

전자부패의 유형과 함의: 사례를 중심으로

E-Corruption: Cases and Implications

이태영(Lee, Tae-Young)* · 최영훈 (Choi, Younghoon)**

ABSTRACT

The authors strives a taxonomic approach in which e-corruptions can be analyzed rather than a conventional, behavioralistic approach in which the phenomena are examined in terms of perception-based survey results. In doing so, this study use a 2 x 2 matrix of e-corruption types, using two criteria of offenders' and supervisors' ability to use ICT. Using the resultant 4 types of e-corruptions, they provide theoretical and policy implications.

Key words : 전자부패(e-Corruption), 유형화(Typology), 사례연구(case study)

I. 들어가며

전자정부는 과연 우리사회의 부패를 감소시킬 수 있는가? 기존의 전자정부 관련 문헌들에서는 이를 긍정하는 논의들이 주류를 이루고 있다. 이러한 주장의 일관된 논거는 전자정부가 구현되면 부패발생의 조건들이 제약된다는 것이다. 예컨대 부패발생 요인으로서 부패행위에 대한 처벌의 크기, 부패행위가 발각될 확률, 부패행위가 처벌될 확률을 높임으로서 사전 또는 사후적으로 부패행위를 확인할 수 있게 된다는 것이다. 이와 더불어 부패가 발생하는 또 하나의 조건으로서 공무원과 민원인간의 대면 기회를 차단할 수 있다는 점을 들고 있다. 이러한 대면기회는 출신지역, 학교 등 특정 연고의 확인, 안면관계, 인사치레, 접대 등의 기회를 만들어 공적 업무를 사적 특혜관계로 전환시키는 역할을 하는데 전자정부의 구현으로 이러한 기회들을 원천적으로 차단시킬 수 있다는 것이다. 그 결과 투명성이 증진되고 부패가 제거 또는 저감될 것이라는 것이 긍정론의 논리이다.

그러나 최근 들어 전자정부가 반부패에 기여한다는 논리들을 재고케 하는 사례들이 제기되고 있다. 정보화의 영향은 민간의 영역에서 공공의 영역으로 그리고 사회적 차원에서 개인적 차원으로 범위와 차원을 넘나들며 급속하게 확대되고 있다. 전자정부에 관한 한 세계적 선도국임을 자부하는 우리의 입장에서 이론적 영역은 물론 실천적인 영

* 한국지역정보개발원 책임연구원

** 광운대학교 행정학과 교수

역에서 조차 이에 대한 별다른 논의가 이루어지지 않았다. 이러한 우리의 현실과는 대조적으로 국제기구 및 선진외국에서는 이미 이에 대한 위험성을 인식하고 구체적인 가이드라인도 제시되고 있다. OECD의 문건에서는 이러한 전자부패의 상황을 방치할 경우 전자화에 대한 희망(e-dreams)이 전 세계적인 악몽으로 변할 수 있음을 경고하고 있다(OECD, 2001).

전자정부가 추진된 지 10여 년이 되는 지금까지 정보화의 무한한 가능성과 성과에 관한 문헌들은 헤아릴 수 없을 정도로 많다. 이로 인해 전자부패의 존재에 대한 회의적인 시각도 존재한다. 그러나 현재 드러나고 있는 전자부패의 사례와 증거들은 논란의 여지를 잠재울 수 있을 만큼 다양하고 광범위하게 발생하고 있다.

이 연구는 지금까지 이룩한 우리나라 전자정부의 성과를 부정하거나 폄하하기 위한 이라기보다는 우리사회가 한 단계 진일보하기 위해 극복해야할 현안을 부패의 문제로 보고 이를 해결하기 위한 수단 중 하나가 정보화라는 대전제 속에서 출발한다. 지금까지 국가 정보화를 추진하는 과정 속에서 우리가 인식하지 못했던 새로운 위험요소를 발견하고 그것에 대한 이해와 논의를 촉발시키는 장을 제공하며 이를 통해 우리사회의 부패문제를 획기적으로 개선하기 위한 단초를 제공하고자 하는 것이다. 또한 전자정부라는 업무환경 속에서 새롭게 대두 될 수 있는 신종부패로서 전자부패를 소개하고 이것이 기존의 부패에 어떤 영향을 주고 어떤 결과로 나타날 것인지를 예측해 보고자 한다. 객관적인 연구수행을 위해 방송 및 각종 언론을 통해 이미 공개된 사건들의 구체적인 사례를 제시하며 이에 대한 원인과 대처방안을 모색하는데 초점을 맞추어 논의한다.

II. 이론적 논의

1. 전자부패의 개념 정의

전자부패(eCorruption)라는 용어는 전자정부가 등장하고 난 이후 소개된 최근의 개념이다. 이러한 이유로 전자부패의 개념에 대해서는 아직 합의된 정의가 존재하지 않는다. 전자부패의 개념을 협의의 관점에서 보아 부패수단의 변화에 초점을 맞추고 있는 시각에서는 “공적으로 위임받은 자 또는 기관이 사적인 이득을 추구하기 위하여 새로운 전자매체를 이용해 권한을 오용하는 행위”로 정의한다(Shadrach, 2003). 한편 광의의 관점에서 접근하는 시각(최영훈·명승환·이태영, 2003: 63)은 “전자정부의 저해요인으로 작용하는 특징적인 부패현상”으로 전자부패를 정의한 바 있다.

기존의 부패행위에 대한 개념정의들은 정보통신기술의 발전이라는 동태적인 환경에 적용하는데 일정한 한계를 지닌다. 최근의 연구들 중에는 정보통신기술과 부패의 관계를 구체적으로 규명해 보려는 시도들이 나타나고 있다. 예컨대 Heeks(1998, 1999a)는 기존의 부패연구와는 다른 정보화의 시각에서 부패의 문제를 다루고 있다. 호주 ICAC

에서 지속적인 관심을 쏟고 있는 전자부패 관련 연구 결과물들은 전자정부 사업을 실제로 운영하면서 드러나고 있는 문제점들을 체계적으로 정리해 실제 사례들을 제공함으로써 실무적인 시사점들을 제공하고 있다.

이 연구에서는 전자부패(eCorruption)의 개념을 “공공정보¹⁾에 접근할 수 있는 권한을 획득한 자가 공공의 목적으로 생성된 정보를 전자적인 조작 또는 생성함으로써 공공의 이익을 훼손하거나 사익을 추구하는 행위”로 정의하고자 한다.

2. 전자부패의 존재에 대한 추정

정보사회에서는 기술과잉으로 인한 삶의 가치나 의미의 상실, 감시체제의 발달로 인한 사생활침해, 정보 과적과 정보 빈곤, 기술관료의 부상에 따른 권력편중현상, 도시의 과잉성장 등 열거할 수 없을 정도로 많은 문제점들이 상존한다(Fennegan et al., 1987). 보다 시각을 좁혀 전자정부에 관한 세계 여러 나라들의 정부문건에서 그려지고 있듯이 여기에는 긍정적인 모습만이 있는 것이 아니라 위험스러운 모습도 동시에 지니고 있음을 지적하는 논의(황성돈·정충식, 2002: 1)들이 존재한다.

한 사회에 있어서 새로운 기술의 도입은 그 기술을 지원하는 많은 현실공간의 변화를 수반해야만 된다. 그러나 이러한 현실공간에 존재하는 기존의 기술 및 습관들은 그것의 관성으로 인해 새로운 기술을 지체시키는 경우가 많다. 즉 새로운 기술의 발전은 급속도로 이루어지지만 사람들이 그 기술을 사용하기 까지는 매우 오랜 시간이 소요된다(하영수, 2002: 258). 변화가 진행되고 있는 다양한 분야 중에서도 정보화에 대한 예견에는 극단적 예찬론에서 극단적 비판론에 이르는 폭넓은 시각들이 공존하고 있다.

그렇다면 전자부패가 과연 우리사회에 존재하는가? 또한 전자부패의 존재가 기존의 부패연구에 시사하는 점은 무엇이며 개념조차 생소한 이러한 현상을 전통적인 부패행위와 구분해야 할 실익이 있는지에 대한 논의가 선행되어야 할 것이다.

이에 대해 한세익(2003: 337)은 전자정부를 추진하는 과정 속에서 역기능적 편린들이 속출하고 있음을 지적하며 기존의 전자정부 정책에 관한 평가적 시각을 강조한다. 또한 명승환(2006: 100)은 전자정부가 구현되면 투명성이 제고된다는 인식이 확산되어 있음을 지적하며 투명성의 개념에 대한 결정론적 시각의 수정을 주장하고 있다. 이 연구의 주된 관심사인 전자부패의 개념과 사례는 이러한 결정론적 시각에 대한 대안으로서 이에 대한 이해의 폭을 넓혀 줄 수 있을 것으로 기대된다. 최영훈·김석곤(2006: 97)은 이론적으로 전자정부와 관련된 대부분의 문헌들이 정보통신기술의 ‘밝은’ 측면을 부각시키는데 편중되어 있으며 ‘어두운’ 측면은 논의자체가 제한되어 왔음을 지적한다. 이에

1) 여기서 ‘공공정보’는 공공의 이익을 목적으로 수집, 생성, 가공되어 온라인상에서 획득 가능한 모든 형태의 정보를 포함하는 것으로 이해한다. 이렇게 공공정보의 범위를 광의로 해석한 이유는 예측할 수 없을 만큼 빠르게 진보하는 정보통신기술의 변화와 이를 이용해 의식·무의식적으로 새로운 부패의 기회에 직면하게 될 잠재적 부패행위자들의 양태를 될 수 있으면 포괄적으로 다루기 위함이다.

대한 해결책으로 전자정부의 맥락에서 신종부패의 발생잠재성에 대한 경험적 연구의 필요성을 제기하고 있다.

이상의 논의를 출발점으로 급속하게 진행된 공공부문에서의 전자부패의 발생가능성을 전제로 개념적 구상과 사례를 통해 이론적·정책적 함의를 탐색해 보고자한다. 이를 위해 이 논문에 인용된 전자부패 관련 입증자료들은 언론 등을 통해 드러난 실제 발생 사례를 수집·분석하여 제시하였다.

III. 전자부패의 특성과 유형

1. 전자부패의 특성

1) 발생원인 측면의 전자부패 특성

전자부패가 발생하는 원인이 정보통신기술의 어떠한 특성에 기인하는 것이며 그것의 실태를 정확히 파악할 수 있다면 전자부패에 대한 최선의 대응방안을 모색할 수 있을 것이다. 발생원인 측면에서 바라본 정보통신기술의 특성들을 정리하여 제시해 보면 다음과 같다.

첫째, 자동화와 신속성을 들 수 있다. 전자정부시스템의 가장 큰 특징 중의 하나는 자동화된 시스템과 자료의 개방성에 있다. 기존의 일처리 방식과 비교해 볼 때 이는 많은 장점과 편리성을 제공한다. 그러나 부패행위자(또는 외부인과 공모한 내부직원)는 이들 자동화된 시스템에서의 절차상 허점을 이용한다. 이러한 행위에 대해 전통적인 감사나 부패적발장치들은 적절한 통제장치로서 역할을 하지 못하게 될 가능성이 크다(ICAC, 2001: 6). 또한 자동화에 대한 맹목적인 신뢰는 전자부패를 인식하지 못하게 하는 주된 원인을 제공하게 된다. 전자정부의 구현으로 인한 변화의 특징을 가장 단적으로 보여주는 것 중의 하나가 바로 전자상거래이다. 전자상거래의 핵심적 특성 중 하나가 거래의 발생 속도이다. 전자상거래는 실시간으로 이루어지며 구매자가 일단 어떤 제품을 구매하기로 의사결정을 하면 판매자는 온라인으로 즉시 결제를 받을 수 있다. 데이터의 조작력은 늘어나는 반면 그만큼 개인정보 및 외부에 유출되어서는 안 될 기밀 정보나 부패행위와 관련된 정보들이 남용될 수 있는 여지도 커지게 된다는 점이다.

둘째, 면대면접촉의 부재이다. 전자정부의 투명성 강화 효과를 주장하는 입장에서는 민원인과 공무원의 면대면 접촉의 기회를 차단함으로써 부패의 기회가 원천적으로 봉쇄된다고 주장한다. 그러나 전자정부를 통해 부패행위자에게도 편의가 제공된다. 이것이 전자부패와 관련된 신기술로서의 특성 중 하나로 이른바 RGEC(Commonwealth

2) 예컨대 온라인상에서의 업무감독이나 처리된 업무의 검토, 사용자 인증 등이 이에 해당된다.

Research Group into the Law Enforcement Implications of Electronic Commerce)에 의해 추가정보(collateral information)라고 명명되고 있는 정보의 손실이다. 여기서 추가정보란 과거 면대면 접촉에 있어서 거래당사자들 사이의 신뢰구축을 위해 필요한 일련의 정보를 일컫는다. 면대면 접촉이 기계 대 인간 혹은 기계 대 기계의 접촉으로 대체되면, 부패행위를 감시하는 자의 입장에서는 이러한 정보들을 더 이상 얻을 수 없게 된다는 점이다. 이러한 정보는 거래의 의도나 목적에서 필수적인 것은 아니지만 거래의 당사자들에게는 유용한 상황적 정보를 제공한다.

셋째, 시간과 공간의 극복을 들 수 있다. 정보와 같은 무형의 자산은 그 소유자가 알아채지 못하는 사이에 절취되거나 부패행위에 사용될 여지가 많아진다. 공공부문 업무현장에서는 직원들이 자신의 업무와 무관한 시스템에 쉽게 접근할 수 있음으로 인해서 부패행위가 발생할 수 있다.³⁾

넷째, 은폐의 용이성을 들 수 있다. 이는 정보통신기술의 발전과 더불어 진보를 거듭하고 있는 암호화 기술과 관련된다. 암호화는 법집행 기관(또는 수사기관)이 증거에 접근하는 것을 결정적으로 방해할 가능성을 지닌다. 부패행위자들은 이를 통해 법적인 개입 없이 서로 정보를 주고받을 수 있으며 수색이나 압류 등이 어려운 문서를 만들 수 있는 수단을 제공한다. 암호화 수단은 탈세, 돈 세탁, 스파이활동, 불법자료의 저장 등 다양한 형태의 부패행위를 예방하거나 색출해내는데 심각한 장애요인으로 작용할 수 있다. 전자적으로 처리된 불법정보의 블랙마켓이 생겨날 수 있으며 이곳에서 내부자는 대가를 받고 이해관계자에게 민감한 정보를 유출할 수 있다. 또한 부패행위를 입증하는데 있어서 중요한 증거들이 조사를 회피하거나 증거를 은폐하기 위한 목적으로 암호화⁴⁾될 가능성이 있으며 또 다른 법적증거인 부패행위 당사자 간의 통화 내용 등도 역시 그들이 사용한 암호화기법으로 인해 해독 불가능한 경우가 생길 수 있다. 공적자료의 암호화로 인한 전자부패의 문제는 크게 이슈화되고 있지는 않지만 부패를 적발해야 하는 담당기관들로서는 심각한 위협에 처할 수 있다.

마지막으로 새로운 지대추구영역의 제공을 들 수 있다. 전자정부 서비스를 제공받는 시민들 중에는 새로운 행정서비스에 빠르게 적응하고 편리함을 향유하는 집단과 이러

3) 관련된 외국사례로 직원 채용 시 한 계약직 직원은 자신 역시 지원자이면서 채용과 관련한 내부정보를 담은 디스켓을 소유하고 있었다. 구체적으로 그 디스켓에는 면접 시 질문과 답안을 포함하고 있었다. 이와 유사한 사건은 우리나라의 일선 지방자치단체에서 발생한 적이 있다. 청탁도 아니고 뇌물을 쓰지도 않았지만 인사담당자가 자기 점수를 높게 매겨 승진하는 '철면피형' 인사비리가 새롭게 등장했다. 서울시 마포구 인사담당자는 지난해 자신과 승진 경쟁을 벌이고 있는 직원의 근무성적평정 순위를 자신보다 후순위로 조작해 동료를 제치고 먼저 승진하는데 성공했다. 서울 강서구 모 국장도 지난해 반영시기가 도래하지 않은 최근 근무성적 점수를 임의로 적용해 지방서기관으로 부당하게 승진하기도 했다(동아일보 2005년 2월 16일).

4) 이와 관련된 사례로 호주의 NSW의 공무원들이 사무실에서 암호화된 아동 포르노 사진을 교환하고 다운로드 함으로써 인터넷을 오용한 경우를 들 수 있다. 몇몇 자료나 이미지의 제목은 비 암호화된 형태였지만 어린이의 포르노 사진으로 추측되는 데이터의 상당부분은 암호화되어 그 것의 해독에 많은 시간이 소요된 사례가 보고된 바 있다.

한 환경에 익숙하지 못하여 새로운 행정서비스를 제공받는 것이 어렵거나 불가능한 집단이 있게 된다. 후자의 경우 전자정부 서비스는 복잡하고 번거로우며 난해한 일이 될 것이다. 이런 집단에 대해 공무원이 전자정부서비스를 전달 또는 매개하는 역할을 하는 과정에서 일부 공무원들은 행정적 편의 혹은 행정서비스의 복잡성을 해결해 주는 대가로 뇌물을 받을 수 있는 여지가 생기게 된다. 다른 한편 전자정부서비스를 시민들에게 제공하는 공무원들의 입장에서 전문성을 갖춘 사람과 그렇지 못한 사람이 존재할 수 있다. 이 경우에도 새로운 지대추구의 영역이 발생할 가능성이 존재한다. 이른바 정보격차로 인해 초래 되는 투명성에 대한 위협은 공무원들이 복잡한 행정서비스의 중간 매개 역할을 충에 의한 심각한 부패의 개연성을 내포하고 있다.

2) 발생규모 및 영역 측면의 전자부패 특성

민간부문을 포함한 우리사회 전반의 상황을 놓고 볼 때 온라인 조직문화의 문제점으로 인한 부패의 정도는 이미 심각한 수준에 도달했다⁵⁾. 대부분의 정부기관이나 기업들이 대외적인 신뢰도를 고려하여 외부에 발표하지 않거나 피해 사실조차 모르는 경우가 많은 점을 감안하면 그 심각성은 더욱 커질 것으로 예상된다. 이에 대한 논리적 추정을 위해 기존의 모형 중 적절한 대상을 선정하는 것이 필요하다.

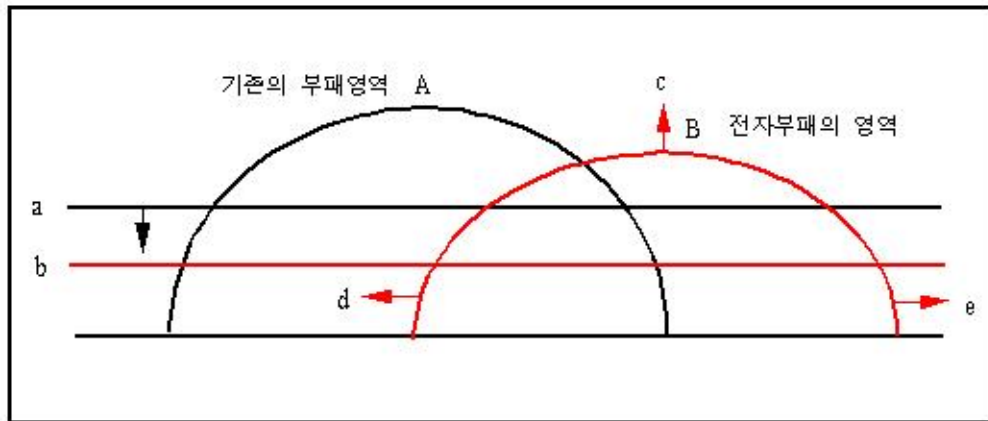
전통적인 부패의 규모를 추정하는데 주로 이용되는 모형 중 하나로 빙산(Iceberg)모형을 들 수 있다. 이모형의 수정 및 응용을 통해 전자부패의 논리적 영역을 확인하고 잠재된 위험의 규모를 추정하는데 도움을 얻을 수 있다. 기존 모형으로부터 얻을 수 있는 시사점은 공식적인 신문보도 등을 통해 드러나는 부패가 실제 발생 건수에 비해 극히 적다는 점이다. 이러한 시사점은 이 연구에서도 그대로 적용될 수 있다.

기존의 전자정부 논의에서 주장되어온 투명성 강화의 논리는 아래에 제시된 모형에서 정보화로 인한 긍정적인 효과를 일방적으로 부각시킨 것에 불과하다. 이는 전자정부로 인해 변화될 환경과 관련하여 정보화의 다양한 특성들을 반영하지 못하고 있다는 점에서 한계가 있다. 즉 기존의 부패행위에 대한 인식으로는 감지할 수 없는 새로운 유형의 부패가 발생할 가능성을 전혀 설명할 수 없다는 점이다. 정보화는 긍정적인 측면에서 볼 때 현실세계에서 상상할 수 없었던 다양한 편익을 구현하고 있다. 이를 반대로 생각하면 정보화의 부정적 측면도 예측할 수 없는 영역에서 발생할 것이라는 추론이 가능하다. 이 연구에서는 이와 같은 전자부패의 영역이 기존의 인식으로 감지할 수 없는 새로운 정보화 영역에서 발생할 것이라는 점을 감안하여 기존의 빙산모형을 수정한 것이 【그림 1】이다. 이러한 작업을 통해 전자부패의 발생가능성과 영향을 추정해 보고

5) 실례로 우리나라에서 발생한 증권사의 사이버계좌 도용사건은 내부공모자의 결탁여부에 관심이 집중된 바 있다. 사이버 증권거래는 1997년 말 국내에 처음 도입되었다. 98년 사이버거래 비중은 전체의 1.9%에 불과했지만, 99년 19.0%, 2000년 46.6%, 2001년 52.3%로 폭발적인 증가세를 보였다(이에 대한 상세한 내용은 한국일보, 2002년 8월 27일자 33면 참조).

각 영역별 특성에 따른 논의의 필요성을 제기할 수 있을 것이다.

【그림 1】 전자부패(e-corruption)의 발생영역과 규모의 추정⁶⁾



a: 기존의 부패수준 b: 전자정부의 부패수준 c: 전자부패의 적발가능성
d: 기존 부패의 전자부패로의 전이가능성 e: 전자부패의 확대 가능성

출처: 최영훈·명승환·이태영 (2003: 80).

첫 번째는 기존의 인식을 반영한 것으로 전자정부 환경에서 기대되는 부패방지 효과이다. 이는 【그림 1】의 부패의 적발률을 나타내는 선 a에서 b로의 변화로 표시할 수 있다. 전자정부 환경에서 새롭게 도입되는 정보통신기술은 기존의 방법으로 적발하지 못했던 다양한 부패행위들을 효율적으로 적발할 수 있게 됨을 의미한다. 전자정부에서의 부패방지 효과에 대한 긍정론자들에 의하면 이는 업무의 투명성 강화 내지 자동화 등의 기능으로 인한 심리적 위축 효과로도 설명된다. 즉 부패행위자들은 정보통신기술로 인해 적발가능성이 높아짐으로서 부패행위의 기회 자체가 축소된다는 것이다. 그러나 이러한 효과는 전자정부에서 부패통제 효과를 주장하는 학자들 사이에서도 회의적인 견해가 적지 않다. 왜냐하면 이러한 효과를 거두기 위해서는 제도적 보완과 정보통신 윤리의 강화 등 부패방지를 위한 부수적인 조건들이 갖추어져야 하기 때문이다.

두 번째는 정보통신기술이 가져다주는 편의의 이면에 존재하는 위험요인을 고려하여 새로운 부패의 영역을 표시한 것이다. 새롭게 등장하게 될 부패의 영역은 위의 【그림 1】에서 B의 영역으로 표시할 수 있다. 이 영역은 혁명적인 변화를 주도하고 있는 정보통신기술이 지금까지 인식하지 못했던 신종부패를 유발하는 원인으로 작용하고 있음을 의미한다. 이는 부패가 각 사회가 처한 특수성을 반영하는 사회문화 체계의 하위요인이라는 속성과 정보통신기술로 인한 변화가 긍정적인 변화이외에 부패에도 그대로 반영될 것이라는 전제이다. 그림에서 A와 B의 영역이 중첩되는 부분과 온전히 B의 영역만으로 표시되는 부분이 존재한다. 먼저 A와 B가 중첩되는 영역은 기존의 전통적인

6) 수정된 Iceberg 모형은 최영훈·명승환·이태영(2003)에 의해 수행된 한국전산원 연구과제에서 필자가 고안한 것이다.

부패행위들이 정보통신기술의 특성들을 부패행위에 적용하는 경우이다. 이 경우 부패행위 자체는 기존의 형태를 유지하면서 수단이 첨단화하는 경우라고 할 수 있다. 예컨대 기존의 뇌물이나 상납, 횡령 등의 전통적 형태가 다양한 가치저장수단 즉 사이버머니나 게임머니 등을 활용해 적발가능성을 현저히 낮추거나 부패행위의 입증자료를 더욱 용이하게 은폐하는 경우이다. 이런 상황을 가정한다면 통제자의 입장에서는 정보통신기술을 활용해 적발을 제고하려 할 것이고 부패행위자의 입장에서는 부패행위를 기회를 확대내지는 보다 안전하게 실행하고자 할 것이다. 이러한 측면에서 양자의 상호간 의지는 충돌하게 된다. 즉 【그림 1】에서 통제자의 입장에서는 a에서 b로의 영역을 확장시킴으로써 부패적발 내지 예방의 효과를 극대화하고자 할 것이고 부패행위자의 입장에서는 d의 방향으로 영역을 확장시킴으로서 안전한 부패행위를 보장받거나 은폐를 용이하게 하는 효과를 극대화 하고자 할 것이다. 다음으로 【그림 1】을 통해 상정해 볼 수 있는 것은 순수하게 B만의 영역이 확대될 가능성이다. 이는 기존의 인식으로는 적발할 수 없는 새로운 부패의 특성을 나타낸다. 즉 부패행위자의 입장에서 새로운 기회의 발생이자 새로운 사익추구 영역이 되는 셈이다. 이러한 상황 하에서는 앞서의 경우처럼 통제자와 행위자 사이에 충돌관계는 형성되지 않는다. 따라서 부패행위자는 아무런 제약 없이 목표로 하는 부당한 사적이익을 안전하게 취할 수 있게 된다. 이에 대한 확대가능성을 표시한 것이 【그림 1】에서 e방향으로의 변화이다. 단 이러한 가정은 통제자보다 부패행위자의 능력이 현격한 차이를 보여야 한다는 전제조건을 충족시킬 때 이다. 즉 통제자와 행위자간의 정보격차(digital divide)가 크면 클수록 새로운 전자부패의 영역은 e의 방향으로 그 영역을 확대시켜 나갈 것이다.

이 연구는 이상에서의 전제조건을 토대로 전자부패를 이해하고 이를 실증적으로 접근하기 위해 사례분석을 시도함으로써 기존의 인식으로 감지할 수 없었던 전자부패에 관한 논의를 전개해 보고자 한다.

2. 전자부패 유형

전자부패의 개념적 유형분류에는 다양한 분류기준이 있을 수 있다. 이 연구에서는 감시받는 자와 감시하는 자의 시각을 유형분류의 거시적 차원으로 삼고자 한다. 이를 전자정부환경 속에서 일어난 전자부패 상황에 적용시키게 되면 감시받는 자는 부패행위자이며 반대로 감시하는 자는 정부 또는 조직이 될 것이다. 이러한 구분을 보다 구체화하여 보면 먼저 전자부패의 핵심적인 구성요소인 ICT라는 기술적 요소를 부패행위자의 능력에 적용해 하나의 차원을 구성한다. 또한 이러한 부패행위를 예측하고 적발해야 하는 감시자의 능력을 또 다른 구성차원으로 하여 유형분류의 기준으로 삼고자 한다. 즉 ‘행위자의 ICT 활용도’라는 차원에서 ICT의 활용능력을 그리고 부패의 ‘통제자의 인식도’라는 차원에서 부패의 통제능력을 분류기준으로 삼아 전자부패를 유형화하고자 한다. 이를 보다 쉽게 이해하기 위하여 【그림 2】와 같이 제시하였다.

【그림 2】 사례의 유형화를 위한 개념적 유형

		행위자의 ICT활용도	
		낮다	높다
통제자의 인식도	낮다	제1유형: 무지형	제2유형: 기술형
	높다	제3유형: 방임형	제4유형: 해커형

각 유형으로 분류된 전자부패의 개념에 대한 특징과 개념적으로 분류된 각 유형들이 나타낼 것으로 특성들을 서술해 보면 다음과 같다.

1) 제1유형: 무지형 전자부패

이 유형은 통제자의 입장에서 부패행위에 대한 통제인식이 낮고 행위자의 입장에서 낮은 수준의 ICT활용도를 지닌 상황에서 발생할 수 있는 전자부패의 유형이다. 이러한 전자부패의 유형은 정보통신기술이 도입되는 초기단계에 발생할 수 있는 부패의 전형으로 여겨진다. 전자부패의 행위자가 부패행위를 하는데 있어서 특별한 ICT능력을 필요로 하지 않는다는 점은 행위자의 입장에서 이러한 행위를 심각하게 고려하지 않고 있음을 특징으로 한다. 이 유형의 대표적인 사례는 다음과 같다.

검찰청 일용직원이 컴퓨터 범죄 수사를 보조하면서 취득한 수만 명의 개인 신상정보를 인터넷을 통해 팔아오다 달미를 잡혔다.

서울지검 컴퓨터수사부(부장 이창제)는 17일 2만6천여 명의 신용카드 정보 등을 돈을 받고 판매한 혐의(신용정보의 이용 및 보호에 관한 법률 위반)로 같은 부서 소속 일용직 공무원 이 아무개(28)씨를 구속했다.

이씨는 지난 8월부터 최근까지 서울 방이동 집 근처 피시방 등에서 검찰 수사업무를 보조하면서 수집한 2만6679명의 이름과 주민등록번호, 신용카드 정보 등을 12차례에 걸쳐 이메일과 패신저 등을 이용해 민 아무개씨 등에게 넘기고 모두 302만원을 받은 혐의를 사고 있다. 이 씨는 이 가운데 116명의 것은 검찰 수사 자료에 기재된 신용카드 비밀번호 앞 두 자리를 카드 소유자의 생년월일, 전화번호 등과 비교하고 인터넷 신용카드 조회 서비스로 확인하는 방법으로 네 자리 번호를 모두 알아낸 뒤 판매한 것으로 밝혀졌다(이하 생략).

자료: 한겨레 2003년 10월 17일자

통제자 역시 이러한 행위의 심각성에 대한 인식이 없는 상황이 결합할 때 발생할 수 있다. 또한 이러한 유형은 Heeks가 주장하는 정보화 수용단계의 무지(ignore)단계에 나

타나는 현상과 일치한다. 이러한 유형의 전자부패가 지니는 일반적인 공통점은 자료의 위·변조나 삭제의 행태를 보인다고 보다는 단순한 정보의 유출을 통해 사익을 추구하는 유형이다. 비록 단순한 정보유출이라 할지라도 반복적인 복제가능성, 정보유통의 신속성, 유출된 자료의 영구성 등의 정보화 특성들로 인한 파급효과는 기존의 부패와 비교해 볼 때 커다란 차이점을 지닌다. 이러한 유형의 전자부패에 대한 핵심적인 특징들을 요약 정리해 보면 다음과 같다.

- 통제자의 측면에서 부패발생에 대한 위기의식이 존재하지 않고 부패행위자 역시 특별한 ICT능력 없이 정보를 유출할 수 있는 유형이다. 또한 조직차원의 부패통제 의식이 낮은 상황에서 잠재적인 부패 행위자들은 우연히 정보를 습득하게 될 개연성이 높다. 이러한 유형은 특별한 의도 없이 잠재적인 부패 행위자를 양산할 수 있다는 면에서 사안의 심각성이 있다.
- 이 유형은 업무관리나 업무분장의 측면에서 조직적 체계가 잘 갖추어진 대규모 조직보다는 이에 대한 대처가 미비하고 인력이 충분치 않은 소규모 조직 또는 자체적인 운영규정을 가지고 있는 독립적 조직에서 발생하는 특성을 나타낸다.
- 시기상 정보시스템이 보급되는 초기단계에 나타날 수 있는 유형이며 지리적 위치상 중앙의 통제가 비교적 덜 미치는 원격지 조직이나 업무처리 기준이 아직 갖추어지기 이전의 신설조직에서 발생할 수 있는 유형이다.
- 이 유형은 부패 행위자의 ICT능력이 아직은 낮은 단계라는 점에서 부패행위 통제자 차원의 인식확대와 시스템 보안의 강화 등 일반적인 수준의 통제기제로도 예방효과를 기대할 수 있다.
- 이러한 유형에 속하는 전자부패의 행위자는 공식적인 권한을 가진 직원일 수도 있지만 통제자의 통제능력이 낮은 상황을 이용하려는 권한을 갖추지 않은 물리적 내부자에 의해서도 전자부패가 발생할 것으로 예상된다. 여기서의 물리적 내부자는 권한이 없는 동료직원이 될 수도 있으며 사무실을 방문한 공무원의 가족이 될 수도 있다.

2) 제2유형: 기술형

이 유형은 전자부패가 발생할 수 있는 영역들 중 전혀 새로운 영역에서 발생하는 특징을 나타낸다. 부패행위 통제자의 입장에서는 전자부패가 발생하여 막대한 손실을 입고 있음에도 불구하고 그러한 사실조사 인지하지 못하는 경우이다. 이런 경우 법적, 제

도적 미비로 인해 부패행위자를 적발했다 하더라도 처벌근거 마련되지 않아 적절한 조치를 취할 수 없는 경우가 발생할 수 있다. 이런 유형의 대표적인 사례는 다음과 같다.

전라남도 전자입찰시스템을 통한 입찰과정에서 건설업자·담당공무원과 입찰시스템을 개발한 업체 등에 의해 250억 원대의 부정 낙찰이 발생한 것으로 밝혀졌다. 전자입찰은 관급공사에서 제기된 담합·예정가 유출 등 각종 불법행위를 방지하기 위해 입찰부터 개찰까지 전 과정을 컴퓨터시스템에 의해 자동으로 진행하는 것으로 전자입찰 부정사건은 이번이 처음이다(중략). 이 시스템의 개발자인 이 모 씨 등은 전자입찰시스템 내부의 파일만 바꾸면 간단히 이미 응찰한 입찰금액을 비웠을 수 있는 점을 악용, 유지보수 업자와 짜고 낙찰받기 원하는 건설업체들을 상대로 대가를 받고 낙찰 받게 해준 혐의를 받고 있다. 이들은 이 같은 방법으로 지난해 11월부터 올 8월까지 총 21건에 대해 250억 원 상당의 공사를 부정 낙찰 받았다고 사이버테러대응센터는 밝혔다.

자료: 전자신문 2002년 10월 15일자

이 경우 잠재적인 부패행위자는 숙련된 ICT능력을 이용해 사적이익을 취할 수 있는 허점들을 보다 쉽게 찾아 낼 것이다. 이러한 유형의 전자부패는 부패행위자와 통제자 사이에 정보격차에 기인한 것이라고 볼 수 있다. 즉 부패 행위자의 능력이 통제자의 통제능력에 비해 압도적으로 우월한 상황에서 발생한다. 부패행위 통제자는 부패행위자의 행동을 바라볼 수 없고 부패행위자는 통제자의 동향을 낱낱이 파악할 수 있는 여건이 조성된 것이다. 마치 집 주인이 집을 비우고 없다는 것을 알고 침입한 도둑과 같이 부패행위자는 마음먹은 대로 자신의 사익을 추구하는 형태이다. 이러한 유형의 전자부패에서 예상되는 특성들을 정리해 보면 다음과 같다.

- 이 유형은 부패 행위자의 입장에서 고도의 ICT능력이 요구되며 자료의 단순 유출을 벗어나 주로 자료의 위·변조, 삭제 등 사익을 추구하기 위해 보다 적극적인 조작기법이 동원된다.
- 이 유형은 통제자와 행위자 사이의 정보격차가 전자부패 발생의 원인을 제공하는 경우이다. 즉 전자부패의 행위자는 통제자의 통제력을 압도하는 우월한 ICT능력을 보유하고 있는 경우이다. 조직의 낮은 부패통제력은 부패행위자의 입장에서 볼 때 새로운 부패의 사업모형을 제공해 주는 역할을 하게 된다.
- 이 유형은 힘의 균형이 부패행위자에 기울어진 상황으로 설명되어질 수 있다. 예컨대, 통제자와 행위자 사이에 심각한 정보 비대칭이 존재하는 경우이다. 행위자는 통제자의 모든 활동을 세밀하게 파악할 수 있고 통제자는 부패행위자의 활동을 전혀 통제할 수 없는 상황에서 발생한다. 이 경우 통제자는 전자부패가 발생한 이후에도 그것의 규모와 심각성에 대한 인식은 물론 전자부패의 발생 사실조차도 인식하지 못한다.

- 이러한 유형의 전자부패는 부패행위자들 간의 공조가 깨지거나 이해관계자의 고발이나 제보 등 제도적 필터과정을 거치지 않고 행위자들 간의 불화 또는 우연한 기회에 노출되는 경우이다. 이는 통제자의 의도적인 노력에 의해 부패행위가 발각되는 것이 아닌 공범에 의한 제보나 경쟁업체의 신고 등에 의해 노출된다는 점에서 사안의 심각성이 있다.
- 행위자 측면에서 이러한 유형의 전자부패는 ICT능력에 있어서 독점적인 권한을 행사할 수 있는 공무원이나 전문성을 가진 프로그래머 등에 의해 저질러지는 특성을 보인다. 한 사람이 특정 정보에 대한 독점적인 권한을 행사할 수 있으며 동시에 시스템에 대한 감시·감독 기능을 가지는 경우 문제의 심각성을 더한다. 즉, 권한의 행사와 통제권의 행사라고 하는 두 조건을 동시에 충족하는 경우이다. 이 유형의 전자부패는 정보화의 특성인 신속성과 복제성을 이용하여 부패행위에 대한 적발가능성을 현저히 약화시킨다.

3) 제3유형: 방임형

이 유형은 전통적인 부패의 영역과 새로운 부패유형이 중첩되는 영역에 존재한다. 즉 정보화 도입 이전부터 이권개입, 청탁, 뇌물 등 부패행위가 발생하던 영역에서 정보화를 수단으로 이용하는 것이다.⁷⁾ 따라서 부패행위 통제자의 입장에서는 사전에 부패 발생 가능성을 인지하고 있는 경우가 대부분이며 적절한 조치를 취하지 않음으로서 발생하는 특성을 보인다. 부패행위 발생가능성의 인식 하에 통제기능이 정상적으로 작동된다면 이러한 유형의 전자부패는 예방내지 차단할 수 있다. 더구나 부패행위자의 ICT 활용도가 낮은 상황임을 고려하면 이러한 유형의 전자부패가 발생한다는 것은 매우 모순된 현상이다. 그러나 대부분의 부정부패가 모순된 상황 속에서 발생한다는 점에서 발생 가능한 전자부패의 유형이다. 이러한 유형의 전자부패는 부패행위자의 입장에서 1유형의 전자부패 유형에서와 마찬가지로 낮은 수준의 ICT능력을 이용한다. 이는 통제자의 암묵적 방조내지 조직적 공모를 통한 부패행위인 경우에 해당된다. 이러한 유형의 대표적인 사례를 제시하면 다음과 같다.

구청에서 지방세 부과업무를 담당하는 세무공무원이 수억 원의 세금을 부당하게 깎아주고 뇌물을 챙겨오다 경찰에 적발됐다.

서울지방경찰청은 세금삭감 청탁을 받고 세무종합전산망을 조작해 부과된 세금을 취소·감액해준 종로구청 세무과 7급 공무원 김모씨(48세)를 공전자기록변작 및 뇌물수수혐의로 구속했다고 15일 밝혔다. 경찰조사결과 취득세 등의 부과업무를 담당하는 김씨는 지난 2005년부터 11명의 납세자에게 부과된 3억7600만원을 취소·감액해줌으로써 그 중 3억4140

7) 이에 대한 구분의 실익을 따지는 견해도 있을 수 있다. 하지만 정보화의 발달과 함께 하루가 다르게 등장하는 가치저장 수단(사이버머니, T-money 등)들이 사익추구의 대상이 될 수 있는지에 대한 법·제도적 판단은 그렇게 단순하지 않은 것이 현실이다.

만원을 징수 받지 못하게 하고, 그 대가로 5명으로부터 3900만원의 뇌물을 수수한 것으로 드러났다. 또한 그는 지난해 10월 납세자 최모씨(46세) 등 4명으로부터 세금 삭감청탁을 받고, 같은 방법으로 세무종합전산망에 접속해 18차례에 걸쳐 취득세 등 3억1800만원을 깎아준 것으로 밝혀졌다. 경찰 관계자는 “같은 구청내 세무과 직원이라면 누구든지 현재의 세무종합전산망 프로그램에 자신의 ID를 이용, 얼마든지 열람하고 수정할 수 있다는 점을 악용한 범죄”라며 “현재의 세무종합프로그램상의 문제점을 보완할 필요가 있다”고 말했다.

자료: 조세일보 2007년 4월 15일자

이러한 유형의 전자부패는 주로 단순정보 유출의 형태를 띠며 획득한 정보를 외부에 거래하는 형태로 나타난다. 이는 마치 상품을 개발해 판매수익을 얻어야 할 기업이 판촉을 위해 경품행사를 하는 것과 마찬가지로의 상황이다. 즉 구매의도가 없는 고객에게 무료로 상품을 제공하는 격이다. 통제자의 입장에서 부패행위에 대한 통제가능성이 높다는 점은 기존의 영역에서 이미 부패행위가 발생한 영역이라는 점을 의미하는 것이기도 하다. 이는 전통적인 영역에서의 부패행위가 전자부패로 쉽게 전환될 수 있다는 점에 문제의 심각성이 있다. 다음에 서술하는 전자부패의 상황들은 모두 이러한 유형의 전자부패가 나타나게 될 형태들을 제시한 것이다.

- 전통적인 부패 취약영역에 자동화된 시스템을 적절한 검증절차 없이 수용하고, 전적으로 이에 의존하는 경우이다. 즉 기존에 부패가 자주 발생하던 영역의 조직에서 전자정부시스템을 도입한 후 추가적인 검증과정 없이 시스템상의 업무처리 결과를 지나치게 신뢰하여 후속적인 검증 작업을 게을리 하는 경우를 예로 들 수 있다. 이는 자동화에 대한 맹목적인 신뢰가 원인이 되어 나타날 수 있는 형태이다. 전자정부의 도입으로 기존의 부패가 자동적으로 소멸된다는 기대 하에 기존의 부패행위에 대한 점검과 정보화로 인한 변화양상을 점검하지 못했을 때 발생한다.
- 자신의 로그인 패스워드를 업무 편의상 다른 직원에게 알려 주거나 자신의 패스워드나 인증장치를 외부인 등이 이용할 수 있도록 방임하는 경우 발생할 수 있는 유형이다. 이러한 유형은 패스워드 도용사고 등의 결과로 나타나기도 하고 조직적인 차원에서 부패행위를 소극적으로 묵인하거나 적극적으로 이를 조장하는 형태로도 나타날 수 있다.
- 이러한 유형의 전자부패가 발생할 수 있는 영역은 전통적인 부패 취약영역으로 분류된 영역들이 해당할 것이다. 또한 이러한 유형의 전자부패가 공통적으로 가지게 되는 특성은 정보통신기술의 특성을 이용하여 기존에 존재해 온 부패행위를 더욱 용이하게 하거나 신속하게 수행함으로써 적발가능성을 낮춘다는 점이다. 그리고 부패행위자의 측면에서 권한을 가진 내부직원에 의한 경우가 대부분이다.

전자부패의 행위자는 주로 독점적이거나 전문적인 ICT능력 없이 반복된 업무를 통해 체득한 간단한 키보드 조작 또는 기록의 고의적 누락/수정/취소 등의 권한을 행사하게 되며 행위자는 이를 통해 금전적 이득을 추구하는 상황을 가정해 볼 수 있다. 이러한 유형은 주로 민원처리(street level)담당자의 업무영역에서 주로 발생한다. 기존의 논의에서는 일명 송사리 부패(petty corruption)로 칭하기도 하지만 이러한 유형의 부패가 정보통신기술과 결합될 때 동시성으로 인한 피해의 규모는 기존의 부패와는 비교할 수 없을 정도로 심각해 질 수 있다.

4) 제4유형: 헤커형

이 유형은 제시된 두 개의 차원 중 부패 행위자의 능력과 통제자의 통제능력이 모두 높은 상태를 교차시킴으로서 나타날 수 있는 개념 유형이다. 즉 통제자의 통제능력이 높다는 것은 통제자가 이미 부패가 발생할 수 있는 영역으로 인식하고 있으며 이에 대한 통제를 하고 있음에도 불구하고 부패행위자는 ICT능력으로 이를 피해 부패행위를 실행시키는 특징을 나타낸다. 이에 해당하는 사례를 살펴보면 다음과 같다.

국방부 합동조사단은 14일 지인들의 청탁에 따라 전입 신병이나 초임 하사들을 서울과 경기·인천지역 부대에 배치해준 혐의(직무유기 및 위계에 의한 공무집행방해)로 전(前) 특수전 사령부 부관과장 김 모 중령을 구속했다. 합조단은 또 조작이 불가능한 장병분류용 신형 컴퓨터 프로그램 사용지시를 불이행한 이모 상사를 같은 혐의로 불구속 입건하고, 김 중령에게 돈을 건네준 혐의(제3자 뇌물공여)로 합조단 3급 군무원 이 모씨를 구속했다. 합조단에 따르면 김 중령은 2000년 12월부터 올 1월까지 특전사 부관과장으로 근무하면서 전·현직 장교 20여 명으로부터 부탁을 받고 신병 및 초임 하사 50여명을 수도권 일원의 군부대 요원으로 분류해 준 혐의를 받고 있다. 조사 결과 김 중령은 과거 같은 부대에서 근무하면서 친분관계를 유지했던 지인들로부터 부탁을 받은 장병들을 특정 부대에 근무토록 하기 위해 컴퓨터 프로그램을 반복, 가동하는 방법을 사용한 것으로 드러났다. 군무원 이씨는 약 10년간 친분관계를 유지해온 김 중령에게 2001년 2월부터 2003년 7월까지 11차례에 걸쳐 100만~200만원씩 모두 1천 400만원을 개인구좌로 입금해준 혐의를 받고 있다(중략).

한편 이 상사는 2002년 8월 장병분류용 컴퓨터 프로그램을 신형으로 교체하라는 육군참모총장 지시가 하달됐음에도 불구하고, 이를 어기고 조작이 가능한 구형 프로그램을 1년 이상 계속 사용한 사실이 확인됐다.

자료: 연합뉴스 2004년 04월 14일자

이 유형은 마치 퀴즈풀이의 과정과 같이 시간이 흐를수록 문제의 난이도를 높여가며 통제자가 문제를 내면 행위자가 문제를 풀어 나가는 과정이 되풀이 되는 상황이 연출된다. 이러한 상황에서 부패행위자는 통제자의 통제장치를 뚫고 시스템의 허점을 이용해 사적이익을 추구한다. 예컨대 공공정보에 합법적으로 접근할 수 있는 권한을 가진 공무원이 평소 알고지내는 사람이나 동료 또는 특혜를 바라는 외부인등의 청탁을 받고

전산망의 자료를 조작하는 경우를 들 수 있다. 이러한 유형으로 분류되는 전자부패의 특징들을 정리해 보면 다음과 같다.

- 부패행위자의 입장에서 이러한 유형의 부패는 상당한 위험을 감수해야 한다. 따라서 이러한 유형의 부패행위는 뚜렷한 목적의식을 가지고 이루어지는 특징을 나타낸다. 또한 이러한 행위를 할 수 있는 주체는 논리적 내부자이어야 한다. 여기서 논리적 내부자의 범주에는 앞서 언급한 바와 같이 권한의 유무와 관계없이 고급정보에 접근할 수 있는 권한을 획득할 수 있는 전문가도 해당된다. 여기에는 온라인상에서의 정보생성, 조작, 삭제, 파괴행위 등이 이에 해당되는데 전자정부 시스템 공급업체의 핵심기술을 설계한 프로그래머 등 상당한 지식을 가진 내부자에 의해 발생하는 부패행위이다.
- 이러한 유형의 전자부패는 앞에서 언급한 세 개의 유형 중 제1유형인 무지형 전자부패가 조직적·환경적 변화에 적응함으로써 나타날 수 있는 전자부패의 유형이다. 즉 제1유형의 경우 행위자와 통제자가 전자부패에 대한 아무런 인식과 대처방안이 없었던 상태에서 행위자의 입장에서는 업무의 반복처리로 인해 ICT기술을 시스템에 대한 기술과 이해를 증대시킬 것이다. 또한 통제자의 입장에서는 업무처리 과정에서 나타나는 시행착오를 통해 전자부패에 대한 대처의 필요성을 인지하게 될 것이다. 이러한 상황이 실현될 경우 제1유형의 전자부패는 제4유형의 전자부패로 전환하게 될 것이다.
- 제2유형의 전자부패가 제4유형의 전자부패로 전환될 개연성도 존재한다. 부패행위의 통제자가 기존에 인식하지 못했던 부패발생 가능성을 인지하고 정상적으로 통제자의 부패통제 능력을 증대시킬 경우 제2유형의 전자부패는 제4유형의 전자부패로 전환된다.
- 또한 유형의 부패는 시스템상의 허점을 찾아내고 통제가 허술한 부분으로 영역을 확장시켜 나가는 특징을 보인다. 앞서 언급된 세 가지 유형들 보다 통제의 강도가 가장 높은 유형이나 기존의 부패통제 시스템이나 제도적 보완으로는 적발이 용이치 않고 차별화된 전략적 대안이 요구되는 영역이다.

예컨대 사익추구의 가능성이 큰 정보에 접근할 수 있는 권한을 가진 자가 시스템의 취약점을 이해관계인에게 알려주고 관련 정보를 조작하도록 공모함으로써 개인적 이익을 추구하는 경우를 들 수 있다. 또한 본인이 직접 외부인의 아이디를 사용함으로써 권한을 가진 자신의 신분을 숨기고 자신이 알고 있는 시스템의 취약점들을 이용하거나 해킹기법 등 전문적인 기술을 동원해 정보를 조작하거나 삭제하는 경우도 발생할 수 있다. 즉 외부로부터의 침입을 가장한 내부자의 부패 행위가 이러한 유형의 전자부패에 해당된다.

IV. 분석결과 및 논의

1. 분석결과의 요약

제한된 여건 속에서 이루어진 연구결과들 중 이 연구를 통해 특징적으로 발견된 분석결과들을 요약해 보면 다음과 같이 제시될 수 있다.

- 전자부패의 개념적 이해와 규모를 예측하기 위하여 기존의 iceberg 모형을 수정해 제시하였다. 이러한 기존 모형에 대한 수정·보완 작업을 통해 동태적인 현상인 전자부패의 규모와 새로운 발생영역을 추정할 수 있었으며 사례분석을 통해 이러한 영역이 존재할 수 있음을 논리적으로 예측할 수 있었다.
- 전자부패의 개념적 유형분류의 틀을 부패행위자의 차원과 감시자의 차원으로 구성하여 교차시킴으로써 행위자의 ICT능력이 높고 낮음에 따라 감시자의 통제능력이 높고 낮음에 따른 네 가지 개념유형을 도출할 수 있었다.
- 수집된 각각의 사례들에 대한 특성분석을 위하여 여덟 가지 분류요소들을 선정하였다. 분류된 네 가지 개념유형에 속한 사례들의 공통된 특성들을 도출하였다.
- 유형별 대응전략에는 크게 두 개의 범주로 나누어 먼저 행위자에 초점을 맞춘 전자부패 방지전략을 논하였고 다음으로 감시자에 초점을 맞춘 전자부패 방지전략을 제시하였다.

2. 논의

1) 통제전략

(1) 전자부패 행위자에 초점을 맞춘 통제전략

여기서는 지금까지 언급한 전자부패의 유형에 따라 전자부패의 행위자에 초점을 맞춘 관리전략을 모색해보기로 한다. 분류된 유형의 순서대로 논의해 보면 다음과 같다. 전자부패 행위자의 입장에서 제1유형으로 분류되는 유형의 부패 행위자는 감시자의 통제능력이 낮은 상황 속에서 반복되는 업무로 인해 시스템의 특성에 대한 이해가 높아지게 된다. 전자부패 행위자의 시스템 조작능력이 증가하게 되면 제1유형의 전자 부패는 제3유형의 부패로 전환될 가능성이 크다. 마찬가지로 논리로 제2유형의 전자부패는 행위자의 능력이 높아짐에 따라 제4유형으로 영역을 이동할 가능성이 상존한다. 이처럼

변화할 것으로 예상되는 전자부패의 유형을 관리하기 위한 전략으로는 제3유형과 제4유형으로 분류된 전자부패를 제1유형과 제2유형의 영역으로 전환시키는 방법을 고려할 수 있다. 즉 행위자의 전자부패행위 능력을 감소시키는 것인데 이는 견출이나 견근 등의 방법으로 환경적 요소에 변화를 가함으로서 초보적인 수준의 부패에 머무르도록 유지시키는 전략을 고려해 볼 수 있다. 제1유형과 제2유형의 경우 전자부패의 형태가 자료의 유출에 의한 것임을 고려할 때 이에 대한 대응전략은 감시자 차원의 인식확대와 업무처리 절차의 확립, 문제발생시 가이드라인 등의 제공을 통해 예방이 가능하다. 제1유형이 제3유형으로 제2유형이 제4유형의 영역으로 전환되는 원인은 주로 업무의 반복성으로 학습효과의 증대이다. 이러한 변화는 같은 업무를 오랫동안 담당함으로써 나타날 수 있다는 점에 착안하여 주기적인 보직 전환 등의 조치가 필요함을 시사한다.

(2) 전자부패 감시자에 초점을 맞춘 관리전략

이 연구에서 분류된 전자부패의 유형분류는 크게 행위자와 감시자의 능력에 따른 차원을 교차시킴으로서 수행되었음은 주지하고 있는 바와 같다. 여기에서는 전자부패의 감시자에 초점을 맞춘 전자부패의 관리전략을 모색해 보기로 한다. 감시자의 통제능력이 증가할 경우 제1유형의 전자부패는 제2유형의 전자부패로 영역을 이동할 가능성이 존재하고 제3유형은 제4유형의 영역으로 이동할 가능성이 존재한다. 이러한 변화는 전략적 통제효과가 없는 것처럼 보이지만 전자부패의 통제가능이 전혀 없는 상태보다는 바람직한 상황으로의 변화로 설명될 수 있다. 반대로 감시자의 통제능력이 높은 상태에서 낮은 상태로 감소할 때 예상되는 전자부패 유형의 변화는 제2유형이 제1유형으로 제4유형이 제3유형의 영역으로 이동하는 상황이다. 이러한 상황이 나타날 수 있는 여건은 조직의 업무처리 시스템을 전면적으로 교체하는 경우 발생할 수 있다. 즉 기존의 통제력이 상실되고 새로운 시스템에 걸 맞는 전자부패 통제장치를 준비하는 단계에서 나타날 수 있는 바람직스럽지 못한 전자부패의 변화라고 할 수 있다. 이를 위한 관리전략으로 논의될 수 있는 것이 표준화된 전자부패 통제전략을 수립하는 방안이다. 이에 대한 대응전략으로 제시될 수 있는 것이 조직의 전자부패 취약요소를 측정하기 위한 지표의 개발의 필요성이다. 전자부패에 대한 조직적 차원의 대응전략은 호주정부의 정보화 취약요소에 대한 단계별 관리전략에서 언급한 바와 같이 전자위험 요인에 대한 평가기준을 정립하는 것이 이에 대한 첫걸음이 될 것이다.

2) 이론적 함의

전자정부의 구현으로 인해 정부에 의한 정보 집중은 더욱 가속화될 것이다. 이런 상황에서 정보를 둘러싼 부패의 가능성은 과거에 비하여 증대될 수밖에 없다. 또한 전자정부의 운영 과정에는 기존의 기술적·조직적·관리적 수준으로 해결하기 어려운 위험요소들이 존재하게 된다. 예를 들어 실시간성, 익명성, 새로운 영역에 대한 무지 등이 혼재되고 있으며 이러한 정보화의 특성들로 인해 새로운 유형의 부패 발생 가능성

은 상존하게 된다. 이는 정보화 시대에 새롭게 등장할 수 있는 부패현상에 대비한 보다 세심한 준비와 적극적인 대응전략이 모색되어야 함을 시사한다. 그럼에도 불구하고 전자정부 출범 이후 지금까지 전개된 논의들 중에 이에 대한 문제의식과 대응전략에 대한 구체적인 논의들이 존재하지 않는다. 전자정부에 대한 대부분의 논의들이 낙관적인 미래를 예견하고 있음을 고려해 볼 때 이는 심각한 이론적 논의의 편향성을 보여주는 결과라고 할 수 있다. 전자부패는 가상의 공간에서 형성되고 발현되는 것이기 때문에 이를 이해하기 위해서는 정보통신기술의 특성에 대한 면밀한 검토가 필요하다. 시간과 공간의 제약 없이 행정행위가 이루어지는 전자정부의 기술적 특성들은 우리사회의 부패라고 하는 속성과의 상호작용으로 고려되어야 한다. 전자정부 구현과정상의 문제점 내지 취약부문에 대한 관심과 이에 대한 정책적 고려는 소위 선진국으로 분류되는 국가들을 중심으로 진행되고 있지만 그 어느 곳에서도 성공을 확신할 수 있을 만큼의 경험과 추진전략을 확보하지는 못하고 있는 실정이다. 따라서 전자정부의 구현 자체가 기존의 부패를 잠재울 수 있으리라는 막연한 기대는 단순한 기대로 머무를 가능성이 크다. 특히 우리사회의 경우 특혜시비나 공직부패는 정권이 바뀔 때마다 이슈와 논란을 재생산하는 요체가 되어왔다. 사안의 중요성을 감안할 때 전자부패 방지를 위한 정책적 노력은 전자정부라는 새로운 틀 안에서 의식적이고도 체계적으로 접근해야 한다. 이러한 점에서 이 논문의 결과는 전자정부라는 업무환경 속에서 발생할 수 있는 새로운 부패현상을 인식하고 이에 대한 대책을 수립하는데 기초 자료로 활용할 수 있을 것이다.

이 연구를 통해 도출된 결과와 활용방안은 다음과 같다. 첫째, 전자부패의 실제 사례를 중심으로 개념적 유형화를 시도함으로써 전자부패에 대한 인식과 이해의 토대를 마련하였다. 둘째, 실증적인 유형분류를 통해 도출된 유형들은 조직 관리적 시각과 학술적 시각을 제공함으로써 발생 가능한 전자부패 문제를 유사한 유형으로 분류하는 것을 가능케 할 것이다.

이 연구를 통해 일반화를 시도할 수는 없었지만 나름대로 전자부패 현상의 일반화를 위한 새로운 가설 생성의 계기를 제공하였다고 여겨진다. 각 유형별 분석결과는 분류의 기준으로 활용 가능할 것으로 예상되며 분석결과의 논의에서 제시된 전자부패의 전략적 대응 방안 등은 전자부패 예방을 위한 정책적 지침으로 활용할 수 있을 것이다. 셋째, 지금까지 전자정부 분야의 다양한 논의들 중 사안의 중요성에도 불구하고 논의의 사각지대로 방치되었던 전자부패의 문제를 논의하기 위한 학술적 토대를 마련하였다고 여겨진다. 넷째, 연구에 사용된 사례들은 지금까지 단 한 번도 전자부패라는 개념정의 하에 분류된 적이 없는 사례이다. 추후 전자부패에 대한 후속연구가 이루어질 경우 단일한 개념으로 분류된 선행연구 자료로서 활용될 수 있을 것이다. 또한 실무적으로도 공무원들을 대상으로 한 교육 자료로서도 활용할 수 있을 것이다.

V. 나가며

1. 정책제언

이 논문의 서두에서 언급한 바와 같이 전자정부의 구현으로 과연 우리사회의 부패를 감소시킬 수 있을 것인가? 라는 문제제기에 대해서는 이 연구에서 제시한 전자부패의 유형과 사례를 통해 판단해 볼 때 회의적일 수밖에 없다. 왜냐하면 정보화라는 변수 특히 공공부문에서 논의되고 있는 전자정부 내지 국가정보화라는 변수는 신기술을 일의 능률과 투명성을 강화하고자 창의적이고 생산적인 의도이외에 부패행위의 수단으로 이용하려는 불순한 의도를 가진 자들에게도 역시 새로운 기회를 제공하기 때문이다. 즉 새로운 신기술들이 가져다 줄 수 있는 혜택의 이면에 존재하는 부정적인 요소들도 균형적으로 고려해야 한다. 이와 더불어 전자정부의 부패위험요소에 대한 정책적 논의는 사후적 대응 차원뿐만 아니라 사전예방의 차원에서 논의되어야 한다는 점이다. 이를 위해서는 전자부패에 대한 인식확산과 정보화의 특성별 위험요소에 대한 관리가 절실히 요구된다. 새로운 시스템 설계 시 전자부패 취약성에 대한 고려와 체계적이고 종합적인 접근이 요구된다. 이하에서는 연구가 시사하는 바를 정리하고 이를 토대로 요구되는 정책들을 제언해 보고자 한다.

- 전자부패의 환경적 요인들을 분석하고 이에 대한 취약성을 관리하기 위한 세부적인 점검지침이 만들어져야 할 것이다. 이러한 사항에 대한 점검은 요식행사로 치러져서는 안 되며 정기적, 비정기적 점검이 병행되어야 한다. 또한 이러한 업무를 담당할 수 있는 호주의 ICAC와 같은 전담기관이 필요하다. 이러한 전담기관의 선정기준은 우리나라의 처한 현실적 특수성을 최대한 반영하는 방향으로 이루어져야 할 것이다. 예컨대 현재 전자정부 추진 전담기관인 행정안전부의 정보화전략실이나 감사원, 부패방지 전담기관인 부패방지위원회 등이 거론될 수 있을 것이다.
- 이러한 전자부패를 전담할 수 있는 기관이 지정되고 난 후에는 전담기관을 중심으로 정부차원의 전자부패 예방정책이 수립되어야 한다. 이에 대한 다양한 연구 활동의 지원이 이루어져야 하고 실무적 차원에서는 전자부패에 대한 교육·홍보활동이 지속적으로 이루어져야 할 것이다. 특히 이 연구의 결과로 도출된 전자부패의 네 가지 유형 중 무지형 전자부패의 경우 정기적인 점검과 교육으로 상당부분 예방효과를 거둘 수 있을 것이다.
- 전자부패에 대한 예방적 차원에서 공공정보를 다루는 시스템 접속기록을 유지하고 이 기록들의 진정성이 확보되는 기록관리 체계의 도입이 요구된다. 이러한 체계의 도입은 전자부패 행위가 사후에라도 언제든지 적발될 수 있음을 잠재적 부패행위자들에게 각인시키는 역할을 하게 된다.

- 전자정부의 운영과 관계되는 민간인 및 계약직 직원들에 대한 권한통제가 이루어져야 한다. 기존의 부패가 전자부패로 전환되면서 나타날 수 있는 두드러진 특징들 중 하나가 부정한 방법으로 온라인상에서 권한을 획득하는 것이다. 우월한 프로그래밍 능력을 갖춘 잠재된 부패행위자들을 식별하고 다양한 접근권한에 대한 통제장치가 마련되어야 한다.
- 민간위탁으로 인한 기술의존도가 심화될수록 전자부패가 발생할 수 있는 개연성은 점점 커지게 된다. 따라서 정부는 전자정부와 관련된 기술개발과 연구를 독자적으로 실행할 수 있는 능력과 체계를 갖춰야 한다. 또한 공공조직 내에서 직원들 간에 발생할 수 있는 정보격차를 최소화하기 위한 방안이 마련되어야 한다. 공공조직의 의사결정권자 또는 부서장 등의 부패통제 능력이 온라인과 오프라인의 차이 없이 행사되어야 한다. 각 부서의 책임자는 전자부패의 통제자로서 역할을 할 수 있어야 한다.

전자정부와 더불어 도입되는 신기술 및 이에 대한 이해부족은 전자부패라는 새로운 역기능으로 발현될 가능성을 높인다. 성공적인 전자정부의 구현을 위해 필수적인 사항이다. 이상에서 제시된 정책제언들은 가장 거시적인 범주들을 제시한 것에 불과하다. 그럼에도 불구하고 우리나라 전자정부 구현 과정 속에서 전자부패의 취약성에 대한 고려가 전무한 실정임을 감안할 때 전자부패의 문제에 대한 인식과 대응전략의 중요성은 더욱 커진다. 위험사회론의 논의들에서 확인할 수 있듯이 정보통신기술 속에 담겨진 무한한 가능성이 다양한 차원에서 관리되고 인식되어지지 못할 때 기대했던 가능성은 우리사회에 위협으로 변할 수 있으며 의도했던 바와 정반대의 결과를 초래할 수 있다. 전자부패에 대한 대응전략은 투명성 강화를 통한 부패척결이라는 기존의 정책목표와 정보화를 통한 정부혁신이라는 두 가지 정책목표를 포괄할 수 있어야 한다. 이 연구의 주된 관심사인 전자부패의 문제가 사회적 문제로 현실화 될 경우 전자정부 구현에 커다란 장애요인으로 부각될 것이다. 따라서 이에 대한 인식과 대응전략이 미흡하다면 전자정부는 낭비와 비능률이 온상이 될 가능성이 높으며 결과적으로 국민으로부터 신뢰를 잃게 될 것이다. 국민으로부터 신뢰기반이 상실된다는 것은 국가경쟁력의 약화나 국민통합의 저하로 연결되며 나아가 정권의 붕괴로도 현실화될 수 있음을 우리는 이미 역사적으로 확인한 바 있다.

2. 연구의 한계

이 연구는 다음의 몇 가지 한계를 지닌다. 첫째, 이 연구의 분석대상인 전자부패 사례는 전체 부패사례의 일부에 해당하는 것들이다. 공공부문의 부패사건들 중 전자부패로 분류될 수 있는 규모가 어느 정도이고 이로 인한 피해규모도 예측할 수 없는 한계를 지닌다. 이처럼 제한된 사례를 가지고 일반화를 시도할 수는 없는 상황을 극복하기

위해 일반화가 가능한 정량적 연구와 후속연구들이 이어져야 할 것이다.

둘째, 이 연구의 주제와 관련하여 전자부패의 문제는 관련 자료의 축적이 미진⁸⁾한 척박한 분야이며 따라서 이론적 논의가 매우 빈약한 분야임은 주지하고 있는 바와 같다. 이로 인해 연구를 보다 체계적으로 진행하는데 많은 어려움과 장애요소가 있었음을 시인하지 않을 수 없다. 그럼에도 불구하고 이 연구에서 일관되게 추구하고자 한 것은 전자부패의 실체에 근원적으로 접근하기 위해 사례를 통한 실증분석과 그것의 내용분석을 통한 질적 접근을 동시에 시도하였다는 점이다. 보다 명확한 논리전개를 위해 가능한 한 많은 사례를 확보하는 노력들이 뒤따른다면 논의를 보다 객관적으로 접근할 수 있었을 것으로 여겨진다.

셋째, 전자부패의 유형 분류에 대한 논의에 있어서 제한된 요소들만을 분석대상으로 삼고 있다는 점이다. 이러한 취약성에도 불구하고 이 연구의 전자부패에 관한 논의는 기존의 부패와 차별화 되는 정보통신기술의 특성을 배태하고 있다는 점에서 기존의 인식과 대처방식으로는 실체에 접근할 수 없다는 점을 부각시켰다는 점에서 의미를 가진다. 전자부패의 위험성에 대한 정확한 인식과 대응전략이 있다는 것은 정부의 대국민 신뢰와 전자정부 사업의 성과를 향상시키는데 필수적인 사안이라고 할 수 있다.

<참고문헌>

- 감사원.(2003). 「전자정부 구현사업 추진실태 감사결과」.
- 김명준.(2002). "디지털 네트워크시대의 전시주의적 역감시 현상에 대한 고찰"
- 김문조.(1999.) 성숙 정보사회를 향하여, 「정보혁명, 생활혁명, 의식혁명」, 백산서당, pp. 333-364.
- _____. (1998a) 정보사회: 본질과 유형, 「정보화시대의 미디어와 문화」, 세계사, pp. 37-54.
- _____. (1998b) 성숙정보사회의 가능성 진단, 「한국사회」 제1집, 한국사회연구소, pp. 51-80
- 김석주.(2003). "우리나라 전자정부 발전방안에 대한 모색: 현황과 향후 추진방향을 중심으로," 정보통신정책연구 10(2), pp.37-55.
- 김순희·김동환.(2001). "전자정부 추진에 내제된 딜레마," 한국행정학회 동계학술대회 발표 논문집, pp.741-58.
- 김영종.(1999). "정보부패의 패러다임 정립과 치유," 한국부패학회보, p.31.
- _____. (2002). "가상공간(사이버)에서의 부패: 행정윤리적 접근," 한국부패학회보,

8) 이러한 이유는 지금까지 전자부패가 발생하지 않았기 때문이 아니라 이에 대한 유관기관의 인식과 분류 기준의 부재에 기인하는 것이라고 여겨진다. 이 연구에서 조사된 자료에 의하면 본격적으로 정보화가 진행되기 시작한 90년대 중반부터 이미 전자부패의 사례들이 보도된 바 있다.

- pp.75-104.
- 남궁근 외.(2002), 「전자정부를 통한 부패통제: 이론과 사례」, 경상대학교 사회과학연구소, 서울: 한울 아카데미.
- 명승환.(2006), "전자정부 연구에서 결정론적 사고의 한계와 극복방안: 행정의 투명성을 중심으로", 정보화정책, 13(1), pp.100-115.
- 목진휴·명승환·윤대범.(2002), "전자정부를 통한 행정부패 감소방안: 정보통신기술(ICT)을 통한 레드태이프의 제거방안을 중심으로," 정보화정책, 9(3), pp.3-17.
- 삼성경제연구소.(2003), CEO Information 인터넷 강국의 취약성과 대응과제.
- 송희준·최홍섭.(2002), "전자정부사업의 투명성 제고효과: 현황과 전망," 한국정책학회 하계 학술대회 발표논문집, pp.337-58.
- 안문석.(2001), "신뢰사회 구축과 전자정부," 한국행정연구원 행정포커스.
- 이태영.(2007), "전자부패의 유형과 통제전략에 관한 연구", 한국외국어대학교대학원 박사 학위논문
- 전자정부특별위원회.(2001), 「전자정부 추진에 있어서 장애요인의 극복방안」, _____.(2002), 「전자정부사업의 투명성 제고효과분석」.
- 최영훈·김석곤.(2006), "사이버문화신희, 정보통신기술 활용수준 그리고 전자부패간의 관계", 한국부패학회보 11(2), pp.97-117.
- 최영훈·명승환·이태영.(2003), "전자부패의 존재양식과 대응방안에 관한 연구", 한국전산원.
- 한국전산원.(2003), 「전자부패의 존재양식과 대처방안에 관한 연구」.
- 한세억.(2003), "사이버 상 역기능방지를 위한 전자정부정책의 평가", 한국정책학회 추계학술대회 발표논문.
- 황성돈.(1998), "不正腐敗의 本質과 政策課題", 『韓國行政研究』, 겨울호 (제7권 제 4호), p.8.
- 황성돈·정충식 .(2002), 「전자정부의 이해」, 한국전자정부연구원, 서울: 다산출판사.
- Baird, M. (2000). Transparency and Corporate Governance, Washington, DC: The World Bank
- Christopher Bell & Lisa Zipparo, 'Exploiting emerging technology corruptly in the NSW public sector', p. 30.
- Grabosky, P., and Smith, R. G.(1998), Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities, New Brunswick, N.J.: Transaction Publishers and Sydney: Federation Press.
- Heeks, R. (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: UK.
- _____.(1999a), "Different Approaches to Information Age Reform," in Heeks(ed), *Reinventing Government in the Information Age*, Routledge.

- Hwang, SungDon et al(1998), "Electronic Government in a Conceptual Derangement: A Practitioner's View" in International Symposium on Electronic Government: Vision and Strategies, KAPA: 9-20.
- ICAC(2001), Risk Management Guideline: Information Management and Technology, NSW Government Office of Information Technology, p.9.
- _____(2003), Information Technology Security Management for NSW Public Agencies.
- OECD, The Hidden Threat to E-Government: Avoiding large government IT failures, PUMA Policy Brief No.8., March 2001.
- Peter G. Neumann(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.
- Shadrach, B.(2002), "eGovernment for Transparency," International Conference on eGovernment for Development, United Nations Department of Social and Economic affairs(UN/DESA).
- Susan Rose-Ackerman(1978), "Corruption: A Study in Political Economy" (N.Y. : Academic Press, 1978), p.17.
- OECD(2001), The Hidden Threat to E-Government: Avoiding large government IT failures, *PUMA Policy Brief No.8., March*.
- OECD(2002), E-Government Flagship Report-The E-Government Imperative.
- Peterson, J.(1995), Playing the transparency Game: Consultation an Policy-making in the European Commission, Public Administration, 73: 473-492.
- Putzel, J.(1998), The Business of Aid: Transparency and Accountability in European Union Development Assistance, *Journal of Development Studies*, 34(3): 71-96.