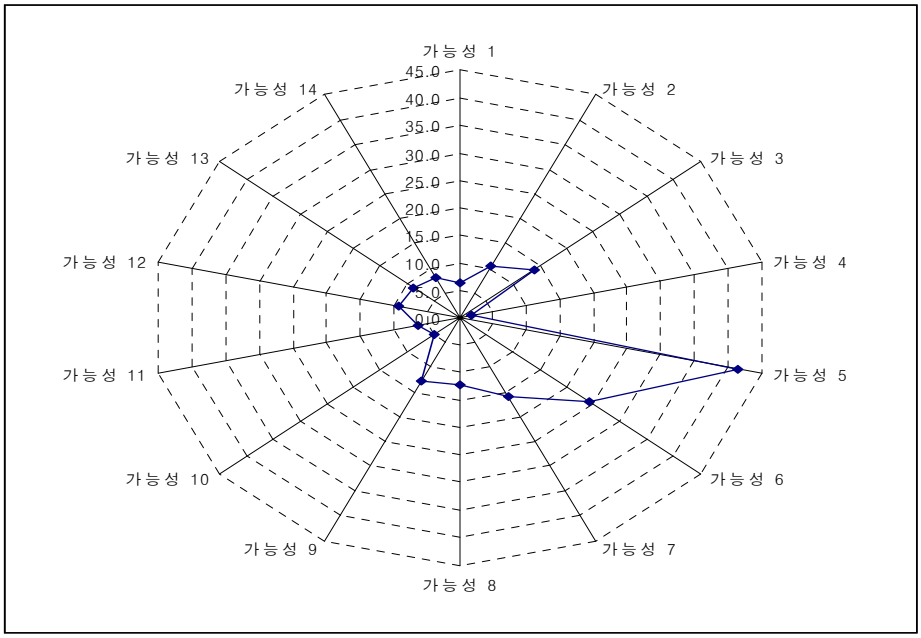
자를 만들어 입찰에 참여하고 내부정보를 이용하여 낙찰받을 가능성
- 계약기간이 만료되어 퇴직한 계약직 근로자가 근무 당시 알고 있던 정보를 이용해 온라인상에서 접속권한이 있는 자로 활동하며 정보를 변조, 파괴할 수 있는 가능성
- 공공의 목적으로 수집된 내부 정보가 시스템을 공급/관리하는 민간업체/직원에 의해 영리목적으로 사용될 가능성
- 내부시스템에 대해 잘 알고 있는 직원이 의도를 가지고 외부인과 공모하여 외부로부터의 해킹, 위변조 등 공격을 유도할 수 있는 가능성
- 업무가 분장되어 있음에도 어떤 직원이 자신의 담당업무 이외의 타업무까지도 정보기술을 이용해 부당하게 처리함으로써, 온라인상에서 분리되어 수행되어야 할 업무를 실제로는 한 사람이 수행할 가능성

2. 전자부패 위험요인에 대한 개관

<그림 1> 및 <표 5>에 제시된 14개의 전자부패 가능성에 대해 가능성5(시스템에 대한 안정성, 보안테스트 등을 시스템 개발회사에 맡길 가능성)(41.4%)와 가능성6(최신 소프트웨어나 시스템을 도입함에 있어서 일정이 촉박하여 안정성을 제대로 검증(Beta Test)하지 못한 채 도입할 가능성)(24.2%)를 제외하고는 발생가능성이 매우 낮은 것으로 인식되고 있다.

<그림 1> 전자부패의 위험요인에 대한 인식

(단위: %)



응답자의 10% 이상이 '높다'고 답한 가능성은 가능성2(조직 내 중요 자료를 암호화하여 E-mail로 외부의 이해관계인에게 유출할 가능성), 가능성3(중요 정보를 담당하는 직원이 휴대폰, PDA, 노트북 등의 무선 통신기능을 이용해 외부에 유통시킬 수 있는 가능성), 가능성7(시스템의 유지, 관리업무를 정부로부터 위임받은 민간회사에 의해 공공 자료가 영리추구에 사용될 가능성), 가능성8(시스템의 인가코드나 취약성을 잘 알고 있는 IT 능력이 뛰어난 내부직원이 외부의 해커를 가장해 불법적으로 정보를 유출해 이익을 취할 가능성), 가능성9(시스템 공급업체 또는 업체의 직원이 정보시스템 내부에 '자신만이 아는 접근통로'(Back Door)를 만들어 놓고 공공정보를 유출하거나 변환할 수 있는 가능성) 등이다.

<표 5> 전자부패의 위험요인에 대한 인식

(단위: %)

전자부패 위험요인	높다	보통	낮다
가능성 1 : 동료의 패스워드를 알아내어 온라인상에서 불법행위를 저지를 가능성	6.3	21.3	72.4
가능성 2 : 조직 내 중요 자료를 암호화하여 E-mail로 외부의 이해관계인에게 유출할 가능성	10.3	25.9	63.8
가능성 3 : 중요 정보를 담당하는 직원이 휴대폰, PDA, 노트북 등의 무선 통신기능을 이용해 외부에 유통시킬 수 있는 가능성	13.8	27	59.2
가능성 4 : 급여를 관리하는 부서에 근무하는 직원이 모든 직원의 급여에서 눈에 띠지 않게 소액을 자신의 계좌로 빼돌릴 가능성	1.7	6.9	91.4
가능성 5 : 시스템에 대한 안정성, 보안테스트 등을 시스템 개발회사에 맡길 가능성	**41.4**	**40.2**	**18.4**
가능성 6 : 최신 소프트웨어나 시스템을 도입함에 있어서 일정이 촉박하여 안정성을 제대로 검증(Beta Test)하지 못한 채 도입할 가능성	**24.2**	**37.9**	**37.9**
가능성 7 : 시스템의 유지, 관리업무를 정부로부터 위임받은 민간회사에 의해 공공 자료가 영리추구에 사용될 가능성	16.0	28.2	55.8
가능성 8 : 시스템의 인가코드나 취약성을 잘 알고 있는 IT 능력이 뛰어난 내부직원이 외부의 해커를 가장해 불법적으로 정보를 유출해 이익을 취할 가능성	12.1	24.1	63.8
가능성 9 : 시스템 공급업체 또는 업체의 직원이 정보시스템 내부에 '자신만이 아는 접근통로'(Back Door)를 만들어 놓고 공공정보를 유출하거나 변환할 수 있는 가능성	12.7	18.4	68.9
가능성 10 : 전자조달부문의 인증절차를 잘 알고 있는 내부직원이 전자조달 시스템에 허위사업자를 만들어 입찰에 참여하고 내부정보를 이용하여 낙찰받을 가능성	4.6	12.6	82.8
가능성 11 : 계약기간이 만료되어 퇴직한 계약직 근로자가 근무 당시 알고 있던 정보를 이용해 온라인상에서 접속권한이 있는 자로 활동하며 정보를 변조, 파괴할 수 있는 가능성	6.4	17.8	75.8
가능성 12 : 공공의 목적으로 수집된 내부 정보가 시스템을 공급/관리하는 민간업체/직원에 의해 영리목적으로 사용될 가능성	9.2	24.1	66.7
가능성 13 : 내부시스템에 대해 잘 알고 있는 직원이 의도를 가지고 외부인과 공모하여 외부로부터의 해킹, 위변조 등 공격을 유도할 수 있는 가능성	8.7	26.6	64.7
가능성 14 : 업무가 분장되어 있음에도 어떤 직원이 자신의 담당업무 이외의 타업무까지도 정보기술을 이용해 부당하게 처리함으로써, 온라인상에서 분리되어 수행되어야 할 업무를 실제로는 한 사람이 수행할 가능성	8.1	23.6	68.3

<그림 1> 및 <표 5>에 요약된 본조사의 결과를 통해 몇 가지 발견사실을 찾아 볼 수 있다.

하나는 전자부패의 주된 가능성은 정보통신기술 관련자들의 개인적 또는 조직적 차원에서의 불법 또는 비윤리적인 행위와는 별다른 관련성을 지니지 않는다는 점이다. 그보다는 오히려 전자정부관련 시스템 또는 보안의 확보와 관련된 공무원들의 전문성 부

족에 따른 시스템개발업체에 대한 의존성 또는 개발목표일정 압박감과 관련된다. 전자정부시스템관련 민간개발업자에 대한 의존은 문헌(Ewusi-Mensah, 1997; Keil, Cule, Lyytinen and Schmitt, 1998; Boehm, 1991; Bell & Zipparo, 2000; Tho, 2005)들에서도 자주 언급되고 있는 가능성일 뿐만 아니라, 실제로 감사원(2003)에 의해서도 지적된 주된 사항 중 하나이기도 하다. 또한 일정의 압박은 정보통신프로젝트를 비롯한 모든 공사나 프로젝트에서 일반적이다. 일정의 타당성 및 타당한 일정이 설정된 이후 프로젝트 수행에 있어서 이 일정의 준수는 프로젝트관리에 있어서 주된 성공요인 중 하나이다(Duncan, 1996). 이러한 점에서 시스템에 대한 불완전한 안전점검 및 정상작동점검은 프로젝트의 실패의 원인이 될 뿐 아니라 전자정부맥락에서의 주된 부패요인이 되기도 한다.

둘째, 제시된 전자부패 위험요인의 발생가능성의 고저가 위험요인 자체의 경중과 어느 정도 관련되어 있는지는 불명확하다. <그림 1> 및 <표 5>에서 발생가능성이 가장 높은 가능성5 및 가능성6 등의 위험요인들은 전자부패의 직접적인 위험요인이라기 보다는 제시된 다른 위험요인을 보다 가능하게 하거나 증폭시킬 수 있는 잠재적 위험요인일 개연성도 매우 높다. 예컨대, 제시된 위험요인 가운데 가능성4 또는 가능성10이 가능성5나 가능성6보다 위험요인으로서 더 중대할 수도 있다.

셋째, 이러한 점에서 본 발견사실은 '부패'라고 하는 '바람직하지 못한 현상'들에 대해 '전자정부사업을 담당하고 있는' 직간접적인 당사자들을 대상으로 한 인식조사가 지닌 한계점을 보여주는 것이기도 하다. <그림 1> 및 <표 5>에서 보듯이 이러한 발견사실은 몇 가지 측면으로 나누어 볼 수 있다. 하나는 본 조사에 응답한 공무원들이 전자부패의 위험요인을 공무원이나 민간계약자의 의식이나 행태가 아닌, 시스템의 보안에 대한 전문성의 결여 등에 두려는 인식이 강하다. 또 다른 하나는 전자부패가 잠재되어 있다면 그 위험요인은 공무원 자신보다는 시스템이나 민간업체에 있다는 인식이다. 그리고 전자정부의 맥락에서 일반적으로 이해되는 부패의 발생가능성은 낮다는 인식이다.

3. 군집별 전자부패 위험요인에 대한 인식차

<표 4>의 군집(I~IV)별 전자부패 위험요인에 대해 통계적으로 유의미한 차이를 보이는 것은 가능성4, 가능성7~가능성13 등이다(<표 6>).

이 가운데 가능성10(전자조달부문의 인증절차를 잘 알고 있는 내부직원이 전자조달시스템에 허위사업자를 만들어 입찰에 참여하고 내부정보를 이용하여 낙찰받을 가능성)의 경우 네 개의 군집 모두 통계적으로 매우 강한 유의미한 차이를 보이고 있다. 가능성10에 대해, IV(낮은 활용수준, 낮은 사이버문화신뢰), II(낮은 활용수준, 높은 사이버문화신뢰), III(높은 활용수준, 낮은 사이버문화신뢰), I(높은 활용수준, 높은 사이버문화신뢰) 순으로 높은 응답을 보여, 사이버문화에 대한 신뢰수준의 고하 보다는 정보통신기술 활용능력의 고저가 집단간 통계적으로 강한 유의미한 차이를 낳고 있다. 그러나

가능성 10은 <표 5>에서 보듯이 낮은 발생가능성(4.6%)을 보이고 있고 집단간 평균이 최대 2.13점에서 최소 1.51점으로 전 집단에 걸쳐서 발생할 가능성이 낮게 인식된다는 점에서 부패행위로서의 심각성에 대한 판단이 불가능한 상황에서는 집단별 차이가 큰 의미를 주지 못한다.

집단간 상대적으로 강한 통계적으로 유의미한 차이는 가능성8, 9, 11, 13에서도 발견된다. 가능성8(시스템의 인가코드나 취약성을 잘 알고 있는 IT 능력이 뛰어난 내부직원이 외부의 해커를 가장해 불법적으로 정보를 유출해 이익을 취할 가능성)의 경우는 군집I(높은 활용수준, 높은 사이버문화신뢰)과 타 군집간에 인식에 있어서 통계적으로 유의미한 차이(발생가능성인식 집단I < 집단II, III, IV)를 보이고 있다. 가능성9(시스템 공급업체 또는 업체의 직원이 정보시스템 내부에 '자신만이 아는 접근통로'(Back Door)를 만들어 놓고 공공정보를 유출하거나 변환할 수 있는 가능성), 그리고 가능성11(계약기간이 만료되어 퇴직한 계약직 근로자가 근무 당시 알고 있던 정보를 이용해 온라인상에서 접속권한이 있는 자로 활동하며 정보를 변조, 파괴할 수 있는 가능성)에서는 집단IV(낮은 활용수준, 낮은 사이버문화신뢰)와 타집단은 통계적으로 서로 상이한 인식(발생가능성인식 집단 IV > 집단 I, II, III)을 보였다. 가능성13(내부시스템에 대해 잘 알고 있는 직원이 의도를 가지고 외부인과 공모하여 외부로부터의 해킹, 위변조 등 공격을 유도할 수 있는 가능성)에 대해서는 집단I(높은 활용수준, 높은 사이버문화신뢰) 및 II(낮은 활용수준, 높은 사이버문화신뢰) 그리고 집단III(높은 활용수준, 낮은 사이버문화신뢰) 및 집단IV(낮은 활용수준, 낮은 사이버문화신뢰)는 서로 다른 인식(발생가능성 인식 집단I, II < 집단 III, IV)을 지닌 집단들임을 알 수 있다.

통계적 유의미한 차이는 가능성4, 가능성7, 가능성12에서도 발견된다. 가능성4의 경우 집단III과 집단IV이 집단I과 집단II 보다 발생가능성을 높게 인식하였고, 가능성7과 가능성12의 경우는 집단 III, IV가 집단I, II 보다 발생가능성을 높게 인식하였다.

<표 6>의 조사결과로부터 몇 가지 발견사실을 도출할 수 있을 것이다. 하나는 <표 5>에서 제시된 바대로 전자부패의 위험요인으로서 가장 가능성이 높은 것으로 인식된 가능성5와 가능성6에 대해서는 집단간에 통계적으로 유의미한 차이가 없다는 점에서, 이들 두 가능성은 사이버문화에 대한 신뢰수준이나 정보통신기술 활용수준에 무관하게 발생가능성이 높은 위험요인으로 간주할 수 있다.

둘째, 정보통신기술 활용수준과 사이버문화에 대한 신뢰수준 모두가 높을수록 전자부패 위험요소의 발생가능성을 낮게 인식하고 있는데 비해, 정보통신기술의 활용수준과 사이버문화에 대한 신뢰수준이 모두 낮을수록 전자부패 위험요소의 발생가능성을 낮게 인식하고 있다는 점이다. 전자부패 위험요인의 발생가능성을 감소 또는 예방하기 위해서는 정보통신기술 활용수준을 지속적으로 높이면서 아울러 사이버문화를 건전하게 확립하고 유지하는 것이 최선의 방안이라는 점이다.

<표 6> 전자부패 위험요인에 대한 집단별 인식차

변수	군집				ANOVA F-ratio
	I	II	III	IV	
가능성 1 : 동료의 패스워드를 알아내어 온라인상에서 불법행위를 저지를 가능성	2.0541 (37)	2.1429 (35)	2.0000 (31)	2.3239 (71)	1.727
가능성 2 : 조직 내 중요 자료를 암호화하여 E-mail로 외부의 이해관계인에게 유출할 가능성	2.1622 (37)	2.1143 (35)	2.5161 (31)	2.4085 (71)	1.761
가능성 3 : 중요 정보를 담당하는 직원이 휴대폰, PDA, 노트북 등의 무선 통신기능을 이용해 외부에 유통시킬 수 있는 가능성	2.1892 (37)	2.4571 (35)	2.5161 (31)	2.5211 (71)	1.175
가능성 4 : 급여를 관리하는 부서에 근무하는 직원이 모든 직원의 급여에서 눈에 띠지 않게 소액을 자신의 계좌로 빼돌릴 가능성	1.4324 (37)	1.4286 (35)	1.8387 (31)	1.7042 (71)	3.291*
가능성 5 : 시스템에 대한 안정성, 보안테스트 등을 시스템 개발회사에 맡길 가능성	3.1892 (37)	3.1429 (35)	3.2581 (31)	3.3239 (71)	0.400
가능성 6 : 최신 소프트웨어나 시스템을 도입함에 있어서 일정이 촉박하여 안정성을 제대로 검증(Beta Test)하지 못한 채 도입할 가능성	2.6216 (37)	2.4857 (35)	2.9355 (31)	2.9000 (70)	2.105
가능성 7 : 시스템의 유지, 관리업무를 정부로부터 위임받은 민간회사에 의해 공공 자료가 영리추구에 사용될 가능성	2.2432 (37)	2.3429 (35)	2.3871 (31)	2.7183 (71)	2.721*
가능성 8 : 시스템의 인가코드나 취약성을 잘 알고 있는 IT 능력이 뛰어난 내부직원이 외부의 해커를 가장해 불법적으로 정보를 유출해 이익을 취할 가능성	1.9189 (37)	2.2000 (35)	2.3548 (31)	2.5571 (71)	4.000**
가능성 9 : 시스템 공급업체 또는 업체의 직원이 정보시스템 내부에 '자신만이 아는 접근통로'(Back Door)를 만들어 놓고 공공정보를 유출하거나 변환할 수 있는 가능성	1.9167 (36)	2.1714 (35)	2.1290 (31)	2.5634 (71)	4.984**
가능성 10 : 전자조달부문의 인증절차를 잘 알고 있는 내부직원이 전자조달 시스템에 허위사업자를 만들어 입찰에 참여하고 내부정보를 이용하여 낙찰받을 가능성	1.5135 (37)	1.9143 (35)	1.7000 (30)	2.1286 (70)	5.765***
가능성 11 : 계약기간이 만료되어 퇴직한 계약직 근로자가 근무당시 알고 있던 정보를 이용해 온라인상에서 접속권한이 있는 자로 활동하며 정보를 변조, 파괴할 수 있는 가능성	1.7297 (37)	1.8000 (35)	2.000 (31)	2.2857 (70)	4.776**
가능성 12 : 공공의 목적으로 수집된 내부 정보가 시스템을 공급/관리하는 민간업체/직원에 의해 영리목적으로 사용될 가능성	1.9730 (37)	2.0857 (35)	2.1613 (31)	2.4507 (71)	2.918*
가능성 13 : 내부시스템에 대해 잘 알고 있는 직원이 의도를 가지고 외부인과 공모하여 외부로부터의 해킹, 위변조 등 공격을 유도할 수 있는 가능성	1.8649 (37)	2.0571 (35)	2.2581 (31)	2.4429 (70)	3.957**
가능성 14 : 업무가 분장되어 있음에도 어떤 직원이 자신의 담당업무 이외의 타업무까지도 정보기술을 이용해 부당하게 처리함으로써, 온라인상에서 분리되어 수행되어야 할 업무를 실제로는 한 사람이 수행할 가능성	1.9459 (37)	2.0571 (35)	2.2581 (31)	2.3803 (71)	2.511

*p<.05, **p<.01, ***p<.001

셋째, 정보통신기술 활용수준 보다는 사이버문화에 대한 신뢰수준의 정도가 전자부패 위험요소가 더 발생가능 한 것으로 보는데 영향을 미친다는 점이다. 전자부패의 발생가능성을 예방하기 위해서 정책적으로 초점을 두어야 할 점은 정보통신기술 활용수준의 향상 보다는 사이버문화에 대한 신뢰수준을 진작시켜 정보통신기술의 활용에 있어서 자기규율 할 수 있는 사이버문화를 확립하고 이를 지속적으로 관리하는 것이 필요하다는 점이다.

Ⅳ. 결론

본연구는 전자정부사업이 지속적으로 확대되면서 이에 수반한 역기능적인 현상들이 포착되기 시작하고 있는 시점에서 나타난 전자정부 논의의 괴리, 즉 기능적 관점의 논의에 대한 보완으로서 전자부패의 발생가능성을 살펴보고자 하였다. 전자부패가 가시화되어 있지 않고 잠재화 되어 있는 상황에서 전자정부사업과 직간접으로 관련된 공무원들의 인식을 토대로 하여 살펴 보았다. 공무원들의 인식은 행정직 대 전산직이나 국가공무원 대 지방공무원 등 제도적 신분의 차이에서 살피기 보다는(한국전산원, 2003), 정보통신기술활용능력 및 사이버문화신뢰수준이라는 변수를 사용하였다. 이러한 변수를 이용한 군집화를 통해, 전자부패 위험요인에 대한 군집간 인식차이를 밝히고자 공무원들에 대한 인식조사결과를 활용하였다.

본연구는 '스스로 꺼림칙한 사안'에 대한 회피적 응답, 또는 '스스로를 정당화하는' 응답에 따른 방법론상의 한계점을 노정하여, 응답자들이 전자부패 위험요인을 행태적인 측면 보다는 기술적 또는 전문지식적인 측면으로 전가하는 모습을 보였다. 또한 군집화를 위해 사용한 정보통신기술활용능력 및 사이버문화신뢰수준 역시 각변수에 대해 대체적으로 긍정적인 (즉 '높다' 그리고 '중간') 자기평가가 높게 나타나 사실상 각 변수에 대해 높다는 응답자와 낮다는 응답자간에 통계적으로 필요한 충분한 변이(variation)을 확보하지 못한 상태로 이루어졌다. 이러한 점에서 본연구는 탐색적인 의미가 더 짙다고 볼 수 있다.

그럼에도 본연구는 몇가지 흥미로운 발견사실을 통해 전자정부에 관한 연구에 있어서 관심을 환기시킬 수 있다고 생각된다. 하나는 전자정부사업의 추진에 있어서 정보시스템의 보안 및 안정성에 대해 정부기관이 스스로 관리할 수 있는 역량을 갖추어야 한다는 점이다. 정부가 이러한 역량을 갖추는 방법은 다양할 수 있다. 행정자치부 정부전산소(GCC)에 이를 위한 총괄적인 기능을 부여하거나 전자정부시스템 보안 Call Center로 활용하는 방법, 개별 행정기관 정보화담당관실 또는 전산실에 보안관련 1급기사를 최소한 1인 확보토록 하여 전담토록 하는 방법 등을 고려할 수 있다.

둘째, 전자정부시스템의 도입 시에 시험운영 이전에 안정성이나 보안관련 검증(Beta Test)이 완료되지 않은 경우 본격가동을 금지하는 제도적 장치를 강화할 필요가 있다. 아울러 시험운영이 전자정부시스템개발 프로젝트의 일정타당성(schedule feasibility)에 포함되는 사안이라는 점에서 검증이 일정내 이루어지지 못한 경우 개발업체에 강한 패널티를 부과하는 방법 역시 현실적으로 강화되어야 한다.

셋째, 공무원들의 정보통신기술 활용능력을 증진시키는 노력은 지속적으로 추진되어야 하지만, 이와 아울러 향후에는 공무원들의 사이버문화신뢰수준을 높일 수 있는 교육훈련이나 제도의 개발을 강화하여야 한다.

이론적으로는 공무원의 전자부패 위험요인의 발생가능성을 예측하고 진단하기 위한 각 측면의 연구가 지속적으로 확산되어야 한다. 부패는 개인과 조직의 문화 또는 윤리

적 측면에 의해 영향을 많이 받고, 또한 부패를 방지하기 위한 제도적 요인에 의해서도 영향을 받음은 물론이다. 사실 이러한 측면에서 오프라인 차원에서 많은 연구들이 이루어져 왔다. 그럼에도 전자정부의 맥락, 즉 정보통신기술이 행정의 전반의 분야에서 인프라로서 작동하는 맥락에서 전자부패의 위험요인에 대한 기술과 행정이 결함되는 부분에서의 지속적인 연구의 축적이 필요하다. 본연구를 통해 한가지 떠오르는 점은 전자부패의 위험요인의 발생가능성과 함께 위험요인별 부패로서의 심각성에 대한 개념적 그리고 경험적인 추후연구가 필요하다는 점이다. 전자부패 위험요인의 발생가능성과 심각성간에 관련성은 무엇인지? 심각한 부패란 어떤 것인지? 심각한 부패를 유발하는 요인은 어떤 것인지? 등에 대한 후속 연구가 필요하다.

참고문헌

감사원(2003). 「전자정부 구현사업 추진실태 감사결과」.

권해수. 2002. 전자정부를 통한 조달부패의 해결방안 연구. 한국부패학회보 6: 55-75.

김순희・김동환. 2001. “전자정부 추진에 내제된 딜레마,” 한국행정학회 동계학술대회 발표논문집, pp.741-58.

김영종. 1999. 정보부패의 패러다임 정립과 치유. 한국부패학회보 3: 25-40.

김영종. 2002. 가상공간(사이버)에서의 부패: 행정윤리적 접근. 한국부패학회보 6: 75-104.

김정덕 , 이성일. 2001. 정보기술 위험관리 과정과 기법. 정보보호학회지 1193): 16-23.

남궁근 외(2002).「전자정부를 통한 부패통제: 이론과 사례」, 경상대학교 사회과학연구소, 서울: 한울 아카데미.

명승환 최영훈. 2002. 디지털 사회와 행정의 투명성: 개념적 다면성과 연구과제. 한국행정학회 동계학술대회 발표논문집.

명승환·최영훈. 2005. 차세대 전자정부에 대한 인식: 주요광역시를 중심으로. 정보화정책 12(4): 131-149.

목진휴·명승환·윤태범. 2002. "전자정부를 통한 행정부패 감소방안: 정보통신기술(ICT)을 통한 레드테이프의 제거방안을 중심으로," 정보화정책, 9(3).

소홍렬. 1999. 사이버문화의 인간적 조건. 정보과학회지 17(8): 45-50.

송희준・최홍석. 2002. 전자정부사업의 투명성 제고효과: 현황과 전망. 한국정책학회 하계학술대회 발표논문집 pp.337-58.

여명숙. 1999. 사이버문화의 형이상학적 기초. 정보과학지 17(8): 4-15.

오강탁. 2002. 통합적 전자정부 발전모형에 따른 한국 전자정부의 수준진단과 향후 발전방향. 한국정책학회보. 12(1):

오강탁.이연우. 2005. 참여정부 전자정부수준과 향후 추진전략. 한국행정학회 하계학술대회 발표논문집. 29-48.

정익재외. kisa 보고서.

최영훈. 2003. 정보기술, 레드테이프 그리고 부패의 관계성: 업무분야를 중심으로 한 탐색적 고찰. 한국부패학회보 8(1): 147-173.

최영훈・명승환・이태영. 2003. “전자정부의 부패취약성에 관한 탐색적 고찰.” 사이버커뮤니케이션학보 11: 143-175.

최영훈외. 2005. 정보통신기술과 윤리. pp. 303-322. 정보통신윤리위원회 편저. 정보사회윤리학. 서울: 이한출판사.

최영훈외. 2006. 전자정부에 있어서의 행정윤리: 전자부패를 중심으로. 전자정부론. 서울: 대영문화사.

한국전산원. 2003. 전자부패의 존재양식과 대처방안에 관한 연구.

홍성태. 1999. 사이버문화: 개념, 특성, 이미지. 동향과전망(한국사회과학연구소). 43(11): 77-99.

Bac, M. 2001. Corruption, connections and transparency: Does a better screen imply a better scene? *Public Choice* 107: 87-96.

Bell, Christopher, and Lisa Zipparo. 2001. *Exploiting Eemerging Technology Corruptly in the NSW Public Sector*. p.25.

Boehm, Barry W. 1991. Software Risk Management: Principles and Practices. *IEEE Software* 8(1): 32-41.

Bragg, Steven M. 1998. *Outsourcing: A Guide to Selecting the Correct Business Unit, Negotiating the Contract, Maintaining Control of the Process*. New York: John Wiley & Sons.

Brown, Dan. 2005. *Digital Fortress* (한글번역본: 이창식 옮김. 베텔스만코리아).

Demchak, Chris C., Christian S. Friis and Todd M. La Porte(2000), "Webbing Governance: National Differences in Constructing the Face of Public Organizations," in G. David Garson, eds., *Handbook of Public Information Systems*, New York, Marcel Dekker Publishers.

Donovan, S., "Security of PCs in the Distributed Environment," *Computer & Security*, Vol. 12, No. 1, 1993, pp.28-31.

Duncan, W, 1996. *A Guide to the Project Management Body of Knowledge*, Upper Derby, PA: Project Management Institute, 1996.

Echeverr. J. 2003. Science, technology, and values: towards an axiological analysis of techno-scientific activity. *Technology in Society* 25 (2003) 205-215.

Ewusi-Mensah, Kweku. 1997. Critical Issues in Abandoned Information Systems Development Projects. *Communications of the ACM* 40(9): 74-80.

Garnham, H. 1994. What Ever Happened to the Information Society? pp. 42-51. in Management of Information and Communication Technologies: Emerging Patters of Control. London: Aslib,

Haque, Akhaque. 2003. GIS, Public Service and the Issue of Democratic Governance. *Public Administrative Review* 61(3): 259-265.

Heeks, Richard H. 1998. Information Technology and Public Sector Corruption. Information Systems for Public Sector Management Working Paper Series Paper No.4, Institute of Manchester, Precint Center, Manchester, M13 9GH, UK.

Heiddeger, Martin. 1977. The Question Concerning Technology. New York: Harper Colophon.

Hellstrom, Tomas. 2003. Systemic innovation and risk: technology assessment and the challenge of responsible innovation. Technology in Society 25: 369-384.

ICAC, 2001. *eCorruption Vulnerablities*. New South Wales.

ICAC, The Need to Know: eCorruption and Unmanaged Risk, 2001, p.5

Keil, Mark, Paul E. Cule, Kalle Lyytinen, and Roy C. Schmidt. 1998. A Framework for Identifying Software Project Risks. *Communications of the ACM* 41(11): 76-83.

Kuo, Feng-Yang, and Meng-Hsiang Hsu. 2001. Development and Validation of Ethical Computer Self-Efficacy Measure: The Case of Softlifting. *Journal of Business Ethics* 32(4): 299-315.

Lisa zipparo(2001), "exploiting emerging technology corruptly in the NSW public sector", emerging technology corruption strategic assessment.

Marshall, Kimball P. 1999. Has Technology Introduced New Ethical Problems? *Journal of Business Ethics* 19: 81-90.

Neumann, Peter G. 1999. The Challenges of Insider Misuse. Post-workshop version, 23 August 1999. Prepared for the Workshop on Preventing, Detecting, and Responding to Malicious Insider Misuse. 16-18 August 1999, at RAND, Santa Monica, CA. (http://www.csl.sri.com/users/neumann/pgn-misuse.html).

OECD Public Management Policy Brief, *The Hidden Threat to E-Government: Avoiding large government IT failures*, PUMA Policy Brief No.8., March 2001.

Ogburn, W. F. 1966, *Social Change with Regard to Cultural and Original Nature*, New York.

Perris, C. 2001. E-Governance: Do Digital Aids Make a Difference in Policy Making? in J. E. J. Prins. edited. *Designing E-Government: On the Crossroads of Technological Innoation and Institutional Change*. Hague, Netherland: Kluwer Law International.

Tho, Ian. 2005. *Managing the Risks of IT Outsourcing*. Netherlands: Elsevier Science & Technology Books.

UN. 2004. *Global E-Government Readiness Report*.

저자 약력 : 저자 최영훈은 미국 시라큐스대학교에서 정책학박사학위(논문: Partnering Government Laboratories with Industry: A Comparison of the United States and Japan, 1996)를 취득하고, 현재 광운대학교 행정학과 교수로 재직하고 있다. 관심분야는 과학기술 정책 및 과학기술계 연구기관 관리, 전자정부를 포함한 정보통신정책 및 관리, 행정이론 등이다. 주요 저서 및 논문으로는 Catharsis and Policymaking(2004) 등 다수가 있다. (cyhoon@kw.ac.kr).

저자 김석곤은 광운대학교 대학원 행정학과를 수료하고 행정학박사학위(논문: 지방재난관리의 조직간관계와 성과에 관한 연구, 2006)를 취득할 예정이다. 관심분야는 재난관리 및 성과평가임. 주요 저서 및 논문으로는 김대중정부의 정보정책 성과 평가(2006) 등이 있다.