농협 전산장애, 정말 북한 소행인가?

농협전산마비사태를 통해 돌아본 금융 IT의 안전성

2011.5.2 | 김병권_새사연 부원장 | bkkim21kr@saesayon.org

목 차

새로운 사회를 여는 연구원

http://saesayon.org

1. 농협 전산망마비 사태, 공안사건으로 가나?

“아이가 아파 병원을 찾게 되었습니다. 차로 이동을 했던 터라 미리 은행에 들르지 못해 지갑에 딱 5700원이 있었던 지라 카드결재를 하기로 했지요. 하지만...승인오류....다시 한 번 했지만... 또...승인오류...그래도 마침 진료비가 5500원이 나왔기에 현금을 긁어모아 결재를 할 수 있었죠. ... 아이들과 나와 재잘재잘...아이들은 약국 앞의 풀빵 집에서 풀빵을 사주기로 한 약속을 잊지 않고 보채는데...엄마는 달랑 200원밖에 없는 이 상황이...”

농협 전산장애 피해카페(http://cafe.naver.com/ims300)에 올라온 한 피해자의 글이다. 실제로 농협 전산장애가 시작되고 나흘 만에 신용카드와 체크카드 기본 기능이 되돌아 왔으므로 그 동안 이런 유형의 다양한 고객 불편사항들은 충분히 여러 형태로 발생할 수 있었고 발생했을 것으로 추정된다. 금융서비스 역사상 거의 초유의 사태라 할 만하다.

도대체 무슨 일이 있었던 것일까. 사건이 발생한지 보름이 넘었지만 여전히 문제의 원인과 발생경로, 피해규모 등을 제대로 알 수가 없다. 농협의 공식발표는 지금 시점에서 완전히 신뢰하기는 어려울 뿐 아니라 검찰수사도 아직 확정된 것이 없다. 우선은 대고객 사과문에서 표현된 농협의 공식 발표를 통해 사건 경위를 요약해보자.

농협발표에 의하면 4월 12일 오후 5시 “농협중앙회 IT본부 내에서 상주 근무하던 협력사 직원의 노트북PC를 경유하여 각 업무시스템을 연계해 주는 중계서버에서” “형체를 알 수 없는「시스템 파일 삭제 명령」이 실행되어” “약 5분 동안 275개의 서버에서 데이터 일부가 삭제되는 피해를”보게 되었다는 것이다. 농협은 삭제 명령이 실행된 지 10분 후에 삭제 명령이 실행된 모든 중개 서버를 셧다운시키고 대고객 거래를 전면 중단시켰다고 발표했다.

그리고 사건 발생 4일이 지난 4월 15일에서야 일부 카드거래를 제외한 대부분의 금융거래를 복구했지만 일부 대외계와 연계된 카드결제 등은 최종 복구를 약속한 4월 22일까지 복구되지 않았고 신용카드 거래 관련 일부 원장 유실가능성까지 있는 것으로 파악된다는 것이다. 아울러 농협 측은 “전산장애로 인해 고객여러분께서 입은 경제적 피해에 대해서는 적절한 절차에 따라 보상해드릴 것을 약속”한다고 했지

만, 아직 피해 규모도 산정이 안 되고 있고 피해 입증을 어디까지 해야 보상할 것인지도 불명확한 상태이다. 이런 가운데 농협 측은 집단 소송 대상은 아니라고 했지만 일부에서는 집단 소송까지 준비하고 있는 상황이다.

수사를 담당하고 있는 검찰은 내부 시스템에 접근이 가능한 전산관련 내부 직원과 협력업체 직원을 소환하여 수사 중이지만 아직 확실한 결론은 내지 못한 상황이고, 내부자가 아닌 외부에서의 침투, 심지어는 중국에서 들어온 IP가 해당 IBM 노트북에 있다는 이유로 북한 소행 추정으로 가고 있어 졸지에 '공안 사건'으로 비화되고 있는 중이다. 장기간의 서비스 중단도 초유의 사태이지만, 보름이 지난 지금까지 시스템 복구가 안 되고 있는 점이나 문제를 누가 어떻게 일으켰는지 제대로 파악하지 못하고 있는 점도 초유의 사태라고 할 만 하다.

표: 농협 전산망 마비 사태 주요 일지

일자	기관	내용
4.12	농협	- 오후 5시, 275개 중개서버에 시스템 파일 삭제 명령 실행, 5시 10분부터 전산시스템 가동 중지, 금융 거래 전면 중지
4.13	농협	- 오후 12시 40분, 창구 거래 정상화
4.14	농협	- 오전 2시 ATM 거래 정상화, 인터넷 뱅킹 정상화 - 최원병 농협중앙회장 대국민 사과문 발표
4.15	농협	- 신용카드와 체크카드 거래 정상화, 신용카드 현금서비스 정상화(대금 결제 등 일부 서비스 여전히 불가)
4.17	검찰	- 삭제 명령어가 노트북 컴퓨터의 키보드에서 직접 입력된 것은 아니라고 발표하여 외부 해킹 가능성 암시
4.19	검찰	- 내부시스템을 잘 아는 사람이 한 달 전에 삭제명령을 심었다고 발표
	농협	- 입출금 등 일반 업무 정상화, 카드업무 97%가량 복구되었다고 발표 - 4월 22일까지 전산망 완전 복구하겠다고 발표
4.20	검찰	- "외부에서 침입한 흔적이 많다"며 외부 해킹 가능성 조사
4.21	농협	- 피해보상 접수건수 총 1천96건, 이중 898건, 758만원은 보상처리 - 카드 대금 결제 일을 5월로 한 달간 연기하기로 함
4.22	농협	- 완전복구 실패, 4월 말까지 최대한 복구노력, 안 되면 별도 방침 결정, - 신용카드 일부거래 완전 유실 가능성 인정.(카드 업무 일부 거래 장애 지속)

		- 이재관 농협전무 사의 표명
4.24	검찰	- 외부에서 '좀비 PC'나 원격조종 등의 방법으로 서버 파괴를 실행했을 가능성이 있다고 보고 국내외 관련 IP(Internet Protocol)를 역추적
4.26	검찰	- 북한 소행 가능성 있다고 발표

2. 농협 전산 마비사태는 무엇이 다른가.

지난 2009년 7월 국내외 주요 기관과 금융 사이트에 감행된 디도스(DDos) 공격에서부터 지난 4월 8일 현태캐피탈 시스템 해킹에 의한 개인정보 유출, 그리고 25일 BC카드 일시 거래중지 사태에 이르기까지 크고 작은 금융전산망 보안 문제는 지속적으로 존재했다. 그러나 지금의 농협 사태는 이들과 몇 가지 국면에서 차원을 달리한다.

우선 고객 서비스 차원에서 확인해보자. 이번 농협사태가 기계적 장애에 의한 거래 서비스 지연이나 (최대 수 시간 이내)의 일시 중지, 또는 특정 고객의 거래처리 오류라고 하는 통상적인 장애를 넘어서는 것은 물론, 최근 현대 캐피탈 사태처럼 상당한 빈도로 발생하고 있지만 중대 사고에 속하는 고객정보 유출과도 또 다르다. ▶ 창구, ATM, 인터넷 뱅킹 등 모든 고객 채널이 예고 없이 일시에 중단되었던 점, ▶ 수일 기간 동안 입금 출금이나 결제, 이체 등의 금융거래가 불가능해지면서 농협 고객들의 전체 범위에 걸쳐 실제 생활과 업무에 중대한 차질을 줄 수 있게 되었다는 점(잠재적 피해 가능성이 아니라 현실적인 유 무형 피해가 상당할 것이라는 점), ▶ 농협 측의 당초 주장과 달리 일정 시점에 거래된 (신용카드 관련) 고객의 거래 정보가 유실될 가능성이 있었고(물론 농협측은 계정계 자체가 손상된 것이 아니라 중계 서버 고장으로 VAN 망을 통해 들어온 거래정보가 고객 원장에 쌓이지 못한 것이라고 주장하고 있다.), 경우에 따라서는 원장 계정계 시스템 자체까지 완전히 망가질 수도 있는 상황으로 발전할 수 도 있었던 점 등이 대표적이다.[1)]

IT 시스템 차원에서 보면 문제는 더욱 심각하다. ▶ 통상 고객 서비스와 직접 연결된 창구 단말 서버나 인터넷 뱅킹서버의 뒤쪽에 위치하고 있고 원장 정보를 처리하

1) 당초 농협 측은 14일 발표한 사과문에서 “소중한 고객정보와 금융거래 원장은 모두 정상이며 전혀 피해가 없었음을 이 자리에서 국민 여러분과 3천만 고객 여러분께 확실하게 말씀”드린다고 단언했다가 22일 카드 거래 일부 유실을 인정하는 식으로 말을 바꾸었다.

는 계정계 바로 앞단에 있는 백 엔드 중개서버까지 장애가 발생했다는 점, ▶ 내부 핵심 시스템에 접근할 수 있는 시스템 관리자 계정 권한으로 중개서버 수백 대가 동시에 정지되었다는 것, ▶ 일부 프로세스나 일부 데이터 손상이 아닌 운영시스템 파일 삭제 같은 운영체제 자체의 손상이 발생했다는 점 등에서 거의 전무후무한 사고에 속한다고 볼 수 있다.

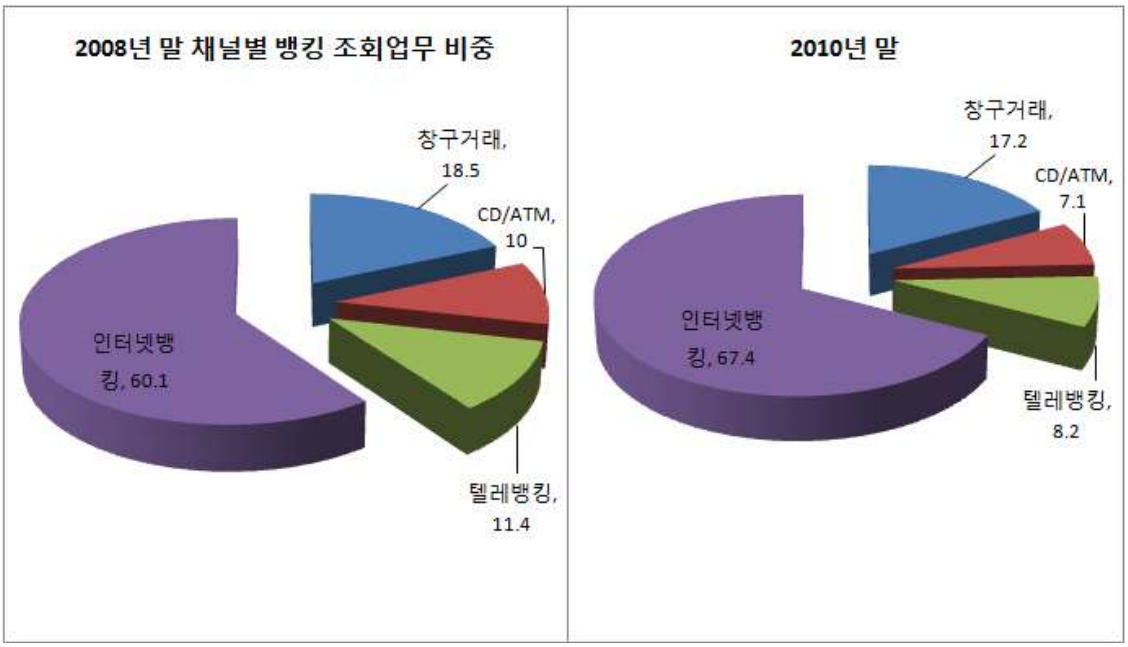
금융권의 핵심 계정계 관련 시스템은 기본적으로 인터넷과 같은 외부 망과 단절된 내부 망 체계를 갖추고 있을 뿐 아니라, 복잡한 아키텍처를 갖고 있기 때문에 몇 단계의 인증시스템, 암호화 시스템, 다중 방화벽, 침입탐지 시스템을 통과해야 접근이 가능하다. 그 마저도 핵심 백 엔드 서버에 대한 루트 계정 권한을 확보해 해당 서버의 시스템 파일을 삭제하는 것을 일반 명령어라인 상에서가 아닌 정교한 스크립트를 작성하여 실행하는 것은 내부 시스템 정보에 대한 지식이 없는 일반 외부인으로서는 불가능하다고 해도 좋다.

명령어가 실행되었던 단말 노트북 컴퓨터도 외부 망이 아닌 내부 망에 연결되어 있었다고 알려졌다. 내부 전산시스템과 관련이 없는 외부인 또는 내부 전산망에 전혀 접근 경험이 없는 원격의 해커 등이 인터넷 망 등 외부 망을 경유해 내부 전산망을 해킹한 사건으로 보기에는 여러 가지로 무리가 있다는 것이다. 일단은 공식적인 조사가 여전히 진행 중이므로 불필요한 예단을 하지 말고 농협과 검찰에서 최종적으로 어떻게 판단을 내리는지 지켜보기로 하자.

다만, 문제의 당사자인 농협 경영진들과 책임자들이 조기에 사고 경위를 제대로 공개하고 피해를 입은 고객과 시민들에게 충분한 상황 공유를 하지 못해 불신을 키우고 있는 점은 지금이라도 충분히 지적되어야 하고 이후 피해보상 등에 대해 적극적인 자세를 보일 필요가 있다. 현대 캐피탈 고객정보 유출에 이어 연이은 농협 전산망 마비 사태에도 불구하고 “금융회사의 전산시스템 보안 강화 및 고객정보 보호 등을 위해 필요한 투자를 확대하고, 특히 관련 업무에 경영진이 각별한 관심을 기울일 것을 당부”하는 수준의 간담회에 그치거나, 충분한 앞 뒤 설명이 없는 채로 ‘북한 소행’등 애매한 정보를 흘리는 검찰 수사태도도 문제다. 대개의 경우 ‘북한 소행 추정’은 영원한 미제 사건으로 끝이 난 경우가 적지 않아 우려가 앞선다. 확실한 문제파악과 더불어 고객피해에 대한 적극적인 대책강구를 농협과 함께 진행할 필요가 있다.

3. 높아지는 금융거래의 IT의존도

금융회사들의 내부 업무시스템이나 대 고객 서비스에서 IT기술 활용도는 제조업과 같은 다른 산업분야와는 비교가 안 되게 빠르게 확대되어 왔다. 일반적인 업무가 정보의 이동과 함께 (택배 배송 등을 통해) 실물이 동시에 움직이는 것과는 달리 뱅킹, 트레이딩, 보험판매와 계약, 카드거래 등 모든 금융거래는 실물이 움직여야 할 필요 없이 단순히 정보를 변경하면 거래가 완료되기 때문에 IT기술이 거의 모든 업무에서 가장 전형적으로 적용될 수 있기 때문이다.



이는 실제 통계로도 입증된다. 지금은 일반적 조회나 입출금 뱅킹 업무를 보기위해 은행을 직접 찾아가는 경우는 거의 없다. 절반이 훨씬 넘는 국민들은 인터넷 뱅킹을 이용한다. 예금 조회서비스의 67%, 입출금과 이체 업무의 40%를 인터넷 뱅킹이 차지하고 있다. 그 결과 지금 인터넷 뱅킹 이용자는 등록 고객 수 기준으로 6천 666만 명이다. 경제활동 인구수의 거의 두 배가 된다는 얘기고 일반적인 국민은 두 개 정도의 인터넷 뱅킹 계좌가 있다는 소리다. 지난 10년 동안 무려 16배가 늘어났다. 이 뿐이 아니라 모바일 뱅킹 등록 고객 수는 1500만 명을 넘어섰고 최근 스마트폰 기반 모바일 뱅킹 고객 수도 서비스개시 1년 만에 261만 명을 기록하고 있는 중이다.[2] 세계 최고 수준이다.

2) 한국은행, “2010년 중 국내 인터넷 뱅킹 서비스 이용 현황”, 2010.2

뱅킹 업무만이 아니다. 온라인 증권거래도 전체 금액 기준으로 50%를 넘어선 지는 오래되었다. 2009년 기준으로 온라인 거래비중은 58.7%였다. 보험의 온라인화도 눈에 띄게 증가하고 있다. 2008년 말 현재 38개 생보사와 손보사가 서비스하고 있는 인터넷 마케팅 이용자가 연 중 1124만 명이다. 아직 대부분은 조회서비스에 국한되고 있지만 빠르게 확대되고 있는 중이다.[3)]

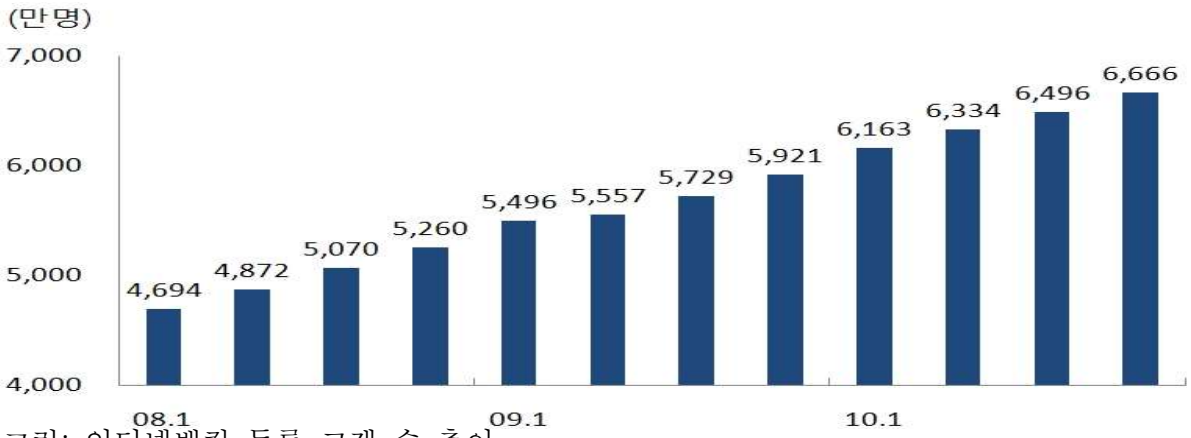


그림: 인터넷뱅킹 등록 고객 수 추이

출처: 한국은행, “2010년 중 국내 인터넷뱅킹서비스 이용현황”, 2011.2.8

그 만큼 금융 전산시스템에서 장애가 발생하면 즉각적이고 광범위하게 국민들이 피해를 당할 소지가 크다는 것이다. 피해의 성격 역시 단순한 정보 유출의 문제로 한정되는 다른 산업과는 전혀 다르다. 금융정보 유출이나 유실, 변경은 그 자체가 곧 직접적으로 돈의 문제이고 간접적으로 자금처리를 예정대로 하지 못함으로써 발생하는 생활적, 사업적 손실을 의미하게 되기 때문이다.

두 번째로 외부 망과의 연계성이 갈수록 높아지고 있다는 것이다. 현재 뱅킹 업무 가운데 고객대면 접촉 채널, 즉 고객과 대화하며 창구직원이 입출금과 조회 업무를 직접 처리하는 비중은 15%도 안 된다. 반면 비대면 고객채널 즉, CD/ATM, 텔레뱅킹, 인터넷 뱅킹 등 고객이 기기나 인터넷을 통해 뱅킹 시스템에 접근하여 업무 처리를 하는 비중이 압도적이다. 여기에 최근 폭발적으로 증가하고 있는 모바일 뱅킹까지 가세하게 되면 유선 망 뿐 아니라 무선망까지를 경유하여 외부에서 다양하게 금융 서비스 시스템에 접근하게 된다. 그 만큼 금융 전산시스템의 보안과 관리가

3) 한국정보화진흥원, “2010 한국정보화 통계집”, 2010.10

철저하게 이루어져야 한다는 것이고 장애가 발생했을 때 수동으로 대체할 수단도 없다는 뜻이다.

셋째로, 이와 같이 팽창하는 전자 금융서비스를 지원하기 위한 금융회사의 전산 시스템 규모와 복잡도가 갈수록 커지고 있다는 것이다. 사고가 난 농협 전산시스템은 주요 서버가 553개가 되는 것으로 발표되었고 그 가운데 절반에 해당하는 275개 서버가 단 5분 만에 시스템 파일이 삭제되는 중대한 사고를 발생시켰던 것이다. 최 뒷단의 코어뱅킹 시스템을 시작으로 전자금융서버, 비지니즈 서버, 프리젠테이션 서버 등이 각각 수 십 대 이상 배치되어 있을 뿐 아니라 각종 정보계 서버, 보안과 인증관련 서버도 상당한 규모로 결합되어 있고 별도의 백업과 복구를 위한 시스템까지 운영되고 있다. 외부 금융망과 연계하기 위한 서버 시스템도 적지 않다.

여기까지는 외형적인 하드웨어 구조다. 각 하드웨어 구조가 복잡해지는 것 이상으로 소프트웨어 구조는 더욱 복잡하게 얽히게 된다. 예의 '전산실' 개념과 차원이 달라진 지도 매우 오래된 얘기다. 매우 체계화 된 관리시스템과 운영 정책과 매뉴얼, 다종 다기한 전문가와 운영인력이 전체적으로 결합되어 금융서비스를 하는 거대한 구조가 되었다는 것이다. 모바일과 같은 새로운 고객 채널이 추가될 때마다, 새로운 금융상품과 서비스가 추가될 때마다 하드웨어와 소프트웨어 구조는 지금도 확장되어 나가고 있다.

한마디로 서비스를 제공하는 금융회사 입장에서나 서비스를 받는 국민들의 입장에서나 금융은 현재 절대적으로 IT 기술과 인력의 집합체에 의존하여 동작되고 있다고 할 것이다. 이런 상황에서 농협 전산시스템의 핵심부의 절반이 일부 기능정지가 아니라 '시스템적으로 망가지는' 사태가 발생한 것이다.

4. 전산 마비 사태가 발생할 수 있는 환경이었을까.

그렇다면 이토록 복잡하고 엄격한 농협 전산망의 핵심 내부 시스템이 어떻게 치명적 수준으로 광범위하게 파손될 수 있었던가. 현재 공식 확인할 수 있는 것은 농협 정보시스템의 절반이 피해를 당했다는 것, 일부 데이터베이스 데이터 문제나 일부 실행 프로그램 문제가 아니라 운영시스템 파일 자체가 삭제되는 치명적인 피해를 당했다는 것, 운영 관리를 위해 내부 망에 연결된 한 노트북 컴퓨터에서 정교한 스

크립트로 세팅된 시스템 파일 삭제명령이 5분이라는 짧은 시간 동안 해당 시스템 전부에 대한 루트 계정 권한을 확보한 상황에서 동시에 서버에 전달되었다는 것 정도이다.

그 외에 검찰이 수사과정에서 흘리고 있는 것처럼, 외부에서 해당 노트북을 경유하여 서버에 접근했을 가능성이라든지 중국을 통해 들어온 IP의 흔적이 노트북 컴퓨터에 있는 정황이 포착되었다든지 하는 정보들은 정확한 내역은 알 수 없으나 현재로서는 이런 외부 요인만으로 사태발생을 설명하기에는 절대적으로 무리가 있다.

문제는 어떻게 위의 사태가 발생할 수 있었냐는 점인데 아직은 전혀 합리적인 대답이 나오고 있지 않다. 왜냐하면 시스템 내부 구조 정보를 전혀 몰라도 상관없는 바이러스 침투의 사례나, 일부 외부 해커의 해킹과는 양상이 전혀 다르기 때문이다. 무려 553대의 서버가 아키텍처링 된 복잡한 하드웨어 구조와 세팅된 운영체제 버전에 관한 정보는 물론이고 그 모든 서버에 대한 최상위 접근 권한을 가진 계정 정보를 확보해야만 현실적으로 발생한 시스템 파괴의 설명이 가능하다는 것이다.

이런 엄청난 시스템 정보 수집에 근거해 삭제 명령을 담은 스크립트가 작성되고 실행이 준비되었다는 것인데, 대략 지금까지 보도로 확인된 시스템 운영상의 허점들은 몇 가지를 짚어보자. (물론 그 정도만으로는 단지 개연성을 좀 더 크게 만들 뿐 전혀 사태 발생의 확정적인 요인이라고 볼 수 없다.)

기술적인 관리 문제를 예를 들면, 허술한 비밀번호 관리다. 규정에는 3개월에 한 번씩 비밀번호를 바꾸기로 되어 있는데 최장 6년 9개월까지 비밀번호를 변경하지 않은 경우가 있었다. 바꾸었다 하더라도 누구나 추정할 수 있는 단순한 비밀번호를 사용했다는 것이다. 또한 운영과 관리를 위해서 협력 업체들이 사용하는 노트북 컴퓨터의 외부 반출이나 반입 시에는 모든 데이터를 삭제하는 것이 원칙이지만 이를 제대로 이행하지 않아 외부 반출시 심어진 잘못 된 명령어가 유입되었을 수 있다는 것이다. 더욱이 내부 정보시스템 접근을 위해 반입한 노트북으로 외부 망에 수시에 연결할 수 있게 하여 내외부 망 단절성 사실상 무의미하게 만들었다는 보도도 들린다. 또한 단 한 대의 협력업체 노트북 단말이 수백 대의 주요 서버에 직접, 간접적으로 루트 권한으로 로긴할 수 있을 정도로 업무 구획과 보안 구획이 부실했다고도 판단된다.

경영적인 관리 문제도 못지않게 허술했다. 일단 현대 캐피탈과 농협사태가 터진 후에 해당 CEO들이 보여준 사고내용에 대한 무지에 가까운 태도는 경영적으로 정보 시스템 분야가 어떤 취급을 받고 있는지 잘 알 수 있다. 농협 CEO가 “사고에 대해 보고받은 바도 없고 자신도 피해자”라는 발언은 이를 극명하게 보여준다. 정보 시스템에 심각한 장애가 발생하면 최근 경영적으로 그토록 중시 여기는 고객 서비스에 치명적인 타격을 받는다는 사실을 전혀 인지하지 못하거나 아니면 고객중심 경영이라는 것이 빈말일 가능성이 높다고 할 수 밖에 없다.

당연한 결과로 정보 시스템에 대한 예산 배분과 투자는 관련 종사자들이 수 없이 반복하듯이 대단히 빈약할 수밖에 없다. 지난해 주요 금융권의 IT 예산 가운데 보안관련 예산이 은행의 경우 3.4%, 증권 3.1%, 카드 3.6%, 보험사 2.7%에 그쳤다고 한다. 금감원에서 권고한(강제한 것이 아니라 권고한 것이다.) 5%에 모두 미치지 못한다고 할 수 있다.

이상의 몇 가지 짧은 정황만으로도 최고의 체계성과 정교함을 갖추어야 할 금융 전산 시스템이 기술적으로 경영적으로도 상상외로 느슨하고 허술한 가운데 운영되고 있었음을 알아 볼 수가 있다. 더구나 스스로 3천만 고객을 얘기할 정도로 국민의 예금을 받는 예금은행이고 온갖 최첨단 IT 하드웨어와 소프트웨어 기술이 총망라되어 적용된 곳이 은행의 전산시스템이 아니었나. 이런 환경이라면 고의적으로 치밀하게 계획을 했든 아니면 일련의 연쇄적인 실수들이 이어졌든 대형 사고가 발생할 수 있는 개연성이 있다고 판단할 수밖에 없다. 어느 경우든 서비스에 치명적인 타격을 줄 수 있고 믿고 예금을 맡긴 고객들이 심각한 피해를 입을 수 있다는 사실은 변하지 않는다.

5. ‘비용절감’, ‘효율성 중시’ 경영과 IT아웃소싱

아직 완전한 복구는 물론 문제의 파악 자체도 끝나지 않았고 검찰수사도 거의 초입 수준이지만, 재발방지와 이후 대책을 두고 의견이 분분하다. 그런데 이를 종합하면 대체로 금융 ‘보안 시스템 강화’쪽으로 모아진다. 보안 관련 투자를 실질적으로 5% 이상 하도록 강제하자든지, 최고보안책임자(CISO) 등을 새로 두어서 보안 통제를 집중하자든지, 아니면 IT 담당자에 대한 정기적인 보안기술 관련 교육을 강화하자는 식의 대책들이다. 모두 필요한 작업이기는 하다. 그러나 어쩌면 부차적일 수 있

는 기술적인 문제들이다.

대부분의 IT장애는 하드웨어적인 시스템 부실이나 시스템적인 보안장치와 관리자의 절대적 부족 때문에 발생하는 것이 아니다. 핵심은 '사람 문제'이다. 아무리 최첨단의 시스템에 철통같은 보안이 갖추어져 있다 하더라도 고의든 실수든 이를 관리 운영하는 사람과 조직의 체계와 능력에 허점이 생기면 반드시 장애는 발생하기 때문이다. 농협사태에서 보듯이 비밀번호의 주기적 변경이 시스템적 투자나 고도의 보안지식이 부족해서 발생한 것은 아닌 것이다.

이 시점에서 농협사태를 일으킨 노트북 컴퓨터가 내부 직원용이 아닌 협력업체가 시스템 운영 관리를 위해 사용하던 것이라는 사실이 밝혀지면서 새삼스럽게 유지보수 외부 의뢰나 아웃소싱 문제가 부상하고 있다. 외부 업체 직원이 핵심 시스템 권한을 가지고 있었고 이에 대한 통제 관리가 부실했다는 것이다.

금융에서 IT가 갖는 막대한 중요도와는 달리, 경영진들은 금융IT를 '핵심 경영 인프라'로 보고 있는 것이 아니라 '코스트 센터(비용소모 부서)'로 그 동안 인식해왔고 "비용을 줄여서 수익을 극대화 한다"는 경영논리의 유행에 따라 IT비용을 줄이는데 초점을 두었다. 또한 그 동안 '효율성'을 중시하는 경영추세가 IT부분에도 별 검토 없이 그대로 적용되어 가능한 '안정성' 보다는 '효율성'쪽에 무게를 실었다. 비용절감과 효율성 극대화 논리가 관철되어온 금융IT의 연장선에서 진행되어 온 것이 금융회사 IT 부분의 분사, IT아웃소싱(ITO)이었다.

표: 금융권 IT내부인력과 외부용역 현황

구분	내부인력(명)	외부인력(명)	외부용역 비중(%)
시중은행(16개)	3,518	2,722	43.6
저축은행(6개)	45	8	15.1
증권사(26개)	1,997	1,229	38.1
생명보험(22개)	836	1,523	64.6
손해보험(16개)	329	2,024	86.0
카드사(5개)	370	943	71.8
* 출처: 이성헌 한나라당 의원(2010년 8월 기준), 경향신문에서 재인용			

사실 국내적 차원의 아웃소싱이든 글로벌 아웃소싱이든 비용절감 효과를 기대하면서 유력 기업들이 아웃소싱을 활용해온 것은 어제 오늘의 얘기가 아니며 줄잡아 1990년대 말부터 일종의 유행처럼 확대되어 온 것이다. 더구나 특정산업에만 국한

된 것도 아니다. 경비나 청소 용역에서부터 콜센터 운영, 심지어 최첨단으로 절대적 시장 지배력을 행사하고 있는 아이폰도 애플의 브랜드가 찍혀 고객에게 판매되지만 전형적인 글로벌 아웃소싱으로 생산되고 있음은 잘 알려진 사실이다.

그런데 아웃소싱이 합리적인지 인 하우스(in-House)가 합리적인지는 해당 산업의 구조나 해당 업무의 성격에 따라 다양한 각도로 판단해보아야 할 문제이지 업종과 업무를 가리지 않고 무차별적으로 적용할 성질은 아니다. 또한 기업 내부적으로 아웃소싱 요건이 발생했다 하더라도 외부에 아웃소싱을 할 수 있는 시장 여건이 제대로 갖추어져 있는지도 함께 검토해 보아야 한다.

특히 '핵심 경영 인프라'로 굳어진 금융IT분야의 경우라면 검토할 사항들이 더욱 많을 수 밖에 없다. 특화되고 독립된 업무 일부 영역을 아웃소싱 하더라도 전반적인 시스템 통제와 핵심 데이터, 핵심 프로세스는 내부조직과 깊게 연계되어 움직여야 하고 내부적 의사결정체계와 긴밀하게 연계되어 하나의 완결된 체계로 통합되어 운영되어야 한다는 것이다. 그러나 이러한 '통합성'이나 '안정성'이라는 측면 보다는 '비용대비 효율성'이라는 측면만을 극대화시켜 편의적으로 ITO을 운용한다면 그 어떤 업무보다 문제가 될 소지가 크다.

정부 공식자료를 보면 아웃소싱을 하는 이유로 다음과 같이 지목하고 있는데 이는 한국의 기업들도 크게 차이가 없다.

"IT아웃소싱을 함으로써 핵심역량에 집중하면서 IT관련 비용절감과 정보시스템 성과향상이라는 목적이 달성 되리라는 판단을 하게 되면 아웃소싱을 선택할 것이다 즉 발주기관은 인소싱(In-sourcing) 함으로서 발생 가능한 여러 내부적인 갈등과 문제점을 제거하고, 경쟁우위를 획득할 수 있는 다른 차별화 요인에 발주기관의 자원을 집중적으로 투자함으로써 경쟁력을 강화하고 효율성을 극대화 할 수 있다"[4)]

주로 비용절감을 핵심 기대효과로 지목하고 있고, 반대로 위험요소는 통제력의 상실이나 보안 유지의 어려움을 꼽고 있다.(주목할 것은 단점에서 다시 비용증가 요인을 거론하고 있다는 것이다.) 그런데 이와 같은 아웃소싱의 일반적인 장단점을 금융IT에 적용하면 어떻게 될 것인가. 금융에서는 IT가 어떤 다른 집중해야 할 핵심역량 이외 요소가 아니라 그 자체가 핵심역량의 일부가 되어야 한다는 것, 그리고 '통

4) 정보화진흥원, "IT아웃소싱 운영관리 매뉴얼", 2009.12

구분	분류	상세 내용
장점	비용절감	정보시스템을 외부의 전문기관에 위탁함으로써 내부에서 운영하는 비용에 비해 저렴하게 서비스를 받을 수 있다.
	전문인력 및 전문기술 활용	외부 전문기관에 정보시스템 서비스를 위탁함으로써 전문인력의 전문기술을 활용할 수 있다.
	정확한 비용 예측	아웃소싱 계약에 따른 비용의 지급 및 향후 비용모델에 따른 비용을 지불하게 됨으로 정보시스템과 관련된 정확한 비용예측이 가능하다.
	핵심역량 강화	정보시스템에 투입되던 조직의 역량을 좀더 핵심적이고 전략적인 부문에 투입할 수 있다.
단점	비용증가 가능성	계약에 따른 계약부대 비용, 서비스수준향상을 위한 각종 비용의 지출, 아웃소싱 이전에는 비용 없이 처리되던 업무가 아웃소싱 후 비용 처리되는 경우 등 각종 비용 증가 가능성이 있다.
	우수인력 상실	인력의 이전이 수반되는 경우 내부인력 직업 안정성의 저해로 인한 퇴직과 인력의 이전 등으로 인한 내부기술 축적 미흡과 우수 인력이 상실될 가능성이 있다.
	공급업체 종속 가능성	이전된 서비스에 대하여 다시 내부로 수용하거나 제3의 업체에게 서비스를 이전하기가 어려워 교체비용이 증가될 수 있다.
	통제력의 상실	정보시스템에 대한 많은 권한이 외부업체에 이관됨에 따라 내부 정보화수준이 저하되어 외부 전문기관에 대한 통제력이 상실될 가능성이 있다.
	보안유지의 어려움	내부에서 운영되던 정보시스템이 외부 서비스 제공업체로 이전됨에 따라 각종 정보 및 기능에 대한 보안유지가 어려워질 가능성이 있다.

제 가능성과 안전성'이 오히려 비용 요소와 같은 수준이거나 더 비중 있게 중시되어야 할 업무라는 것을 고려한다면 금융IT의 장단점은 서로 역전될 수도 있는 업무가 될 수 있다는 것이다.

또 다른 측면에서 과연 금융IT 아웃소싱의 타당성(예를 들어 급변하는 정보기술 발전 환경에서 안정적으로 전문화된 기술과 인력의 공급)이 있다고 하더라도 이를 맡길 아웃소싱 시장 환경은 제대로 갖추어져 있는가. 우리나라에서 금융IT와 같은 규모가 있고 민감한 업무를 아웃소싱으로 운영해줄 수 있는 업체는 국내 재벌 계열SI 업체와 외국계 기업을 포함해서 10개도 안 되는 극소수이다. 농협도 이 범주 안의 기업이 아웃소싱을 해왔다.

그렇다면 이들 아웃소싱 수행능력이 있는 기업들의 아웃소싱 부서 직원이 모두 합쳐서 많아야 천 단위 정도에 불과할 것인데, 이들이 해당 계열사들의 아웃소싱 수행은 물론 금융회사들의 아웃소싱을 모두 수행해 줄 수 있는가. 당연히 아니다. 이들은 다시 자사 직원이 아닌 중 소 규모 외부 업체에서 인력을 공급받고 이런 식의

인력 공급사슬은 심지어 3,4단계까지 내려간다는 것은 너무나 잘 알려진 업계의 실태다. 금융회사의 '비용절감에 초점을 둔 ITO' - 극소수 ITO기업들의 '하청관행' - 2,3,4차 하청업체의 '열악한 인력공급'이 종합되면 체계를 갖춘 조직력과 조직적 업무수행능력을 보유한 금융IT운영구조가 나올 수가 없는 형편이라고 할 수 있다. 부실한 인력운용구조에서는 하드웨어적 시스템 보안 인프라가 아무리 훌륭해도 보안이 뚫리고 장애가 나는 것은 피할 수 없다.

물론 금융 전산 장애의 모든 문제를 아웃소싱 탓으로 돌릴 수는 없다. 아웃소싱과 전산 장애가 상호 깊은 연관이 있다는 것을 통계로 입증하는 것도 쉽지 않다. 그러나 모든 전산 장애를 아웃소싱 탓으로 돌릴 수는 없지만, 반대로 무분별하고 부실한 아웃소싱이 심각한 전산 장애와 보안 위험성을 상당히 안고 있다는 판단은 상당 부분 맞을 가능성이 높다는 점도 확실히 해야 한다.

전문화를 살려 부분적 아웃소싱을 한다면, 우선 금융회사들이 IT부분에 대한 경영 마인드를 바꾸는 것을 최우선 전제로 종합적인 내부 통제력과 안정적 체계를 확보하는 것이 조건이다. 그 가운데 하드웨어나 시스템 소프트웨어 의존적 ITO보다는 구획된 업무를 분할해 실질적 업무수행 능력이 있는 견실한 중견 기업에게 충분한 대가를 지불하고 특화 외주를 주는 방안이 차라리 안정성과 효율성을 달성할 수 있는 방안이 될 수도 있을 것이다.

6. 향후 재발 방지를 위해 검토해 보아야 할 과제

금융은 돈과 직접 관련이 된 업무이기 때문에 해킹이나 보안 침투 유인이 그 어디보다 강한 곳이다. 안전성이 가장 중요한 업무라는 뜻이다. 금융거래의 IT 의존도가 갈수록 높아져가는 환경에서 금융 전산망, 특히 거래 원장과 고객 정보를 포함하는 내부 핵심 시스템이 보안 위험에 노출되면 결과는 치명적이며 피해는 광범위하다.

그러나 이번 사태에서 드러난 것처럼, 대부분 금융회사들이 금융 IT 시스템을 금융수익을 내기 위해 '불가피하게 비용을 들여야 하는 외적인 기술요소'로 간주해왔던 것도 다시금 확인되었다. 그 연장선에서 최소 비용을 지불하려는 유인이 발생했고 보안관련 투자와 관리도 부실했으며, 치밀한 내부 연계성과 종합적 기준 없이 아웃소싱에 의존했던 것도 사실이다. 이런 상황에서 현재 금융 전산망이 매우 취약하다

는 사실이 속속 확인되고 있다.

다방면적인 대책이 필요하다. 우선 경영진들부터 금융IT는 '핵심 경영 인프라, 핵심 고객서비스 통로'라는 경영정책상의 변화를 주어야 한다. 대부분의 경우 IT 보안과 안전성의 핵심 요소는 하드웨어나 기술적인 것이 아니라 사람 문제이고 조직의 시스템 관리 체계와 능력의 문제이다. 그에 상응하는 권한과 책임, 조직 구조를 짜야 한다. 아웃소싱 확대가 보안 위험의 전부는 아니지만 현재 왜곡된 아웃소싱 시장구조는 보안 취약성을 노출시킬 가능성을 상당히 높이고 있는 것도 사실이다. 엄격하게 재검토하고 제대로 기준을 재설정 할 필요가 있다.

금융회사들의 효율성과 수익성 중시 경영이 이번 사태를 계기로 급격히 전환될 가능성은 커 보이지 않는다. 그렇다면 예금을 맡긴 고객, 즉 국민들에게 은행들의 전산장애가 미칠 광범위한 피해를 감안하여 정부가 보다 엄격한 금융IT 관리 기준을 정할 필요가 있다. 강제력도 없는 5% 보안투자 권고안 수준으로는 어렵다.

마지막으로 짚어둘 것은 이미 피해는 발생했다는 사실이다. 이번 경우에는 피해 고객이 특정하게 제한되지도 않았고 때문에 명료하게 피해를 입증하기도 쉽지 않다. 구체적 피해가 확인되면 배상한다는 식의 전례를 적용하겠다고 농협이 나오면 다수의 피해사례는 묻혀버릴 수 있다. 더욱이 고객 정보 유출이나 IT보안위험 노출 등의 장애로 소송을 한 경우 승소를 한 경우가 매우 적다는 사실도 감안해야 한다. 마치 금융회사의 불완전 판매를 입증하여 피해 배상을 받기가 어려운 경우와 유사하다고 할 수 있다. 이번 사건을 계기로 피해를 좁게 해석할 것이 아니라 보다 확장하여 포괄적으로 규정하는 법과 제도를 만들 필요도 있다. 정부가 고민해야 할 대목이다.

* 이 글은 지난 4월 28일 사무금융노련 주최 토론회 발제문을 보완한 것입니다.