참여연대 토론회

10.26 재보궐 선거시 중앙선관위 인터넷서비스 장애 어떻게 볼 것인가

일시 | 2012년 2월 23일 (목) 오후 2시

장소 | 참여연대 B1 느티나무홀

주최 | 참여연대

프로그램

14:00 사회 장유식 변호사

14:10 발표 1 **DDoS 사태 이후 중앙선관위의 입장과 평가**

송봉섭 중앙선거관리위원회 의정지원과장

14:30 발표 2 **중앙선관위 공개 자료의 1차 분석 결과와 남은 과제들**

김기창 고려대 법학전문대학원 교수, 변호사, Openweb 대표

14:50 지정토론 박혁진 중앙선관위 정보화담당관

김유승 중앙대 문헌정보학과 교수

동네북의 난(네티즌, 네트워크 보안 전문가)

아고라 샤 (유권자자유네트워크 네티즌 집행위원)

황규만 (진보네트워크센터 서버 관리자)

15:30 휴식

15:40 종합 토론

16:30 폐회

목 차

여타 토론자는 현장 토론

발제 1

DDoS 사태 이후 중앙선관위의 입장과 평가

송봉섭 / 중앙선관위 의정지원과장

참여연대 주최 공청회
(2012. 2. 23.)

DDoS 사태 이후 중앙선관위의 입장과 평가

중앙선거관리위원회
(의정지원과장 송봉섭)

차 례

Ⅰ. 들어가며

하루에 수십 대의 차량이 운행되는 것을 예상하고 만든 2차선 도로에 어느 날 갑자기 수만 대의 차량이 나타나면 어떻게 될까? 도로는 단순 정체를 넘어서 주차장으로 변할 것이고, 결국 오도 가도 못하는 통행불능에 빠질 것이다. 이와 같은 현상은 온라인에서 발견된다. 바로 분산서비스거부(Distribute Denial of Service), 다른 말로 '디도스(DDoS) 공격'이라고 불리는 트래픽의 일종이다.

DDoS 공격은 수십 대에서 수백만 대의 PC를 원격 조종해 특정 웹사이트에 동시에 접속시킴으로써 단시간 내에 과부하를 일으키는 행위를 뜻한다. 공격자들은 서버나 네크워크 대역이 감당할 수 없는 많은 양의 트래픽을 순간적으로 일으켜 일반사용자들의 사이트 접근 및 사용이 차단된다. DDoS 공격의 목적은 자료를 유출하거나 삭제하는 것이 아니라 단순히 서버를 마비시키는 것이다. 하지만 지속적인 서비스 운영이 필수인 관공서 웹사이트는 서버가 단 몇 시간만 마비되어도 치명적인 피해를 입을 수 있다는 점에서 그 심각성이 크다.

최근 인터넷 보안체계를 공격하는 양태는 네트워크 및 시스템 자원을 모두 소비해서 실제 자원을 사용해야 하는 사용자가 서비스를 받을 수 없게 하는 이 DDoS 공격방법이 주를 이루고 있다. DDoS 공격의 인지는 시스템이나 네트워크가 느려지거나 접속 불능의 상태 또는 CPU, 메모리 사용량 등을 통해 인지할 수 있다.

2011. 10. 26. 서울시장보궐선거의 선거일에 DDoS 공격으로 인해 중앙선거관리위원회(이하 '중앙선관위'라 함) 홈페이지가 일시 접속이 지체되는 현상이 발생[1]하였다. 이러한 접속 지체의 발생 초기에 중앙선관위 직원들의 자체대응과 통신망사업자(KT)와의 협력(사이버대피소 이용)을 통해 시스템을 정상화했으나, 장애발생 및 복구시간 지연으로 인해 홈페이지에 접속하려는 유권자들이 많은 불편을 겪은 것이 사실이다. 중앙선관위는 시스템 복구 즉시 공식 입장을 발표하는 한편, 동 사안을 '경찰청 사이버테러대응센터'에 수사의뢰한 바 있다.

---

1) 김학재의원이 대표발의한 특검법안에 의하면 "한나라당 최구식 의원 비서 공현민 등은 지난 10. 26. 재·보궐선거의 투표율을 낮춰 나경원 한나라당 후보에게 유리하도록 하기 위하여, 중앙선거관리위원회 및 박원순 홈페이지에 대한 DDoS 공격을 감행하기로 공모한 후, 공현민은 재·보궐선거일 전일 고향 후배인 강모씨에게 전화를 걸어 중앙선거관리위원회 및 박원순 홈페이지에 대한 DDoS 공격을 지시하였고, DDoS 공격으로 인하여 중앙선거관리위원회 홈페이지와 박원순 홈페이지는 2011. 10. 26. 새벽 1시경부터 접속 장애를 일으켰으며, 중앙선거관리위원회 홈페이지는 오전 6시쯤부터 오전 8시 32분까지 접속 불능 상태가 되었다"고 주장하고 있음.

경찰과 검찰의 수사결과에 의하면 “2011. 10. 26. 당시 중앙선관위 홈페이지 장애의 원인이 DDoS였고, 내부 DB가 끊어진 적이 없으며, 내부 공모 혐의는 전혀 사실이 아니다”라고 발표하였고, 우리 위원회에서의 분석결과도 같은 결과를 공표하였음에도 의혹이 해소되지 않고 확대, 재생산되고 있음은 매우 유감스러운 일로 안타까운 일이라 아니할 수 없다.

㈜LG엔시스가 작성한 디도스 분석 보고서[2]에 따르면, “디도스 방어장비가 디도스 공격은 정상 방어했고 공격 트래픽의 패턴을 보이지 않는 일반 이용자의 정상적인 접속은 차단되지 않았다”고 적시되어 있는 바, 이는 DDoS 장비가 DDoS 트래픽을 정상적으로 차단하였음에도 홈페이지 접속 장애가 있었던 것은 정상 서비스 요청(트래픽)이 DDoS 트래픽에 묻혀 홈페이지에 도달하지 못하였기 때문이며, 간헐적으로 DDoS 트래픽을 뚫고 홈페이지에 접속된 경우도 일부 있었음을 의미한다.

2009. 7. 7. DDoS 공격에 이어, 2011. 3. 4. 공공기관・금융기관・포털 등 다수의 홈페이지에 대한 DDoS 공격으로 산업기밀 유출, 전산 시스템 장애 등 다양한 침해사고가 발생하였을 뿐만 아니라 수천만 건의 개인정보가 유출되는 사고가 발생하였음에도 결과 발표에 대규모의 의혹이 없었으나, 이번 사건에서는 의혹이 그치지 않는 것은, 한편으로는 그만큼 선관위에 관심이 많고, 앞으로 공직선거를 완벽하게 관리하여 자유롭고 공정한 선진 민주선거를 구현하라는 국민들의 바람이라 생각된다.

2012. 2. 15. 참여연대가 LG엔시스 작성 ‘재보궐선거 서비스장애 분석보고서’의 일부 내용을 거론하면서 “그간 제기되어 온 ‘선관위 홈페이지 장애가 디도스 공격 때문이 아닐 수 있다’는 의혹이 단순 괴담이 아니라 사실일 수도 있다”라고 발표함으로써 의혹의 불에 기름을 끼 얹은 꼴이 되었다.

따라서 본 발제에서는 그동안 제기되어 온 이 사건이 DDoS 공격이 아니라는 설과 선관위 내부 직원 가담설, 투표율을 저하시켜 특정 후보자를 위한 투표소 변경설, 부재자투표에서의 선거부정설 등 근거 없는 의혹에 대한 중앙선관위의 대응과 입장을 밝히고, 그에 대한 평가 및 추후 발생될 수 있는 사이버 공격에 대한 대책에 대하여 기술하고자 한다.

---

2) 2011년 10월 26일 재보궐선거서비스 장애 분석 보고서(2011. 11. 26. 작성)

Ⅱ. DDoS 공격에 따른 장애발생 및 대응

1. DDoS 공격 당시 전산시스템 운용실태

우리 위원회는 전국 단위로 실시되는 임기만료선거시에는 사이버위협으로부터 시스템을 보호하기 위하여 2개월 정도 보안전문업체를 통해 24시간 보안 관제를 실시하였으나, 평상시와 재·보궐선거의 경우에는 예산확보 등에 어려움이 있어 사이버대피소를 구축하지 않는 등 전문적 보안관제를 실시하지 못하고 자체 보안시스템을 운용하고 있었다.

사이버공격에 대비한 일반적인 보안시스템은 DDoS 방어장비, 침입방지시스템(IPS), 방화벽, 침입탐지시스템(IDS), 웹방화벽 등 5단계로 구성·운영하고 있는 바, 2009년 이후 DDoS 방어장비 2대를 구축·운영 중에 있고, 2010년에는 DDoS 공격에 대비하여 모의훈련을 2회 실시하여 이를 보완하였으며, 2011. 3월에는 「DDoS 공격 대응지침」을 마련하여 현재까지 시행하고 있다.

2011. 10. 26. 서울시장보궐선거기간 중에는 앞서 언급한 바와 같이 예산부족으로 사이버대피소를 구축하지 못하고 자체 보안시스템을 운용하면서 통신회선을 30M에서 465M로 증속하여 통신량 증가에 대비하였다.

< 표 2-1 > 선거별 통신회선 용량

(단위 : bps)

년 도	선거(투표)명	회선용량	최대이용량	비 고
2008	제18대 국회의원선거	465M	137M	155M/3회선
2010	제5회 동시지방선거	1.15G	491M	1G/1회선, 155M/1회선
2011	상반기 재·보궐선거	300M	153M	100M/3회선
〃	서울시 주민투표	355M	167M	155M/2회선, 45M/1회선
〃	하반기 재·보궐선거	465M	-	155M/3회선

* 평상시 통신회선 운영 용량 : 30Mbps(bps : bit per second)

한편, DDoS 공격 당시 우리 위원회는 이미 마련한 'DDoS 대응 매뉴얼'의

규정에 따라 단계별 조치를 취하였고, 공격이 시작된 시기부터 공격탐지 및 확인, 초동조치, 적극적인 조치를 통한 정상화 처리단계로 조치하였다. 다만, 공격 IP 주소를 차단하고, 공격이 집중되는 통신회선(KT)을 단절 시키는 등 조치를 취하였으나, 이번과 같은 대용량 트래픽 공격을 현재 보유중인 DDoS 방어 장비와 통신회선 증속으로는 완전한 차단이 어려워 초동조치 단계에서 시간이 지연되어, 전체적인 부분에 있어 처리가 원활하지 못했음은 유감스러운 일이다.

2. 전산시스템의 장애 발생 및 주요 조치사항

1) 장애발생 및 복구

2011. 10. 26. 05:50경 중앙선관위 홈페이지에 1차로 접속이 지체되는 현상이 발생(자체인지)하여 06:58경 2개 회사의 회선[3]을 사용하고 있던 것을 KT 인터넷 회선은 단절 조치하였고, LG U+ 서비스만 연결되도록 하였다. 이로써 중앙선관위 홈페이지는 1차 정상화되었다. (07:10~07:35, 25분간)

그러나 당일 07:35경 중앙선관위 홈페이지에 2차로 접속이 지체되는 현상이 발생하였는 바, 08:20경 KT 국가망운용실 (임시)사이버대피소로 홈페이지를 우회 요청하여 08:32경 중앙선관위 홈페이지 인터넷서비스의 2차 정상화가 이루어졌다.

2) 추가 대응상황

○ 08:30경 언론·홈페이지를 통해 장애 및 복구사실 안내·홍보

○ 10:00 경찰청 사이버테러대응센터에 수사의뢰 (서면접수는 14:18경)

○ 12:57 DDoS 공격이 소멸됨에 따라 KT 사이버대피소 우회조치 해제

○ 13:17 투표마감 및 개표 시간대 공격에 대비 회선 증속 (310M⇨1G)

※ 상황발생 및 세부 대응일지 : 덧붙임 1참조

3) 인터넷회선 현황 : 465M [KT 2회선(310M), LG U+ 1회선(155M)]

3. 시간대별 DDoS 공격 당시 대응상황

- ❍ 투표 개시 전 접속지체 자체 인지(05:50) 후, 통신회선·장비 등 점검 및 국정원 등 관계기관과의 협의, 상황파악(06:20경)
- ❍ 06:58경 DDoS 공격으로 추정하고 주요 공격 IP에 대한 수동차단 조치 및 KT 회선차단 검토 ⇨ KT 회선 차단, LG U+망만 운영 ⇨ 홈페이지 서비스 1차 정상화(07:10)
- ❍ 07:35 이후 LG U+망도 공격받게 되어 KT측과 협의, (임시)사이버대피소로 우회조치 ⇨ 2차 정상화(08:32)
- ❍ 다만, 최초 인지 후 공격탐지 및 확인단계를 거쳐 공격이 집중되었던 KT 회선을 차단하기까지의 초동조치와 자체 사이버대피소가 구축되어 있지 않은 관계로 KT측으로부터 (임시)사이버대피소를 할당받아 우회조치 하는데 있어 절차상 불가피한 시간이 소요되었다.

4. DDoS 관련 수사결과 및 특검법 추진상황

1) 경찰청[4)]

2011. 12. 9. 경찰청은 "유권자들이 투표소를 찾지 못하도록 선관위 홈페이지를 다운시키면 서울시장 보궐선거에서 나경원 후보에게 유리할 것으로 생각하고, 평소 알고 지내던 피의자 강모씨에게 전화를 걸어 선거관리위원회·박원순 후보 홈페이지를 DDoS 공격케 하여 마비시킨 것으로 밝혀졌다"고 수사결과를 발표하고 이 사건을 검찰에 송치하였다.

또한, 선관위 내부자 관여 및 DB 고의차단 여부에 대하여 "사건 발생 즉시, 사이버 수사관을 선관위에 급파하고 선관위로부터 사건 당시 로그파일을 제출받아 분석한 바, DDoS 공격 외 기타 다른 원인을 발견하지 못하였다. 웹서버와 연결된 DB서버 상태와 로그기록 등을 분석해 본 결과 임의로 연동을 차단한 흔적도 발견하지 못하였다"고 발표하였다.

---

4) 2011. 12월 경찰청 브리핑자료(사이버테러대응센터장 총경 이영상, ☏ 02-3159-1605)

2) 검찰청[5]

○ 중앙선관위 내부의 공모 의혹에 대하여

일부에서, 중앙선관위 홈페이지(nec.go.kr)에 정상 접속 후 링크를 통해 '내 투표소 찾기' 웹페이지(info.nec.go.kr)에 접속하지 못한 사례가 발생한 것은 중앙선관위 내부에서 투표소 검색 DB와의 연동을 차단한 증거라는 의혹을 제기[6]하였으나 10. 1.~31. 중앙선관위 및 통신사(KT, LG)의 라우터(4대) 로그, DDoS 대응장비(2대) 로그, 네트워크 방화벽(2대) 로그, 침입탐지시스템(2대) 로그, 침입방지시스템(2대) 로그, 투표소 검색 및 홈페이지 관련 웹서버(7대) 로그, DB접속 및 운영 로그 등을 확보하여 교차 분석한 결과,[7] DDoS 공격 당시(1차 01:01~01:43, 2차 05:53~08:54) 의도적으로 중앙선관위 홈페이지와 DB서버의 연동이 되지 않게 하거나, 각 서버를 다운시키거나, 투표소 검색 관련 테이블을 삭제하거나, DB접속을 못하게 한 흔적이 없었고, '내 투표소 찾기' 웹페이지인 선거정보조회 서버의 10. 26.자 웹 접속 로그 분석 결과 정상적으로 서비스된 사실[8] 확인되어, 위와 같은 사례는 DDoS 공격의 본질상 좀비PC들에 의한 트래픽 양이 일정하지 않아 공격 당시 접속 장애 상태가 균일하지 못한 데에서 비롯된 것으로 파악하였다.

○ 중앙선관위의 고의적 장애 상태 방치 의혹에 대하여

중앙선관위는 정보보안을 위하여 DDoS 대응 장비를 포함하여 정보보안 시스템을 구축[9], 운용하여 왔고, 10. 26 재보궐선거 당시 트래픽 증가에 대비하여 회선용량 증속 조치하였다[10]. 중앙선관위는 장애 복구를 위해 DDoS 공격 IP 차단(06:25) 및 트래픽 우회조치(06:58)로 일시 정상 복구(07:10~07:30)되었으나, 지속적인 DDoS 공격으로 장애가 계속되자 KT 국가망운용실 사이버대피소로 대피하여 홈페이지 정상 복구(08:32)하였다.

---

5) 2012. 1월 서울중앙지방검찰청 보도자료(제3차장검사 윤갑근, ☏ 02-530-4304)

6) '내 투표소 찾기' 웹페이지(info.nec.go.kr)는 그 웹주소를 정확히 알고 있을 경우 중앙선관위 홈페이지(nec.go.kr)를 거치지 않고 직접 접속할 수 있지만, 대부분의 경우 중앙선관위 홈페이지를 통해 링크 방식으로 접속

7) 장비 및 서버 : 10종 23대 / 로그 및 설정 파일 : 1,620개(약 5억5천만행)

8) 일반 웹페이지를 통한 투표소 검색 : 181,090건의 요청 중 576건 오류 처리, 모바일 접속 페이지를 통한 투표소 검색 : 30,555건의 요청 모두 정상 처리

9) 중앙선관위는 행정부가 아니므로 국정원의「국가정보통신보안 기본지침」이 적용되지 않고, 다만 위 기본지침을 참고한 내부지침을 제정, 시행 중이며, 필요시 국정원에 보안성 평가 의뢰하고 있음

10) 2011. 10. 5.경 10Mbps 3회선을 155Mbps 3회선으로 증속

○ 투표소 고의 변경 의혹에 대하여

일부에서, 2010. 6. 2. 제5회 전국동시지방선거, 2011. 8. 24. 서울시 주민투표, 2011. 10. 26. 지방자치 재보궐선거를 비교하면 야당 득표율이 높은 서대문구·금천구의 투표소 변경율이 강남구에 비해 높고, 이는 서울시선관위의 의도적인 조치라는 의혹을 제기하였으나, 투표소는 공직선거법 제147조에 따라 그 투표구를 관할하는 읍·면·동선관위가 투표의 편리성을 검토하여 설치하며, 중앙선관위 업무편람에 따르면 서울시의 경우 洞선관위의 투표소 설치에 대해서는 區선관위가 실사하는 것으로 규정되어 있다. 또한, 洞선관위와 區선관위를 비롯한 각급 선관위 구성에는 선거관리위원회법 제4조에 따라 야당도 포함된 국회 교섭단체가 참여하므로, 위와 같은 의혹은 합리적 근거가 없다.

○ 헌정사상 유례가 없는 선거테러 사건에 대해 검찰은 국민적 의혹을 해소하고 사건의 실체를 규명하기 위하여 외부 전문기관의 공동 검증 등 가능한 모든 과학수사 역량을 투입하여 수사에 임하였다.

3) 국　　회[11)]

김학재의원이 대표발의한 「한나라당 관련자들의 중앙선거관리위원회와 박원순 홈페이지에 대한 사이버테러 진상규명을 위한 특별검사의 임명 등에 관한 법률안」과 이두아의원이 대표발의한 「2011. 10. 26 재보궐선거일 중앙선거관리위원회 홈페이지에 대한 디도스 공격 사건 진상규명을 위한 특별검사의 임명 등에 관한 법률안」을 심사한 결과 법제사법위원회 제2차(2012. 2. 8) 회의에서 본회의에 부의하지 아니하기로 하고, 「2011. 10. 26 재보궐선거일 중앙선거관리위원회와 박원순 서울시장 후보 홈페이지에 대한 사이버테러 진상규명을 위한 특별검사의 임명 등에 관한 법률안」을 국회법 제51조에 따라 법제사법위원회 대안으로 제안하여 통과시켰으며, 2012. 2. 14. 국무회의에서 의결한 후 2012. 2. 22. 공포되었다.

이 법은 중앙선거관리위원회와 박원순 서울시장 후보 홈페이지에 대한

11) 2012. 1월 서울중앙지방검찰청 보도자료(제3차장검사 윤갑근, ☏ 02-530-4304)

사이버테러에 대한 진상규명을 위하여 독립적인 지위를 가지는 특별검사의 임명과 직무 등에 관하여 필요한 사항을 규정함을 목적으로 하며, 특별검사의 수사대상은, 1. 중앙선거관리위원회와 박원순 서울시장 후보 홈페이지에 대한 사이버테러 관련 한나라당 국회의원, 비서 등 정치인이나 단체 등 제3자 개입 의혹, 2. 제1호의 의혹사건과 관련된 자금의 출처 및 사용에 대한 의혹, 3. 경찰의 수사과정 및 검찰 수사에 있어 청와대 관련자나 이 사건과 관련된 기관의 의도적인 은폐, 조작 및 개입, 그 밖의 의혹, 4. 제1호부터 제3호까지의 의혹 등과 관련되어 수사과정에서 인지된 관련 사항으로 하여 입법되었다.

Ⅲ. 선관위 관련 의혹제기내용

중앙선관위가 DDoS 공격으로 인하여 피해자임에도 불구하고 합리적인 근거 없이 선관위가 부정을 저질렀다고 의혹을 제기하는 것은 국민에게 선관위와 선거에 대해 불신을 주어 선거에서 선출된 대표자를 인정하지 않음으로써 결국, 국민에게 그 피해가 전가될 수 있으므로 신중을 기할 필요가 있다. 현재 일부에서 제기하는 중앙선관위 홈페이지 DDoS 공격에 대한 의혹을 살펴보고자 한다.

첫째, 중앙선관위 홈페이지 전체가 마비된 것이 아니라 '투표소 찾기'메뉴만 작동하지 않은 것은 DDoS 공격이 아니라 해킹이나 선관위 내부자의 공모가 이루어졌기 때문이다.

둘째, 중앙선관위 홈페이지는 접속되었으나, '투표소 찾기' 등 일부 서비스만 접속이 안되었던 것은 중앙선관위 홈페이지 데이터베이스(DB) 서버를 고의로 끊었기 때문이다.

셋째, 로그파일 기록 및 DDoS 공격과 관련한 자료를 국민들에게 공개하지 않는 것은 선관위 직원이 연루되었기 때문이며, 최근 전산시스템 개선·보완이라는 명목하에 중앙선관위 홈페이지 로그기록 등을 조작하는 한편, 시스템 등을 교체하여 관련 증거를 은폐하려 하고 있다.

넷째, 2011. 10. 26. 서울시장보궐선거에서 선관위가 특정 후보자에게 유리하게 하기 위하여 투표율을 낮추기 위한 목적으로 투표소를 변경하였다. 특히, 야권 지지율이 높은 지역의 투표소 변경비율이 훨씬 높았다.

다섯째, 10. 26. 서울시장보궐선거에서 중앙선관위 홈페이지상에서 '투표소 찾기 서비스'를 이용하는 경우 이전까지 요구하지 않았던 선거인의 주민등록번호를 입력하는 절차를 추가함으로써 투표소 찾기를 그만 두게 하거나 심히 불편하게 하기 위한 의도된 수정이다.

여섯째, 10. 26. 서울시장보궐선거에서 ○○○ 후보자가 낙선되었음에도 진보성향의 20대가 많은 부재자투표에서 ○○○ 후보자가 25개 구에서 모두 승리한 것은 고의적인 부재자투표 개입 등 투표부정이 없었다면 납득할 수 없는 일이다.

Ⅳ. 선관위 관련 의혹제기에 대한 입장 및 보완대책

1. 선관위 관련 의혹제기에 대한 입장

첫째, 이번 사건이 DDoS 공격이 아니라는 주장에 대하여

우리 위원회가 공개한 기술분석보고서에 의하면, DDoS 공격이 발생하여 DDoS 방어장비와 방화벽 장비에서 공격 트래픽을 차단하여 서버 등을 보호하였으나, 회선대역폭 고갈 현상에 의해 서비스 장애가 발생한 것으로 확인하였다. 즉, DDoS 장비가 DDoS 트래픽을 정상적으로 차단하였음에도 홈페이지 접속 장애가 있었던 것은 정상 서비스 요청(트래픽)이 DDoS 트래픽에 묻혀 홈페이지에 도달하지 못하였기 때문이며, 간헐적으로 DDoS 트래픽을 뚫고 홈페이지에 접속된 경우도 있었다고 설명하였다.

또한, ㈜LG엔시스가 작성한 디도스 분석 보고서에 따르면, “LG엔시스의 디도스 방어장비가 디도스 공격은 정상 방어했고, 공격 트래픽의 패턴을 보이지 않는 일반 이용자의 정상적인 접속은 차단되지 않았다”고 주장하고 있다. 이는 DDoS 공격 당시 중앙선관위의 시스템 내부에서 서버 연동을 차단하거나 내부 시스템이 다운되지 않았다는 중앙선관위의 일관된 주장을 뒷받침하고 있다.

경찰・검찰의 수사결과에서도 2011. 10. 26. 당시 홈페이지 장애의 원인이 DDoS였고, 내부 DB가 끊어진 적이 없으며, 내부 공모 혐의는 전혀 사실이 아님이 확인되었고, 곧 특검의 수사를 통해서도 선관위가 무관하다는 사실이 입증될 것으로 판단한다.

둘째, 중앙선관위 홈페이지는 접속되었으나 ‘투표소 찾기’ 등 일부서비스가 접속이 안되었다는 주장에 대하여

2011. 10. 26. 05시 50분경 회선 용량을 고갈시키는 DDoS 공격이 발생하여 대부분의 사용자는 접속이 원활하지 않은 현상이 발생하였고, 일부 사용자의 경우 우리 위원회 홈페이지의 초기화면에는 접속이 가능하였으나 ‘투표소 찾기 서비스’를 이용하고자 재접속하는 경우에 접속이 되지 않거나

지연되는 현상이 발생하였다.

이러한 현상은 DDoS 공격에 의해 발생할 수 있는 접속 불능 또는 지연 때문에 일어난 것으로써 DDoS 공격을 받는 사이트에서 흔히 일어날 수 있는 일반적인 상황이다.

또한, 서울시선관위는 “투표소 변경에 따른 혼란방지와 선거인의 투표편의를 위하여 2011. 8. 24. 주민투표 당시의 투표소를 우선적으로 선정하되, 투표소 변경이 있는 때에는 안내현수막 게시 등을 통해 안내하라”고 지시하였다. 실제 선거현장에서도 선거일전 10일까지 동사무소 게시판 등에 투표소의 명칭과 소재지를 공고하였고, 매세대에 선거인명부확정일 후 2일까지 투표장소 등을 게재한 투표안내문을 우편 발송한 외에 안내현수막 설치, 안내벽보 게시, 안내도우미 배치, 구청 홈페이지에 안내문 게시, 각 후보자측에 투표소현황 등을 문서로 안내하였다.

따라서 중앙선관위 홈페이지상의 ‘투표소찾기서비스’를 이용하지 않고도 다양한 방법으로 투표소를 찾을 수 있었으므로 일부 유권자의 경우 약간의 불편을 초래하였을지는 몰라도 투표소를 찾지 못하게 하기 위하여 ‘투표소 찾기 서비스’를 접속되지 않게 하였다는 주장은 일고의 가치도 없다.

셋째, 이번 사건은 DDoS 공격때문이 아니라 선관위 홈페이지 데이터베이스(DB) 서버를 고의로 끊었기 때문이라는 주장에 대하여

DDoS 공격이란 공격자가 불특정 다수의 좀비PC를 감염시킨 후, 이를 이용하여 대량의 트래픽을 일으켜 특정 서버를 다운시키거나 인터넷 회선을 점유하여 서비스를 불가능하게 만드는 것으로서 2011. 10. 26. DDoS 공격 당시 네트워크 수용 용량이 310Mbps인 우리 위원회 홈페이지에 1Gbps의 트래픽이 유입되어 병목현상이 발생하여 정상서비스를 제공하지 못하였다. DDoS 장비를 포함한 5단계 방어장비가 공격트래픽을 차단했기 때문에 홈페이지 서버, 데이터베이스(DB) 서버 등 내부서버는 피해를 입지 않아 정상적으로 작동하고 있었다.

데이터베이스(DB) 서버의 로그기록 등을 분석한 결과, 데이터베이스 시스템(DBMS)은 모두 정상 작동되고 있었으므로 데이터베이스(DB)를 고의로

끊었다는 주장은 사실이 아닐 뿐만 아니라, 웹서버와 데이터베이스(DB) 서버간의 연결 상태도 정상으로 작동하고 있었음이 명백하다. 이는 검찰 및 경찰 수사에서도 데이터베이스(DB) 서버가 정상작동하고 있었던 것으로 재차 확인된 사항이다.

넷째, 중앙선관위 홈페이지 DDoS 공격과 관련하여 내부직원이 연루되었다는 주장에 대하여

선관위 직원이 연루되었다는 주장은 2011. 10. 26. 서울시장보궐선거시 중앙선관위 홈페이지 장애의 원인이 DDoS 공격이 아니거나 DDoS 공격과 병행하여 데이터베이스(DB) 서버를 누군가가 고의로 끊었다는 것을 전제로 한 것이다. 그러나 앞서 설명한 바와 같이 데이터베이스(DB) 서버가 끊어져 있었다는 주장 자체가 사실이 아님이 명백하므로 중앙선관위 내부직원이 연루되었다는 주장 또한 사실이 아니다.

수사기관에서도 이 부분에 대해 사실여부를 밝히기 위해 수사하였으며, 특히, 검찰 수사에서는 10종 23대의 장비·서버와 1,620개(약 5억 5천만 행)에 이르는 방대한 양의 로그 및 설정파일을 조사하는 한편, 중앙선관위 데이터베이스(DB) 서버 접근권한을 가진 시스템운영 및 정보보호담당 직원 4명을 각각 7 ~ 10시간에 이르는 강도 높은 조사를 하였으나, 어떠한 연루 의혹도 사실이 아님이 확인되었다.

우리 위원회는 'DDoS 대응 매뉴얼'에 의해 단계별 조치를 취하였으며, 공격이 시작된 시기부터 공격탐지 및 확인, 초동조치, 적극적인 조치를 통하여 정상화 처리단계로 조치하였으나, 다만, 공격 IP 주소를 차단하고, 공격이 집중되는 통신회선(KT)을 단절 시키는 등 초동조치 단계에서 시간이 지연되어 전체적인 부분에 있어 처리가 원활하지 않은 측면도 있었다.

상식적으로 생각해 보아도 공무원인 내부 직원이 연루되었다는 것은 그 직원에게 어떤 보상이나 이익이 있어야 하는데 승진이나 금전수수 등 대가가 없었고, 파면과 형사처벌을 감수하면서 이 사건 범죄를 저지른다는 것은 도저히 납득이 되지 않는 부분이다.

다섯째, 로그기록 및 DDoS 공격과 관련한 자료를 공개하지 않는다는 주장에 대하여

로그기록 공개와 관련하여,「공공기관의 정보공개에 관한 법률」 제9조[12]와「통신비밀보호법」제3조[13]에서 로그기록 자료의 공개를 제한·금지하고 있으므로 누구보다도 법을 준수하고 법을 엄정히 집행하여야 하는 우리 위원회로서는 일반국민에게 로그기록을 부득이 공개하지 못했음을 이해해 주시기 바란다.

그러나 2011. 10. 26. DDoS 공격 당일 수사의뢰와 동시에 경찰청 사이버대응테러센터에 관련기록 일체를 제공하였고, 2011. 12. 8. 검찰청의 요구에 의해 관련자료 일체를 다시 한 번 서울지방검찰청에 제공한 사실[14]이 있다.

일부에서 로그파일의 공개가 어렵다면 관련 자료라도 공개하라는 요구가 있어, 우리 위원회는 2011. 12. 23. 국회 행정안전위원회에 출석하여 DDoS 관련 현안보고를 하였고, 2011. 12. 13. 학계와 업계의 보안전문가들을 초청하여 내부 기술분석 자료를 공개하였으며, 12. 29.에는 국회에서 국

---

12) 제9조(비공개대상정보) ①공공기관이 보유·관리하는 정보는 공개대상이 된다. 다만, 다음 각 호의 1에 해당하는 정보에 대하여는 이를 공개하지 아니할 수 있다.
1. 다른 법률 또는 법률이 위임한 명령(국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙·대통령령 및 조례에 한한다)에 의하여 비밀 또는 비공개 사항으로 규정된 정보
2. ~ 3. (생략)
4. 진행중인 재판에 관련된 정보와 범죄의 예방, 수사, 공소의 제기 및 유지, 형의 집행, 교정, 보안처분에 관한 사항으로서 공개될 경우 그 직무수행을 현저히 곤란하게 하거나 형사피고인의 공정한 재판을 받을 권리를 침해한다고 인정할 만한 상당한 이유가 있는 정보
5. ~ 8. (생략)

13) 제2조 (정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.
1. ~ 10. (생략)
11. "통신사실확인자료"라 함은 다음 각목의 어느 하나에 해당하는 전기통신사실에 관한 자료를 말한다.
가. 가입자의 전기통신일시
나. 전기통신개시·종료시간
다. 발·착신 통신번호 등 상대방의 가입자번호
라. 사용도수
마. 컴퓨터통신 또는 인터넷의 사용자가 전기통신역무를 이용한 사실에 관한 컴퓨터통신 또는 인터넷의 로그기록자료
바. 정보통신망에 접속된 정보통신기기의 위치를 확인할 수 있는 발신기지국의 위치추적자료
사. 컴퓨터통신 또는 인터넷의 사용자가 정보통신망에 접속하기 위하여 사용하는 정보통신기기의 위치를 확인할 수 있는 접속지의 추적자료
12. (생략)
제3조 (통신 및 대화비밀의 보호) ①누구든지 이 법과 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열·전기통신의감청 또는 통신사실확인자료의 제공을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다. 다만, 다음 각호의 경우에는 당해 법률이 정하는 바에 의한다.
1. ~ 5. (생략)

14) 선거당일 수사의뢰시 수사 목적으로 제공한 것을 포함하여 검찰과 경찰에 총 20회에 걸쳐 80여건을 제공하였음.

회의원 보좌진을 대상으로, 2012. 1. 18. 정당 및 사이버 유관기관·단체 등을 대상으로 DDoS 공격 관련 자료를 제공하면서 이를 설명하였고, 2012. 2. 11. 참여연대에 LG엔시스에서 작성한 '재보궐선거 서비스 장애분석 보고서'를 제공하는 등 제한적으로나마 이미 DDoS 공격 당시의 로그기록 분석자료를 공개한 바 있다.

우리 위원회는 그 동안 로그기록은 통신기록 뿐만 아니라 시스템 정보 등 중요한 정보들을 포함하고 있어 공개될 경우에는 보안상 중대한 위험이 초래될 가능성이 있고, DDoS 공격의 전 과정을 검증하기 위해서는 선관위 로그파일 외에 통신사 로그파일의 확인도 필요하기에 일부만 공개하였다.

또한, 강제수사를 통한 IP 추적 등이 없이 단순히 방대한 규모의 로그파일에 대한 체계적인 검증이 곤란하고, 선관위의 로그기록 공개가 수사와 재판에 영향을 미칠 수 있다는 우려도 전면적인 정보공개를 주저하게 하였다.

그러나 이러한 신중함이 오히려 의혹을 더 가중시킬 수 있고, 선관위 직원 내부 연루여부에 대한 수사결과도 발표되었으므로 법률에 의해서 공개가 금지되거나 제한되는 자료 외에는 가능한 한 우리 위원회가 관리하는 자료를 공개할 것이다.

여섯째, 관련 증거를 은폐하기 위하여 중앙선관위 홈페이지 로그기록 등을 조작하였다는 주장에 대하여

2011. 10. 26. DDoS 공격 이후 당일 10시 10분 경찰청에 수사의뢰를 하면서 로그기록을 포함한 모든 자료를 제공하였고, 2011. 12. 9. 경찰에서 검찰청으로 사건이 송치되면서 검찰 측의 요구에 따라 경찰청에 제공한 자료보다 더 광범위한 자료 일체를 검찰청에 다시 제공한 바 있다.

경찰과 검찰에 제공한 로그파일 및 관련 기록자료는 80여건 이상이며, 이렇게 광범위한 자료에 대해 무결점을 유지하면서 일관성 있게 조작하는 것은 물리적으로나 현실적으로나 불가능한 일이다.

로그자료의 조작 여부는 우리 위원회와 경찰·검찰에서 각각 보유하고 있는 로그 자료를 상호 비교하면 증명할 수 있으며, 검찰은 사건 송치시 경

찰로부터 일체의 관련 자료를 넘겨받았기 때문에 각 자료간 조작의 흔적이 있었다면 수사과정에서 이미 드러났을 것으로 판단된다.

이번 10. 26. DDoS 공격에서 로그기록의 조작은 선관위 내부자 연루 및 은폐를 전제로 한 것이며, 이러한 내부직원 연루의혹은 이미 여러 경로를 통해 사실이 아님이 밝혀진 만큼 내부직원들이 로그기록을 조작할 어떠한 이유도 없음을 확신한다.

일곱째, 시스템 개편을 통해 증거를 인멸하고, 더 나아가 개발서버까지 교체하려 한다는 주장에 대하여

시스템 개편 작업을 추진하더라도 DDoS 사건과 관련된 서버 및 통신, 보안장비 등 관련 로그파일 등을 폐기하는 것이 아니라, DDoS 사건 당시 로그파일은 선관위에서 별도의 장소에 안전하게 보관하고 있다. 시스템의 교체 대상 장비도 내부 데이터의 현재 상태를 복제하여 별도의 안전한 장소에 보관하고, 하드웨어 또한 일정기간 보관하는 등 모든 증거를 원본 그대로 보존하고 있음을 명백하게 밝혀둔다.

우리 위원회로서는 목전에 다가온 제19대 국회의원선거를 안정적으로 관리하는 한편, 정보시스템의 개선 및 고도화를 추진하여야 하는 바, 이 과정에서 노후화된 장비의 경우에는 시스템의 안정성을 확보하기 위하여 교체하는 경우가 일반적이며, 시스템 교체 및 신규 도입은 내구연한이 지난 노후화된 장비의 교체, 보안 시스템의 업그레이드 및 신규 도입, 망분리 및 통신망 재구성 등 선관위 정보시스템 전체를 대상으로 하고 있다. 이는 그 시급성에 따라 제19대 국회의원선거 전과 제18대 대통령선거 전으로 구분하여 실시하고 있다.

또한, 정보자원의 효율성 확보를 위해 업무별 서버확장 수요를 고려하여 서버 추가 등을 추진할 것이다. 교체대상 장비의 선정까지, 개발서버인지, 다른 서버인지 까지를 가지고 의혹을 제기하는 것은 억지 주장에 지나지 않는다.

제19대 국회의원선거가 48일 남은 시점에서 아무런 일도 하지 않은 채 또 다시 DDoS 공격 등을 당하여 국민에게 피해가 가도록 해야 옳은지, 아

니면 모든 관련 자료 등은 별도 안전한 장소에 보관한 후 관련 장비·시스템을 개선·보완하여 차후에는 완벽한 선거관리가 이루어지도록 해야 하는지에 대한 현명한 판단을 기대한다.

여덟째, 선관위가 2011. 10. 26. 서울시장보궐선거에서 투표율을 낮추기 위한 목적으로 투표소를 변경하였다는 주장에 대하여

서울시의 경우 동(洞)마다 적게는 1개부터 많게는 13개까지의 투표소를 설치하였고, 투표장소는 그 지역의 여러 가지 상황 즉, 행정구역 변경 유무, 재개발 등 지역개발사업 여부, 공공시설 활용 가능 여부, 건물주의 사정이나 승낙 여부 등에 따라 종전에 사용하였던 투표소를 그대로 사용[15]하기도 하고, 사용할 수 없는 때에는 부득이 새로운 장소를 확보하여 권한이 있는 동(洞)선관위에서 일정한 과정과 절차를 거쳐 투표소를 변경하여 설치한다[16].

투표소의 설치는 동선관위에서 중앙선관위가 사전에 시달한 '읍·면·동위원회 사무편람' 등 일정한 기준에 따라 그 장소를 선정한 후 당해 동선관위의 의결로 결정하고 그 결과를 구선관위에 보고하는 절차를 거치도록 되어 있는 점, 투표소 설치 및 설비 등의 업무를 수행하는 동선관위의 선거사무담당자는 구청장의 지휘를 받는 지방자치단체 소속 지방공무원(동주민센터 직원)으로서 불합리하게 투표소 변경을 지휘할 수 있는 시스템이 아니라는 점과 서울시 관내 대부분의 구청장이 민주당 소속이라는 점[17], 더군다나 6인으로 구성되는 동선관위 위원 중에는 국회에 교섭단체를 구성한 정당[18]에서 추천한 인사가 참여하고 있는 점 등 제반절차와 과정을 고려할 때 투표율을 고의로 떨어뜨리기 위하여 의도적으로 서울시 전역에서 투표소를 변경하는 일이 불가능하다는 것은 건전한 상식을 가진 일반인이라면 쉽게 판단할 수 있는 일이다.

---

15) 재·보궐선거는 임기만료에 의한 선거와 달리 공휴일이 아닌 평일에 실시되어 학교수업이나 공공기관·단체 등의 정상 근무·영업 등으로 장소사용에 협조가 어려우나, 서울시선관위는 투표소 변경에 따른 혼란 방지와 선거인의 투표편의를 위하여 주민투표 당시의 투표소를 우선적으로 선정하도록 구위원회에 지시한 바 있음.(2011. 9. 20 교육)

16) 10. 26. 서울시장 보궐선거시의 투표소 변경비율[13.8%(305개)]은 서울시 주민투표시의 투표소 변경비율[19.3%(426개)] 보다 5.5% 감소하였으며 또한, 제5회 지방선거 이후 실시한 전국 재·보궐선거의 투표소 변경비율(18.9%)보다 5.1% 감소한 수치임.

17) 10. 26. 서울시장보궐선거 당시 민주당 소속 구청장은 19명, 한나라당 소속 구청장은 5명이었음.

18) 10. 26. 서울시장보궐선거시에는 한나라당과 민주당이었음.

< 표 3-1 > 투표소 선정기준 및 설치절차

▣ 투표소 선정기준

○ 공직선거법 제147조(투표소의 설치)

투표소는 읍·면·동선관위가 투표구마다 설치하고(법 §147①), 투표소는 학교, 읍·면·동사무소 등 관공서, 공공기관·단체의 사무소 등 선거인이 투표하기 편리한 곳에 설치하며(법 §147②), 병영 및 종교시설 안에는 투표소를 설치할 수 없으나 단 종교시설은 투표소를 설치할 적합한 장소가 없는 부득이한 경우 설치가 허용됨(법 §147④).

○ 공직선거 절차사무편람

투표구안의 생활 중심지로 선거인이 잘 알고 있고 교통이 편리한 곳 , 투표하기 편리하고 투표관리를 원활히 할 수 있는 적정면적 규모의 장소, 장애인 등의 투표편의 시설이 있는 장소

≪투표소 확보과정 및 절차≫

① 관계시설 조사 ⇨ ② 투표소 변경이 필요한 투표구가 있는지 파악 ⇨ ③ 변경하고자 하는 투표소를 중심으로 시설현장 점검 ⇨ ④ 소재지, 면적, 층수, 장애인편의시설, 승강기 유무 등 적정여부 검토 ⇨ ⑤ 시설관리자의 승낙서 징구 ⇨ ⑥ 투표소 결정 및 공고

▣ 투표소 설치절차

투표소설치 예정장소 조사(읍·면·동선관위, 선거기간개시일전 30일까지) ⇨ 투표소예정장소 구·시·군선관위 보고 ⇨ 투표소설치장소 결정(읍·면·동선관위 의결) ⇨ 투표소 명칭과 소재지 공고(읍·면·동선관위, 선거일전 10일까지) 및 구·시·군선관위에 결과 보고 ⇨ 매세대에 투표장소 및 약도를 게재한 투표안내문 발송(읍·면·동선관위, 선거일전 5일까지)

또한, 젊은 층의 투표율이 낮으면 특정후보에게 유리할 것이라고 판단하여 투표소를 변경하였다고 주장하지만, 특정 계층(젊은 층)만을 상대로 투표소 위치를 알려 주는 것은 불가능하며, 일반적으로 투표소를 찾는 데는 노년층보다는 젊은 층이 더 유리할 것임은 상식에 속하는 일이라 판단된다.

다만, 동주민센터 지방공무원인 동선관위 간사가 투표소 변경사유 등을 보고 및 집계하는 과정에서 일부 행정착오[19]가 있었던 것은 사실이나, 선관위가

19) 선거일에 변경전 학교에서 수업이 없었는데도 불구하고 수업이 있다는 사유로 투표소가 변경되었다며 의혹을 제기한 것과 관련, 통상적으로 투표소 예정장소는 ·지방자치단체의 동주민센터 직원이면서 동선관위 간사·서기가 선

어떤 정치적인 의도를 갖고 투표소를 변경한 것은 아니다. 이에 대하여 서울시 선관위에서는 일부 행정착오가 있었음을 인정한 후 유감을 표명했으며, 추후에는 이와 같은 일이 반복되는 일이 없도록 업무 감독 및 교육을 철저히 할 것이라 밝힌 바 있다. 이번 사건을 계기로 2012. 2. 15. 투표소 선정과정의 투명성과 유권자의 편의를 위하여 주민의견 수렴과정을 거치도록 하였다.

아홉째, 10. 26. 서울시장보궐선거 당시 야권 지지율이 높았던 지역의 투표소 변경비율이 높아 그 지역의 투표율이 낮아졌다는 주장에 대하여

여·야당의 지지율이 높은 지역을 객관적·과학적으로 특정하기는 쉽지 않으나, 대체적으로 강북지역은 야당의 지지율이, 강남지역은 여당의 지지율이 높은 것으로 나타나고 있다.

10. 26. 서울시장 보궐선거에서 투표소 평균 변경비율은 13.8% 였으며, 평균 변경비율 보다 높은 상위 5개구와 낮은 5개구의 변경비율과 투표율을 살펴보면 아래의 표와 같다.

< 표 3-2 > 투표소 변경비율과 투표율

구 분	구 분	총 투표소수	8. 24. 주민투표 대비		투표율(%)
			변경투표소수	변경 비율	10. 26. 보궐선거
서울시 전체	**서울시전체**	2,206	305	**13.8%**	**48.6**
상위 5개구	서대문구	72	23	31.9%	49.0
	금 천 구	57	13	22.8%	44.3
	동대문구	86	18	20.9%	47.6
	구 로 구	91	18	19.8%	48.5
	성 북 구	98	19	19.4%	48.5
하위 5개구	중 구	45	2	4.4%	49.9
	종 로 구	42	2	4.8%	49.5
	노 원 구	119	6	5.0%	50.3
	마 포 구	93	5	5.4%	49.9
	용 산 구	59	6	10.2%	47.4

거기간개시일전 30일 경에 각급 학교 등을 방문·전화하여 투표소 사용여부를 문의하면 대부분의 학교에서는 평일이라는 사실에 입각해서 “투표일에 수업이 있다“고 답변하였고, 일부는 보고서 작성과정에서 복사하여 붙이기 작업중에 실수로 잘못 워딩한 사례가 있었음.

<표 3-2>에 의하면 투표소 변경비율이 가장 높은 서대문구의 투표율(49.%)과 가장 낮은 중구의 투표율(49.9%)은 모두 평균 투표율(48.6%)을 상회하였으며, 투표율이 다소 낮은 금천구를 제외한 나머지 지역의 투표율은 평균 투표율과 비슷한 것으로 나타났으므로 2011. 10. 26. 서울시장보궐선거에서는 투표소 변경과 투표율간에 상관관계가 있다고 주장할 수는 없다.

투표소 변경을 최소화하여 유권자가 투표소를 찾는데 도움을 주어야 한다는 것은 부인할 수 없으나, 유권자의 투표편의 제공 등 투표소를 변경하여야 할 사유가 있는 경우에는 관련 법규에 의하여 사전에 정해진 과정과 절차를 거쳐 투표소를 변경할 수 있으며, 투표소의 변경이 있다고 하여 반드시 투표율이 반드시 낮아진다는 어떠한 논리적 근거는 찾아 볼 수 없다.

투표소 변경이 있더라도 법규에서 정하고 있는 안내사항 외에도 2011. 10. 26. 서울시장보궐선거에서처럼 '안내현수막' 설치, '안내벽보' 게시, '안내도우미' 배치, 구청 등 유관기관·단체의 홈페이지에 변경안내문 게시를 통하여 유권자에게 안내를 해 나갈 것이기 때문이다.

< 표 3-3 > 오전 7시, 9시 현재의 투표율 현황

구 분	07시 현재			09시 현재		
	10.26 서울시장보궐선거 (A)	제5회 지방선거 (B)	증감율 (A-B)	10.26 서울시장보궐선거 (C)	제5회 지방선거 (D)	증감율 (C-D)
백분위 환산 투표율[20]	**4.4%**	**4.5%**	**-0.1%**	**22.4%**	**16.7%**	**5.7%**
실제투표율	**2.1%**	**2.4%**	**-0.3%**	**10.9%**	**9.0%**	**1.9%**

투표소 찾기를 어렵게 하기 위해 광범위한 지역에 걸쳐 투표소를 의도적으로 변경한다는 것은 투표소 설치절차, 투표안내문의 매세대 발송, 선거일전 10일까지 투표소의 명칭과 소재지 공고 등 투표소 위치에 대한 사전안내과정 등을 살펴볼 때 있을 수 없는 일이다.

다만, 우리 위원회는 향후 투표소 변경에 더욱 신중을 기하고 부득이 변경하는 경우에는 다양한 방법으로 변경된 투표소를 안내·홍보하여 유권자가 투표권을 행사하는데 지장이 없도록 할 것이다.

20) 총투표자수를 100으로 변환하여 시간대별 투표자수의 비율을 환산하는 방식으로 투표율을 계산함.

열번째, 2011. 10. 26. 실시된 서울시장보궐선거에서 선관위 '투표소 찾기 서비스' 이용시 이전까지 요구하지 않았던 선거인의 주민등록번호를 입력하는 절차를 추가하였다는 주장에 대하여

선관위는 그 동안 법령에 따라 매세대에 발송하는 투표안내문을 통해 투표소를 안내해 오던 방법 외에도 정보통신기술의 진보를 수용하여 유권자에게 적극적인 투표소안내 서비스를 제공하기 위하여 2007년 제17대 대통령선거부터 중앙선관위 홈페이지를 통하여 주소 선택방식으로 '투표소 찾기 서비스'를 개시하였다.

그러나 투표구는 통·리·반을 기준으로 설치되므로, 하나의 읍·면·동안에 여러 개의 투표소가 설치된 경우 유권자가 자신의 주소를 정확히 알고 있더라도 통·리·반을 정확하게 알지 못하면 투표소 찾기에 어렵다는 의견이 많았다.

이에 따라 2010년 제5회 전국동시지방선거시부터 본인의 읍·면·동이나 통·리·반을 모르는 선거인은 자신의 성명과 주민등록번호로도 조회할 수 있도록 투표소 찾기 방식을 추가하였고, 이후 2010년 하반기 재·보궐선거, 2011년 상·하반기 재·보궐선거 및 2011년 실시한 서울특별시 주민투표에서도 동일한 방식으로 서비스를 제공하여 왔다.

따라서 주민등록번호 입력방식에 의한 '투표소 찾기 서비스'는 2010년 이후 지속적으로 제공해 온 방식으로서 2011. 10. 26. 서울시장보궐선거에서 처음 도입한 서비스가 아니라는 점은 사실관계가 명확하다.

이번 사건을 계기로 우리 위원회는 금년 제19대 국회의원선거 및 제18대 대통령선거에서는 주소 입력방식 외에 주민등록번호의 입력 없이도 투표소 조회가 가능하도록 하는 방안을 강구하여 시행할 것이다.

열한번째, 10. 26. 서울시장보궐선거에서 박원순 후보자가 당선되었으나, 진보성향의 20대가 많은 부재자투표에서 나경원 후보자가 25개 구(區)에서 모두 승리한 것은 고의적인 부재자투표 개입이 없다면 납득할 수 없는 일이라는 주장에 대하여

불특정 다수인이 참여하는 재·보궐선거에서의 부재자투표[21]의 특성상 특정 후보자를 지지하도록 하기 위하여 중앙선관위 등 특정인이나 기관이 조직적이고 광범위하게 개입하는 행위는 그 단서나 정황이 쉽게 드러날 수 밖에 없다. 예컨대, 거소투표의 방법으로 투표하는 재·보궐선거에서 군인이 부재자투표를 하는 경우 많은 군인들에게 투표부정을 하였다면 왜 신고가 없었겠는가 반문하고 싶다.

동선관위 간사·서기를 포함한 공무원인 선관위 직원들이 그러한 불법 행위를 범하여 사실이 드러날 경우 파면 등 징계는 물론 경우에 따라서는 형사처벌되는 등 경제적 손실과 명예를 실추 당하는 일은 하지 않을 것이라고 판단된다.

부재자투표의 부정이 조직적으로 행하여지려면 부재자신고자 수가 이례적으로 증가하거나 위장전입 또는 허위신고가 있거나, 부재자 투표과정에서 투표간섭 또는 투표방해 등 부재자투표와 관련하여 불법·부정으로 의심할 만한 사례의 정황이나 신고가 있어야 하는데 현재까지 이 같은 사례는 전혀 없다. 일부에서의 주장과 같이 조직적인 부재자투표의 부정이 있었다면 어떻게 구체적인 정황·증거나 진술이 나오지 않을 수 있겠는가? 예컨대, 대리부재자신고로 대리신고자가 부재자투표용지 받아 투표를 하였다면 선거인명부에 부재자로 표시되어 그 선거인은 일반투표소에서 투표할 수 없는 바, 일반투표소에서 이중투표로 인하여 투표를 하지 못했다는 신고가 한 건도 없을리 있겠는가 반문하지 않을 수 없다. 또한, 조직적으로 투표부정이 있으려면 선관위에서 특정인에게 기표한 투표지를 무더기로 만들어 부재자투표함에 넣어야 하는 바, 모든 과정에 구선관위 정당추천위원이 참여하고 있을뿐만 아니라 각 구선관위의 모든 직원들의 눈을 속이고 부정이 있을 수 있겠는가? 최근 특정 정치사안에 대한 기사글을 직원이 내부통신인 '그룹웨어'에 게시한 사례가 있었는데 그 결과 찬·반의 의견이 반반인 상황이었는 바, 어떻게 상관의 불법·부당한 지시가 먹혀들겠는가 반문하고 싶다.

---

21) 선거별 부재자신고인수는 2011. 10. 26. 서울시장보궐선거에서는 133,597명, 2010. 6. 2. 제5회 전국동시지방선거에서는 154721명, 제17대 대통령선거에서는 148,056명으로서 특별히 부재자신고자수가 증가되지 않았음.

< 표 3-4 > 부재자 신고절차 등

부재자신고(선거인명부작성기준일부터 5일까지) ⇨ 부재자신고인 접수 및 심사처리(구·시·군의 장, 정당한 신고권자인지 여부 등 심사) ⇨ 부재자신고인명부 작성·확정(구·시·군의 장) ⇨ 구·시·군의 장으로부터 부재자신고인명부 통보서 접수(구·시·군선관위) ⇨ 부재자신고인명부와 부재자신고서의 대조·확인(구·시·군선관위, 부재자투표용지발송 전까지) ⇨ 부재자투표용지 우편발송(구·시·군선관위, 정당추천위원 참여) ⇨ 거소투표자의 예에 의하여 투표 후 구·시·군선관위에 발송 ⇨ 부재자투표용지 접수확인·투표함 투입(구·시·군선관위, 정당추천위원 참여, 선거일 20시까지) ⇨ 부재자투표함 개표소 이송·개표(구·시·군선관위, 정당추천위원 등 참여, 일반투표와 별도) ⇨ 부재자투표지 유·무효 판정(구·시·군선관위, 정당추천위원 등 참여)

10. 26. 서울시장보궐선거에서 박원순 후보자가 전체 득표율에서 53.4%를 득표하여 46.2%를 득표한 나경원 후보자와 7.2% 차이로 당선된 것이 사실인 것처럼, 부재자투표에서 나경원 후보자가 박원순 당선자보다 11.7%를 앞선 것 또한 사실[22]이고, 이러한 투표결과는 있는 그대로 유권자의 뜻으로 받아들여야지 구체적인 근거없이 막연한 추측과 의심만으로 부재자투표의 부정의혹을 제기하는 것은 시민단체·언론의 입장에서나 국민 개인의 입장에서나 모두 바람직스럽지 못하다.

국회의원 이○○이 국회에서 기자회견을 통하여 2011. 10. 26. 서울시장보궐선거에서 부재자투표에 대한 부정의혹을 제기한 것과 관련하여 2012. 1. 9. 서울시선관위에서는 해당 국회의원에게 부재자투표 부정을 입증할 수 있는 자료를 제출해 줄 것을 서면으로 요청하였으나, 현재까지 이와 관련한 어떠한 자료의 제출도 없었음은 무엇을 의미하겠는가?

부재자투표의 득표율과 전체 득표율 간에는 선거에 따라 차이를 보일 수 있다는 것이 경험칙에 부합되고, 그 차이는 유권자의 표심에 달려있다는 것은 상식의 영역에 속하는 사항이다. 우리 위원회는 과거에도 그랬듯이 앞으로도 투표부정에 대한 구체적인 증거가 제시되거나 불법의 신고가 있는 경우에는 이를 철저하게 조사하여 관련 법률에 따라 엄정하게 처리할 것임을 누차 밝힌 바 있다.

---

22) 2006년 실시한 서울시장선거에서 오세훈 후보는 전체 득표율에서 61.1%를 득표하였으나 부재자투표는 48.4%의 득표에 그쳤고, 강금실 후보의 경우 전체 득표율에서는 27.3%를 득표하였으나 부재자투표는 40.8%를 득표한 사실이 있었음.

2. DDoS 공격과 관련한 평가

헌법 제1조는 “대한민국의 주권은 국민에게 있고, 모든 권력은 국민으로부터 나온다”고 규정하여 주권재민의 원리를 선언하고 있고, 주권재민의 원리를 대의민주주의 방식으로 구현하는 우리 헌법의 통치구조상 자유롭고 공정한 선거는 민주적 기본질서의 핵심이다. 투표참여를 방해하기 위하여 선관위 홈페이지에 대한 DDoS 공격을 자행한 것은 민주적 기본질서에 대한 중대한 도전이며 헌법 파괴행위로서 그 범행의 배후와 전말에 대하여 반드시 실체적 진실이 명확하게 밝혀져 사법적 정의가 실현되어야 한다.

중앙선관위 홈페이지 DDoS 공격과 관련하여 공격 당일인 2011. 10. 26. 투표 개시 전에 중앙선관위가 자체적으로 인지하여 통신망을 전환하고 관계기관과의 협조 등을 통해 나름대로 최선의 대처를 하였다. 다만, 사상 초유의 사태에 직면하여 초동조치 및 사이버대피소 우회 조치 등과 관련하여 통신사업자 등 관계기관과의 협의 및 결정과정에서 절차상 불가피한 시간이 소요되었음은 아쉬움으로 남는 대목이다.

우리 헌법에서 선거관리와 정당에 관한 사무처리 등 고도의 정치적 중립성과 공정성이 요구되는 정치발전적 집행업무는 독립된 선관위에 부여하고 있는 헌법규정을 감안하여 선거에서 심판기능을 수행하는 선관위에 대한 신뢰는 보호되어야 한다. 국민 모두가 선거결과에 승복하여야 민주정치 발전과 국민통합에 성공할 수 있으므로 선관위의 공정성이나 신뢰성을 훼손하는 행위는 DDoS 공격 못지않게 선거관리에 장애를 초래할 수 있어 민주적 기본질서를 위협하는 요소가 될 수 있다.

일부에서 서버 로그기록이 국정원에 있다느니, 서버연동을 차단하였다느니 내부연루자가 있다는 등 괴담수준을 넘어 터무니없는 의혹 제기로 선관위의 신뢰와 직원들의 명예를 훼손하고 있음은 심히 유감스러운 일이 아닐 수 없다. 사건 당일 경찰에 수사를 의뢰하면서 모든 로그기록을 경찰에 제출함은 물론, 검찰에도 이를 제출하여 수사기관에서 수사한 결과 서버연동 차단이나 내부자연루설 등은 전혀 근거가 없음이 확인되었고, 2011. 12. 8. 학계 및 업계의 정보보호 전문가 7인을 초빙하여 「통신비밀보호법」에 위반되지 않는 방법으로 로그기록과 트래픽을 공개하였고, 서버가 정상적으로

작동하였음을 확인하였음에도 일부의 터무니없는 주장에 편승하여 이를 확대, 재생산한 사람들은 DDoS 공격에 사용된 좀비PC의 역할과 무엇이 다른지, 또 선관위를 흔들어 과연 무엇을 얻으려 하는지 이제는 답해야 할 때가 아닌가 사료된다.

굳이 경찰과 검찰의 수사결과를 인용하지 아니하더라도 이두아 국회의원이 발의한 특검법의 수사대상에 "중앙선거관리위원회의 공모 또는 고의적 장애 방치 가능성, 사건의 은폐 조작 가능성, 중앙선거관리위원회의 전산 시스템 구성의 문제점 및 로그 파일 비공개 의혹"이 포함되어 있었으나, 여·야 의원으로 구성된 법사위 논의과정에서 이 부분이 전부 빠졌음을 음미해 볼 필요가 있다.

합리적 근거에 터잡은 의혹의 제기는 표현의 자유로서 마땅히 최대한 보장되어야 하나, 합리적 근거가 전혀 없는 의혹의 제기는 기본권의 남용으로서 보호받을 수 없는 영역임을 명백히 밝혀두고자 한다.

한편, 우리 위원회는 DDoS 공격의 피해자이기도 하지만 그 공격을 효과적으로 막지 못하여 국민에게 불편을 끼쳐드린 송구스러운 입장이라는 점, 내부 연루 의혹제기로 우리 자신도 자유로울 수 없었다는 점, 로그기록을 공개할 경우 기록의 위·변조 시비로 새로운 논란이 촉발될 수 있다는 점 때문에 우리는 자부심과 긍지에 큰 상처를 입고도 적극적인 대응을 자제하며 인내해 왔다.

2012. 2. 9. 국회에서 「2011. 10. 26 재보궐선거일 중앙선거관리위원회와 박원순 서울시장 후보 홈페이지에 대한 사이버테러 진상규명을 위한 특별검사의 임명 등에 관한 법률안」이 통과되었으므로 특별검사의 수사가 진행될 것이고 수사가 종결된다면 헌법기관인 중앙선관위에 대한 DDoS 공격을 한 관련자는 물론이고 전혀 합리적 근거 없이 의혹을 제기한 사람들도 응당 자신의 행위에 대하여 책임을 져야 할 것이다.

또한, 우리 위원회는 직원의 명예회복이라는 개인적 측면보다 헌법기관의 신뢰회복을 통하여 성공적 선거관리를 담보하고, 선거결과에 정당성과 정통성을 부여하여 민주정치의 발전을 도모할 것이다.

국민 여러분께서는 이제는 선관위에서 금년 양대선거를 차질 없이 준비하고 관리할 수 있도록 격려와 응원이 필요한 시점이며, 아울러 선관위가 중립적이고 공정하게 선거를 관리하는지 항상 지켜보는 자세도 필요하다.

3. 의혹제기가 선관위 또는 국민에게 미치는 영향

1) 사건의 본질이 아닌 내부직원의 연루 의혹제기로 선관위에 대한 불신 초래

2009. 7. 7. DDoS 공격, 2011. 3. 4. DDoS 공격으로 국민의 재산과 개인정보・산업기밀 유출 등이 발생하였음에도 수사기관의 수사결과를 받아들여 추후 이와 관련한 의혹을 제기하지 않았으나, 이번 사건에서는 지속적인 의혹제기로 수사기관의 수사결과에도 불구하고 특검으로까지 이어졌고, 일부에서는 사건의 본질과는 다른 선관위 내부 직원의 연루 의혹제기로 직원 개인 뿐만 아니라 선관위의 공정성이나 신뢰성에 대한 불신을 확산시키고 있다. 근거 없는 의혹제기는 선관위 직원들의 사기를 떠나 국가적으로 국력을 낭비하는 행위가 아닌가 한다.

2) 선관위 직원에 대한 비방 또는 명예훼손

검찰 수사과정에서 중앙선관위 시스템운영 및 정보보호 담당 직원 4명이 각각 7~10시간에 이르는 강도 높은 조사를 받았으나, 연루의혹이 사실이 아닌 것으로 확인되었음에도 지속적으로 내부 직원의 연루의혹을 제기하는 것은 경우에 따라서는 비방 또는 명예훼손으로 볼 수 있다.

수사 또는 연루의혹에 대한 대응뿐만 아니라 본연의 선거관리업무인 전산개발, 보안정보관리 처리에 야근을 밥 먹듯이 하는 선관위 직원들의 사기를 북돋아 완벽한 선거관리가 이루어지도록 하는 것도 필요하다.

3) 전자투표제도의 미래 불투명 및 국가신인도 저하

중앙선관위 홈페이지 DDoS 공격으로 우리 위원회는 많은 것을 잃었다. 그 중에서도 뼈아픈 것은 외부 불순세력으로부터 홈페이지를 지켜내지 못했다는 아쉬움 외에도 전국 어디서나 투표할 수 있는 전자투표제도 실현의 꿈, 후발 민주주의 국가에 수출하고 있는 우리나라의 선진 선거관리시스템과 선거관리기관의 신뢰수준에 대한 불신으로 국가신인도가 저하될 수 있음도 기억해야 할 대목이다.

4) 선거관리 불신은 선거로 선출된 대표자에 대한 정당성과 정통성 약화

이번 사건의 경우 중앙선관위가 DDoS 공격으로 인하여 피해자임에도 불구하고 합리적인 근거 없이 마치 부정을 저지르거나 내부 직원이 공모하였다는 의혹을 제기함으로써 올해 실시되는 양대선거를 앞두고 중앙선관위가 사건의 공범이거나 내부 직원이 연루되었다는 인식을 국민에게 심어 주어 국가기관인 선관위와 선거과정에 대한 불신을 초래하는 등 부정적인 영향을 미치고 있다.

이는 결국 선거결과의 부정으로 연결되어 선거에서 선출된 대표자의 정당성과 정통성을 약화시킴으로써 결국, 국민에게 피해를 전가시킬 수 있다.

4. 사이버 공격에 대비한 보완대책

일부에서 DDoS 공격 관련 증거를 인멸하기 위하여 관련 장비를 교체하려 한다는 주장에도 불구하고, 2011. 12월 국회에서 사이버공격 예방・대응체제 구축 관련 예산이 확보되었는 바, 국회에서의 예산편성 취지에 맞게 우리 위원회는 금년 양대선거를 앞두고 사이버 테러에 대비하여 특단의 사이버 보안대책을 강구하여 시행할 것이다.

DDoS 등 사이버 공격에 대비하여 별도의 사이버대피소를 구축·운영하고, 만일의 상황에 대비해 정보보호전문기관, 통신사업자 등 관계기관과 협조체제를 갖추어 사이버위협행위에 즉시 대응할 수 있도록 하겠다.

DDoS 등 사이버공격 위협행위에 대한 24시간 모니터링을 위해 상시 보안관제 실시와 함께, 내부 PC의 좀비 PC화 방지, 중요정보의 접근 및 유출 경로 차단을 위하여 인터넷과 업무망을 분리하겠다.

「개인정보 보호법」 시행에 따라 개인정보 암호화 및 개인정보유출방지 시스템을 도입하여 개인정보 보호에 만전을 기하고, 투표소 위치정보 등 유권자가 필요로 하는 주요정보는 우리 위원회 홈페이지 뿐만 아니라 주요 포털사이트 등에서도 안내 받을 수 있도록 하는 등 선거정보 접근 채널의 다양화를 통해 쉽게 서비스를 제공받을 수 있도록 하겠다.

아울러, 정보보호 유관기관과 대책회의를 개최하고, 각 관계기관의 상황실 등과 긴급 연락망을 구성하여 유사시 공동으로 대처해 나갈 것이다.

Ⅴ. 맺음말

그 동안 중앙선관위는 과거 3. 15. 부정선거와 같은 선거부정이 다시는 이 땅에 발붙이지 못하도록 헌법에서 부여된 공정관리를 생명처럼 여기면서 「엄정중립 공정관리」를 위해 헌신해 왔다.

2011. 10. 26. 중앙선관위 홈페이지 DDoS 공격 사건은 선거관리기관에 대한 불신과 선거결과에 대한 불신을 싹트게 하였다. 구체적인 증거 없이 심증만으로 또한, 전체적인 내용은 파악하지 아니한 채 극히 일부내용만으로 오해하여 이를 모두 선거부정과 연관시킨다면 과연 누가 좋아하고, 누가 선거결과에 승복할지 묻지 않을 수 없다.

우리나라의 선거제도는 투표·개표 전 과정의 정확성과 공정성 확보를 위해 투표용지 인쇄부터 부재자에게 투표용지 발송 및 접수, 일반투표소로 투표용지 송부와 투표 전 과정, 부재자 투표함과 일반투표함의 개표장으로의 이송, 개함과 개표 전 과정에 정당추천위원, 정당·후보자가 신고한 참관인이 참여하고, 확인·점검하도록 하는 장치들을 두어 투표·개표의 부정을 차단하는 것은 물론 추호의 부정을 의심조차도 할 수 없도록 하는 제도를 갖고 있다.

선거관리의 전 과정이 공개되고 정당과 후보자 측에서 참여하여 선거관리 전반에 관한 모든 것을 확인·참관할 수 있도록 함으로써 외국의 어느 선진 국가보다도 신뢰와 정확성을 확보할 수 있는 선거관리시스템을 갖고 있음에도 이 사건 이후 모든 시스템들이 불신되고, 나아가 피해 당사자인 선관위를 오히려 불신하고 내부직원 연루의혹과 투표소 변경의혹, 부재자투표 부정의혹 등을 일부에서 제기하고 있어 안타까운 마음을 이루 말할 수 없다.

대부분의 선거관리사무가 정보화되어 전산 관리되고 있고, 중앙선관위의 전산실이 선거관리상황실의 중추가 되어 선거관리에 전념하여야 할 시기에, 더욱이 제19대 국회의원선거를 불과 48일을 앞둔 시점에서 담당직원들이 DDoS와 관련된 의혹에 대처하기 위하여 시간을 허비하고 있다.

2012. 4. 11. 제19대 국회의원선거와 12. 19. 제18대 대통령선거를 앞두고 있는 시점에 합리적인 근거 없이 선거관리를 불신하는 것은 선거결과를 부정하게 되고, 선거를 통해서 선출되는 대표자의 정당성과 정통성을 약화시켜 결

국 국민의 부담으로 돌릴 수 밖에 없을 것이다.

이에 우리 위원회는 국민이 공정한 선거관리에 대해 한 치의 의심없이 신뢰하고 안심할 수 있도록 법률에서 금지·제한하고 있지 않는 한 가능한 모든 관련 자료를 공개하고자 한다.

아울러 이미 국회에서 중앙선관위 홈페이지에 대한 DDoS 공격의 진상을 규명하기 위한 특검법안이 통과되어 곧 시행될 것이므로, 근거 없는 의혹제기보다는 그 결과를 지켜보는 자세가 필요하다. 우리위원회는 이번 양대 선거를 앞두고 DDoS 공격이나 해킹으로부터 홈페이지를 지켜내는 것부터 시작하여 한 치의 흠 없는 공정한 선거관리를 위해 각고의 노력을 다할 것이다.

「엄정중립 공정관리」에 대한 감시나 건전한 비판은 언제든지 수용하여 잘못된 점이 있다면 바로 잡아 나갈 것이고 책임져야 할 직원이 있다면 책임질 것이다. 국민 여러분께서도 선거관리위원회와 공정한 선거관리에 대한 근거 없는 비방이나 의혹제기는 국가발전을 위해서 바람직스럽지 않음을 인식하여 자제하여 주시기를 당부드린다.

이번 DDoS 공격으로 우리 위원회는 많은 것을 잃었다. 그 중에서도 뼈아픈 것은 외부 불순세력으로부터 홈페이지를 지켜내지 못했다는 아쉬움 외에도 전국 어디서나 투표할 수 있는 전자투표제도 실현의 꿈, 후발 민주주의 국가에 수출하고 있는 우리나라의 선진 선거관리시스템과 선거관리기관의 신뢰수준에 대한 불신의 싹이 그것이다.

반면에, 디도스 공격과 그에 따른 터무니 없는 의혹제기를 접하면서 우리 위원회가 유권자와 소통의 필요성을 절감하면서 자기성찰의 기회로 삼게 된 점은 하나의 성과이기도 하다.

여지껏 우리 위원회는 법과 원칙을 지키면서 묵묵히 직무를 수행한다면 국민들께서 변함없는 사랑과 신뢰를 보내주실 것이라는 믿음을 갖고 있었다.

그러나 이번 디도스 공격에 따른 의혹제기에 대하여 우리 위원회가 진정성을 갖고 객관적이고 합리적인 근거를 제시하며 적극적으로 언론에 해명하였음에도 불구하고, 의혹이 해소되기는 커녕 팟캐스트, SNS 및 인터넷을 통해서 새로운 의혹이 확대, 재생산되는 현실을 고통스럽게 직시하면서 우리 위원회의 믿음이 얼마나 자기만족적이고 소박한 세계관에 기초하였는지 확인할 수 있었다.

바로 이와 같은 이유로 중앙선관위는 선거관리 집행에서 주권자인 국민의 뜻을 깊이 살펴 유권자가 공감할 수 있는 정책을 수립·집행하겠다는 의지를 밝히기 위하여 2012. 1. 17. 올해 양대선거 관리방향을 “유권자가 중심이 되는 선거”로 공표한 것이다.

<참고자료>

10. 26 서울시장보궐선거 구별 투표소 변경 현황

구분	총투표소수	주민투표 대비			제5회 지선대비			투표율(%)		
		변경 투표소수	변경 비율	순위	변경 투표소수	변경 비율	순위	10. 26. 보궐선거	제5회 지선	증감
계	2,206	305	13.8%	-	544	24.7%	-	48.6	53.9	-5.3
종로구	42	2	4.8%	24	10	23.8%	11	49.5	56.0	-6.5
중구	45	2	4.4%	25	9	20.0%	18	49.9	55.7	-5.8
용산구	59	6	10.2%	21	11	18.6%	21	47.4	53.0	-5.6
성동구	65	11	16.9%	8	12	18.5%	23	48.0	54.0	-6.0
광진구	84	13	15.5%	9	27	32.1%	4	47.4	52.7	-5.3
동대문구	86	18	20.9%	3	26	30.2%	6	47.6	54.0	-6.4
중랑구	85	9	10.6%	18	16	18.8%	20	44.4	50.1	-5.7
성북구	98	19	19.4%	5	29	29.6%	7	48.5	53.4	-4.9
강북구	80	11	13.8%	12	18	22.5%	16	45.2	51.4	-6.2
도봉구	79	10	12.7%	13	18	22.8%	14	48.5	54.6	-6.1
노원구	119	6	5.0%	23	21	17.6%	24	50.3	56.1	-5.8
은평구	97	15	15.5%	10	27	27.8%	9	46.2	51.3	-5.1
서대문구	72	23	31.9%	1	33	45.8%	1	49.0	55.0	-6.0
마포구	93	5	5.4%	22	11	11.8%	25	49.9	55.1	-5.2
양천구	106	12	11.3%	17	24	22.6%	15	50.4	56.2	-5.8
강서구	118	14	11.9%	15	22	18.6%	21	47.4	53.3	-5.9
구로구	91	18	19.8%	4	28	30.8%	5	48.5	55.4	-6.9
금천구	57	13	22.8%	2	22	38.6%	2	44.3	52.6	-8.3
영등포구	97	10	10.3%	20	19	19.6%	19	48.7	54.8	-6.1
동작구	86	15	17.4%	7	25	29.1%	8	50.8	56.6	-5.8
관악구	102	12	11.8%	16	24	23.5%	12	47.9	53.9	-6.0
서초구	98	18	18.4%	6	32	32.7%	3	53.1	54.4	-1.3
강남구	116	17	14.7%	11	24	20.7%	17	49.7	51.2	-1.5
송파구	135	14	10.4%	19	31	23.0%	13	50.3	54.2	-3.9
강동구	96	12	12.5%	14	25	26.0%	10	48.2	54.1	-5.9

발제 2

중앙선관위 공개 자료의 1차 분석 결과와 남은 과제

김기창 / 고려대 법학전문대학원 교수, 변호사, Openweb대표

1. 1차 분석 결과의 요지

○ 10/26일 재보궐선거 당일 06:00-07:00분 사이 낮은 수준의 디도스 공격(평균 초당 221메가비트, 초당 4만4천 패킷 수준)이 있었음

○ 그러나 디도스 방어장비가 공격을 탐지하여 좀비PC들에 의한 접속 요청을 차단하였음. 그 외 정상적 유저로부터 오는 접속 요청에 대한 차단은 없었음. 때문에 당일 선관위 서비스 장애 현상의 원인 규명을 위해서는 디도스 이외의 다른 부분에서 원인을 찾는 것이 합당할 것임.

○ 한편, 중앙선관위의 당일 디도스 현장 대응은 문제가 있었던 것으로 분석되며 추후 특검에서 보다 정밀하고 치밀한 조사가 있어야 할 것으로 판단됨.

① LG엔시스 보고서에는 메모리 증가 현상으로 인한 장애방지 차원에서 06:52과 06:54에 웹서버 사용자에 의해 재기동(Reboot)되었다고 보고됨. 보고서의 다른 기록에도 0시부터 6:54경까지 메모리 사용이 거의 100%에 이르는 것으로 나타나는데 이는 디도스 공격이 본격화되기 이전 상황임. 왜 밤새 메모리가 과부화였는지 규명해야 할 것임.

② 선관위 KT망 2회선과 LG망 1회선을 사용하고 있었는데(각 155M, 총 용량합계 465M), 정보화담당관실은 당일 아침 6:58에 KT회선을 단절하고 LG U+망만 유지하는 등의 행동을 취했음. 이는 명백한 실수이며, 고의성 여부도 함께 판단되어야 할 것임.

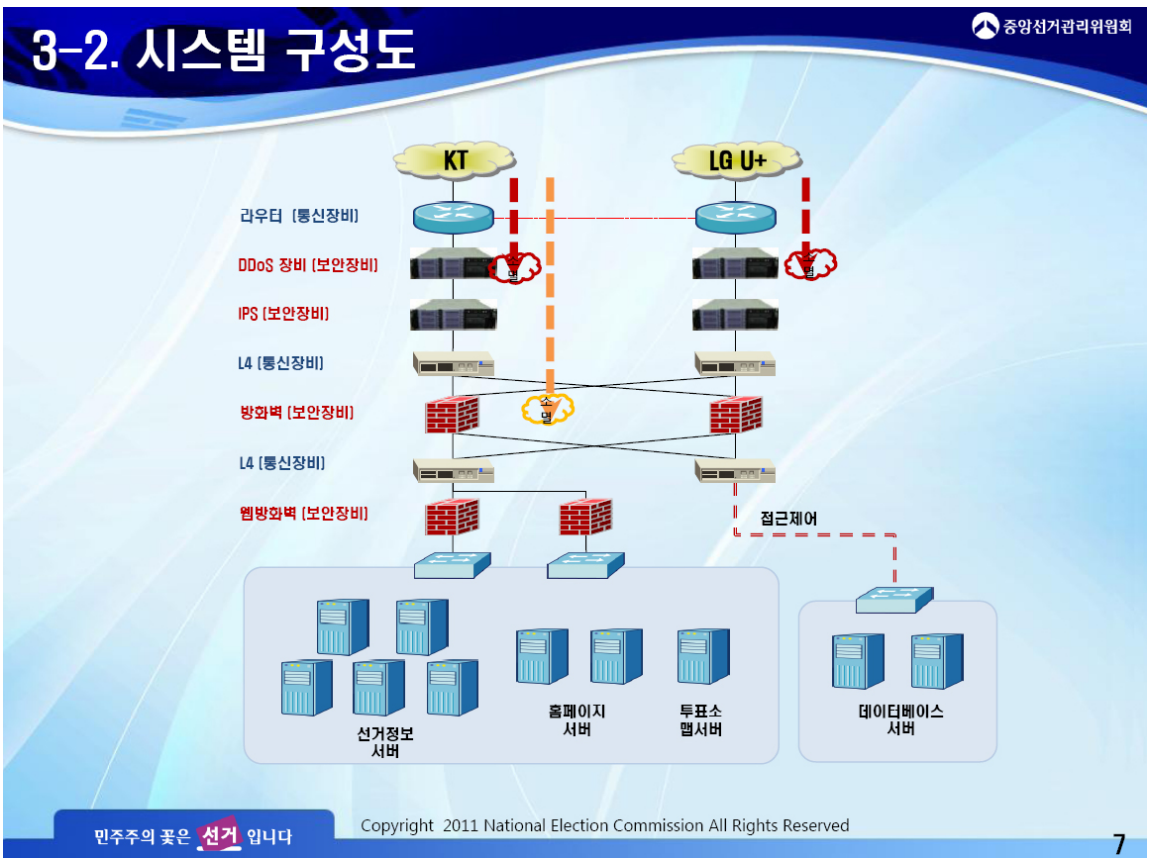
2. 분석 대상

○ 올해 1월27일 중앙선관위는 <10. 26. 재·보궐선거 관련 의혹제기에 대한 10문 10답>(이하 10문10답)공지와 <중앙선거관리위원회 DDoS관련 기술분석 보고서>(이하 디도스 보고서)를 게시함. 10문 10답은 일반인을 상대로, 기술분석보고서는 전문가를 상대로 제시된 기술분석 보고서임.[1)]

○ 두 번째로 참여연대에 중앙선관위가 부분공개한 보고서임. 이는 선관위에 디도스 방어장비를 공급/관리한 보안장비업체인 LG엔시스가 지난해 11월 26일 작성하여 중앙선관위에 제출한 <2011년 10월 26일 재보궐선거 서비스 장애 분석 보고서>(이하 엔시스 보고서)임.

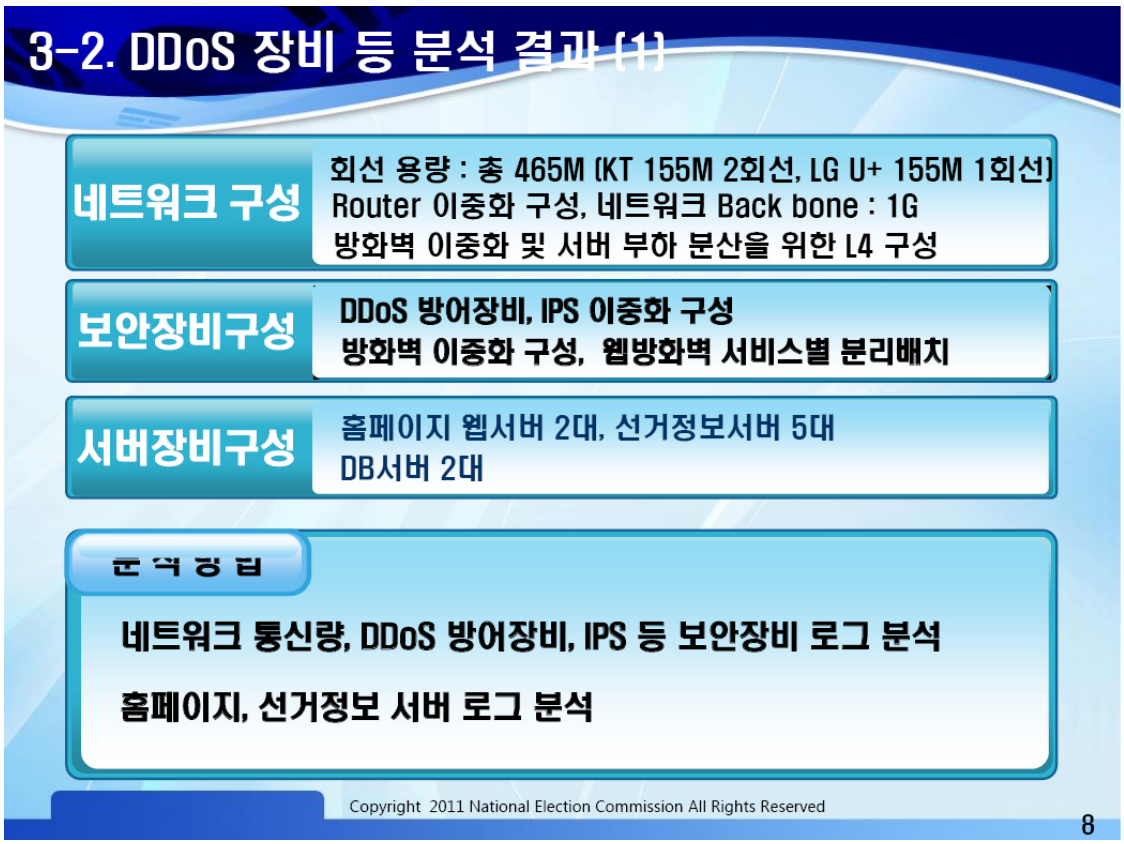
3. 디도스 보고서 분석 결과

1) 선관위의 시스템 구성



1) 이 보고서는 선관위 공지사항에서 다운 가능함.

○ 디도스 보고서의 7p 3-2 시스템 구성도를 보면 서버의 접근경로는 ① 회선 ▸ ② 라우터 ▸ ③ DDos 장비 ▸ ④ IPS(보안장비) ▸ ⑤ L4(통신장비) ▸ ⑥ 방화벽(보안장비) ▸ ⑦ L4(통신장비) ▸ ⑧ 웹방화벽(보안장비) 순의 단계로 이루어짐. 추가로 통신장비 L4(Layer 4의 약자)스위치를 사용하여 네트워크와 서버의 부하조절(load balancing)[2]을 구현하고 있음을 알 수 있음.

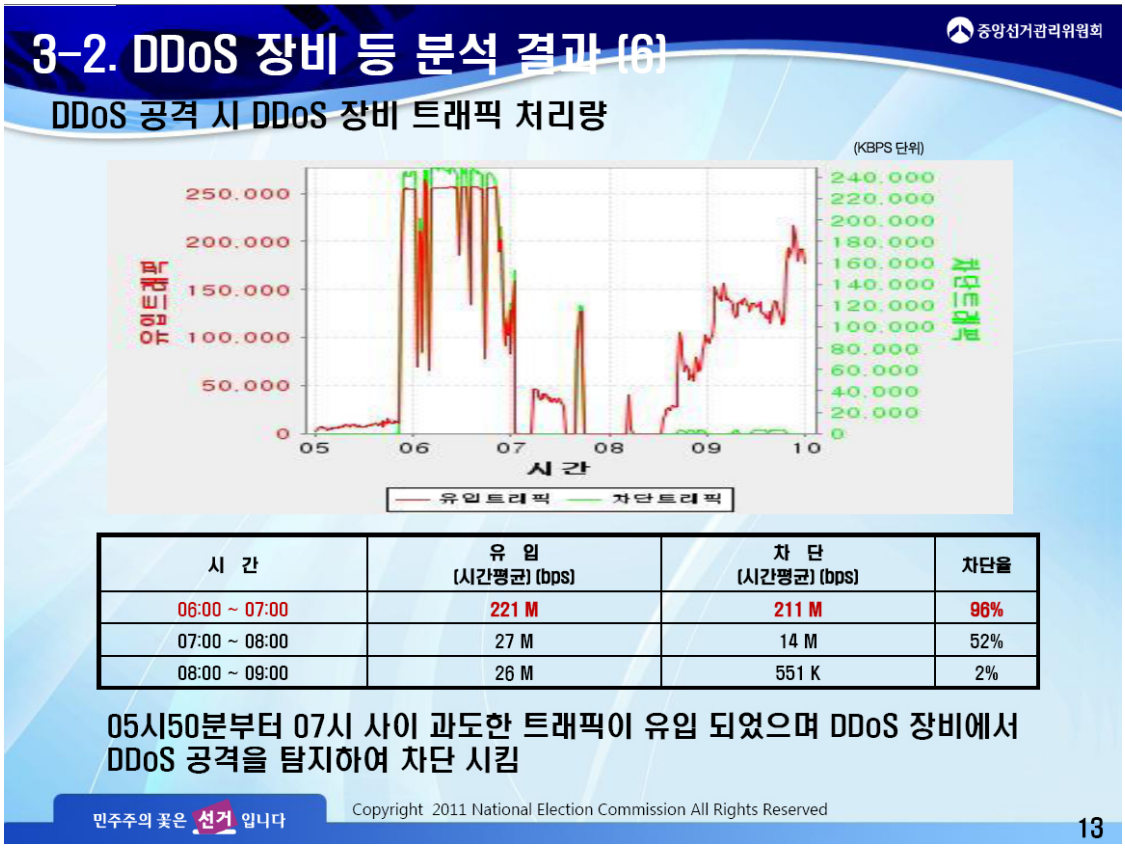


○ 디도스보고서 8p 3-2와 같이 네트워크 구성을 참조하면 중앙선관위 회선 용량은 총 465M임. 이 구성은 KT 155M 2회선과 LG U+ 155M 1회선임. 선관위의 서버는 홈페이지 웹서버 2대, 선거정보서버 5대, DB서버 2대로 구성되어 있음.

2) 10.26 당일 새벽 상황

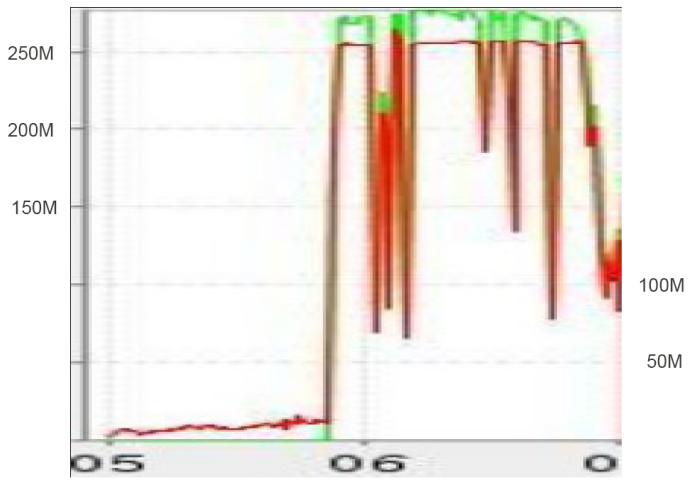
○ 디도스보고서 p13 3-2에는 DDos장비가 처리한 당일 트래픽 처리양에 관련한 표가 그려져 있음. 일견 보기에 유입 트래픽보다 차단 트래픽이 높게 나타날 때도 있어 의아스럽지만, 이는 같은 그래프 안의 유입 트래픽의 단위(붉은 선)와 차단 트래픽(초록 선)의 단위가 각각 달라 생길 수 있는 있는 오해임.

2) 병렬처리 컴퓨터에서 다른 프로세서들은 처리해야할 작업들이 쌓여있는데 반해, 일부 프로세서들이 유휴상태에 있는 것을 방지하기 위하여, 프로세서들 간에 작업들을 고루 분배하는데 목표를 두고 있는 기술

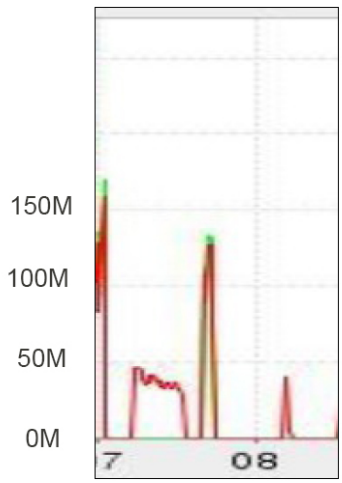


○ 아울러 06:00~07:00 사이 유입 트래픽의 98%를 차단할 정도로 디도스 공격이 집중되었으나, DDos장비는 이를 성공적으로 차단함.

○ 위 그래프 중 05:00~06:58분까지, 07:00~08:32 사이의 유입 트래픽 추이를 확대해 보았음



05:00~06:58분까지 유입 트래픽



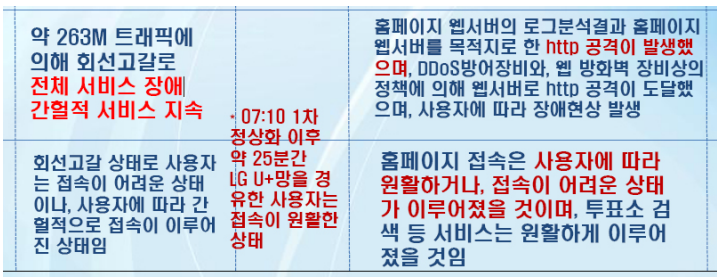
07:00~08:32분까지 유입 트래픽

○ 07:00가 넘어서면 유입트래픽 자체가 불안정하고 불규칙한 양상을 띰. 공격트래픽 또한 미미함(평균 10M bps 가량임)

○ 이러한 추이는 디도스 공격이 시스템에 별다른 영향을 미치지 못했으며 이후까지 지속된 선관위 인터넷서비스 장애 현상과는 무관하다는 것을 반증하고 있음.

○ 한편 디도스 보고서 10p 시간대별 DDos 공격 분석 결과에는 "07:10 1차 정상화 이후 약 25분간 LG U+망을 경유한 사용자는 접속이 원활한 상태"라고 기술되어 있음.

○ 총 유입트래픽 평균 40M(위 오른 쪽 그림)이며 방화벽 도달 트래픽과 일치함. 이 시기 디도스 보고서 다른 페이지를 참고하면 LG U+망 유입 트래픽은 10M 미만(12p) KT망 #1회선 유입은 30M 이상(11p)인 것으로 보임.



4. 엔시스 보고서 분석 결과

1) 디도스 공격 규모는 초당 221M, 4만4천 패킷 정도의 소규모 공격

○ 2011년 후반기 전세계 디도스 공격 추이를 분석한 기사에 따르면, 공격에 동원된 트래픽 규모의 평균치는 초당 5.2G 수준이었음. 선관위에 대한 공격은 이것의 1/20 수준임.

2) 당일 아침 기간 동안 방화벽은 정상 트래픽 규모 유지함.

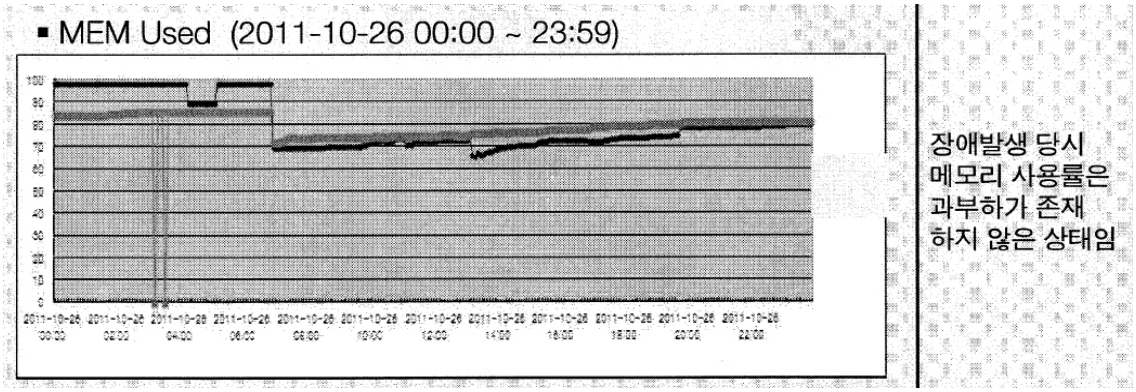
○ 디도스 방어장비는 시스템의 가장 앞에서 공격 트래픽을 걸러내고, 정상 트래픽을 통과시키는 장비임. 이후 방화벽 장비가 그 다음 단계에서 이 트래픽을 처리함. 때문에 방화벽 장비에 기록되는 트래픽은 정상적인 접속 요청 트래픽으로 볼 수 있음. 문제의 기간 동안 방화벽의 정상 트래픽량은 초당 10M 수준이었고, 처리세션도 3000세션 미만의 낮은 수준이었음(3분 단위로 측정), 엔시스 보고서 3.4 방화벽 장비에서는 그 이유를 "앞 단 DDos 보안장비에서 유해 트래픽이 차단되어 세션 수가 적었음"이라고 설명하고 있음.

○ 참고로 그날 하루의 트래픽 추이를 보면 저녁 8시-9시 사이에 접속량이 절정에 달하는데, 이때의 세션 수는 24만 세션(3분 단위 측정) 가량의 수준이었음. 따라서 3000세션이라면 선관위 서버가 아무 부담없이 처리할 수 있는 수준의 부하임.

3) 당일 디도스 공격 있기 전 메모리 과부화 현상

○ 방화벽을 통과한 트래픽은 웹서버가 처리. 선관위 홈페이지는 2대의 웹서버로 구축되어 있고, 선거정보 관련 페이지들은 5대의 웹서버로 구성되어 서비스되고 있음.[3] 그런데 엔시스 보고서 내 <홈페이지 웹서버#1 상세 분석 내역(첨부 3.6)>을 보면, "메모리 증가 현상으로 인한 장애방지 차원에서 06:52에 사용자에 의해 재 기동됨"이라고 되어 있고, <홈페이지 웹서버#2 상세 분석 내역(첨부3.7)>에도 그로부터 2분 뒤에 "메모리 증가 현상으로 인한 장애방지 차원에서 06:54에 사용자에 의해 재 기동됨"이라고 보고됨.

○ 쉽게 설명하면, 선관위 웹서버 관리자가 홈페이지 서버 상태를 살펴보니, 메모리(RAM)가 거의 소진되어 그냥 두면 안 될 것 같아 06:52과 06:54에 홈페이지 서버2대를 다시 시작(reboot)했다는 것임. 다음 표는 당시 메모리의 사용률이 나와 있는 <홈페이지 Web서버 성능 상세 분석 내역(첨부2, 2.3)>임. [4]



○ 이 그래프를 참조하면 00:00시부터 06:50까지 메모리 사용이 거의 100%에 이르고 있음을 볼 수 있음. 04:20경부터 05:20경까지 한시간 여 잠시 떨어졌으나 이후 다시 100%에 달하는데, 06:52과 06:54에 서버관리자가 재기동(reboot)을 한 후, 정상 수준(70%-80%)으로 돌아옴.

○ 접속자가 거의 없는 한밤중이나 새벽에 왜 선관위 홈페이지 웹서버 RAM 메모리 포화상태가 계속되었는지, 04:20경에는 어떤 조치로 메모리가 회복되었는지, 05:20경에는 무슨 일이 있었길래 다시 메모리가 소진되었는지 의문임.

○ 흥미로운 점은, 평가에 "장애발생 당시 메모리 사용률은 과부하가 존재하지 않은 상태임"

---

3) 선관위는 TMax사가 제작 납품한 WebtoB + JEUS 서버 소프트웨어를 사용하고 있음. 웹서버는 유저의 접속 요청을 처리하는 과정에서 DB서버와 교신하여 DB서버로부터 데이터를 가져와서 웹페이지를 실시간으로 생성하는 작업을 함.

4) 그래프 X축의 왼쪽 끝은 2011-10-26 00:00시이고, 오른쪽 끝은 23:59시임(2시간 단위). Y축은 메모리 사용률(0%에서 100%까지)임.

이라고 기입되어 있다는 점임. 그래프 상으로도 명백하게 틀릴 뿐 아니라, 같은 보고서 첨부3.6과 첨부3.7에서 "메모리 증가 현상으로 인한 장애방지 차원에서 06:52(6:54)에 사용자에 의해 재 기동됨"이라 적은 내용과도 모순되는 사항임.

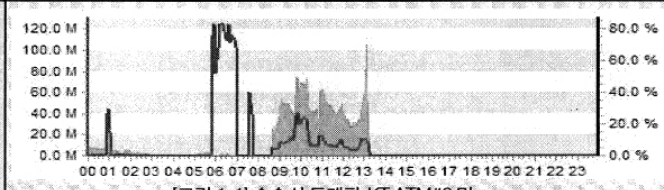
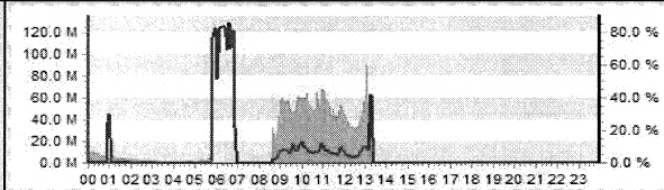
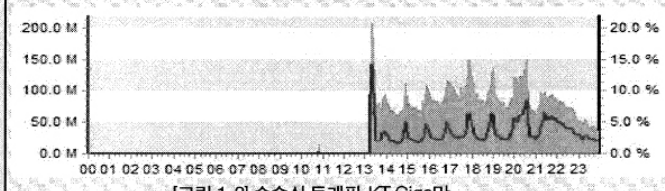
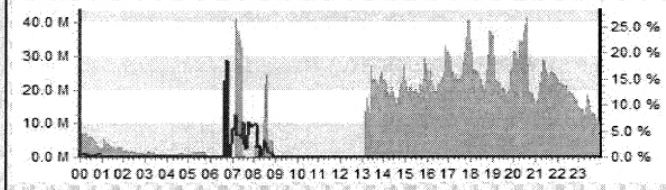
4) DB서버는 이상 없었음

○ DB서버에는 별다른 이상 상황이 발견되지 않음. 그도 그럴것이 06:54까지 홈페이지 웹서버 자체가 메모리 포화 상태였으므로 DB서버에 제대로 요청하지 못한 상황이었기 때문임.

○ 이 점은 선관위 보고서 DB Log에도 공통으로 나타남. 접속량은 3분에 3000세션 밖에 수준인데도, 어떤 이유에선지 웹서버의 메모리가 포화상태로 있었기 때문임.

5) 07:00~08:32 선관위의 KT 회선 차단

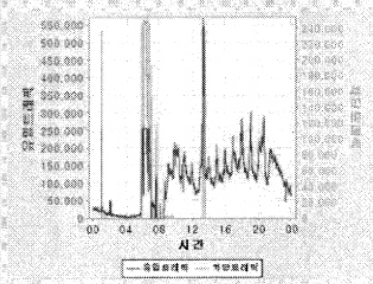
○ 엔시스 보고서 <3.분야별 분석내역 중 3.1 Router장비>에 의하면 웹서버의 메모리 포화상태가 재기동(reboot)로 06:54경에 해소되자, 약 5분 후인 07:00부터 08:32까지 선관위는 KT망 서비스를 끊음.

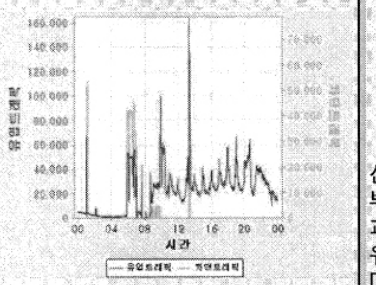
구분	점검 결과	비고
트래픽 추이현황 (KT ATM#0)	 [그림 1-1] 송수신 트래픽-KT ATM#0 망	선거당일 06시부터 07시 사이 대량의 트래픽이 유입됨. 07시부터 08시 32분까지 KT망 서비스를 단절함
트래픽 추이현황 (KT ATM#1)	 [그림 1-2] 송수신 트래픽-KT ATM#1망	선거당일 06시부터 07시 사이 대량의 트랙픽이 유입됨. 07시부터 08시 32분까지 KT망 서비스를 단절함
트래픽 추이현황 (KT Giga망)	 [그림 1-3] 송수신 트래픽-KT Giga망	선거당일 13시 11분 부터 GigaEthernet망 사용함.
트래픽 추이현황 (LG망)	 [그림 1-4] 송수신 트래픽-LGU+망	선거당일 08시42분 에서 13시사이 망 사용 중단함.

○ 이는 기술적으로 논란이 많을 수 밖에 없는 사안임. 앞서 선관위 보고서에 기술된 바와 같이 중앙선관위는 평소 3개의 회선 망을 이용함. KT망이 2회선(KT ATM#0, KT ATM#1) 그리고 LG U+망 1회선이며 각 회선은 초당 155M의 트래픽을 감당할 수 있는 용량임. 따라서 선관위는 이론적으로 합계 465M 규모의 트래픽을 감당할 수 있음.

○ 선거당일 06:00부터 07:00 사이 대량의 트래픽이 유입되었다고 하지만, 실은 221M 규모의 트래픽으로 3개 회선 중 KT망 2회선(용량 310M)만으로도 71% 수준이어서 충분히 처리할 수 있는 정도였음.

○ 그런데 이 상황에서 KT망 두개를 끊어[5] 221M의 트래픽이, 아직 남아 있는 LG U+망(용량 155M)으로 몰리는 과부하 상황이 연출됨. 디도스 장비까지 도달한 추이는 다음과 같음 <3.분야별 분석내역 중 3.2 DDos장비 중>

<table>
<tr><th>구분</th><th>점검 결과</th><th>비고</th></tr>
<tr><td>트래픽
추이현황</td><td>


[그림 1-1] 유입 트래픽(KBPS)


[그림 1-2] 유입 트래픽(PPS)
<table>
<tr><th rowspan="2">시간</th><th colspan="2">유입</th><th colspan="2">차단</th></tr>
<tr><th>BPS</th><th>PPS</th><th>BPS</th><th>PPS</th></tr>
<tr><td>06:00 ~ 07:00</td><td>221 M</td><td>44,679</td><td>211 M</td><td>35,854</td></tr>
<tr><td>07:00 ~ 08:00</td><td>27 M</td><td>4,892</td><td>14 M</td><td>2,393</td></tr>
<tr><td>08:00 ~ 09:00</td><td>26 M</td><td>6,052</td><td>551 K</td><td>871</td></tr>
</table>
</td><td>선거당일 06시 부터 07시 사이 과도한 트래픽이 유입 되었으며 DDoS 장비에서 DDoS 공격을 탐지하여 차단을 시킴</td></tr>
</table>

○ 위 표를 보면 06:00~07:00 사이에는 초당 221M 수준이던 유입 트래픽이 7시 이후에는 26M 수준으로 대폭 줄어듬. 왜 이렇게 유입 트래픽 자체가(공격 트래픽인지 정상 트래픽인지 가릴것 없이) 거의 1/10 수준으로 줄어들게 되는지에 대하여, 엔시스 보고서 <2. 장애분석요약 2-2 네트웍/보안 분야>를 보면, "07시 이후 08시30분까지 LG망을 통해 서비스하였으나 LG망과의 BGP Down/UP 연속발생으로 인해 서비스가 중단된 것으로 판단됨"이라고 기입함.

○ 이는 07:00에 KT망 2개를 끊고 LG U+망 하나로만 트래픽이 몰리는 한편, LG U+망과 연

5) 회선을 끊는다고 트래픽은 사라지지 않음. 인터넷은 애초에 군사목적의 교신 수단으로 개발된 것이기 때문에 회선의 일부가 절단되었다고 해서 트래픽이 사라지지 않으며 남아있는 다른 회선을 어떻게라도 찾아서 가도록 설계되어 있음.

결된 선관위 라우터가 꺼졌다/켜졌다(link up/link down)를 반복해서, 트래픽이 어느 망으로 선관위를 찾아가야 할지 판단하지 못하여 접속 트래픽(공격트래픽이건 정상트래픽이건)이 네트워크 주소를 제대로 찾아 오고가지를 못하게 되어 전반적으로 접속량이 줄어들었다는 것임.

6) 소결

○ 당일 00:00이전부터 06:54까지 홈페이지 웹서버 메모리가(어떤 이유에선가) 포화 상태로 내내 있었기 때문에 접속 요청을 제대로 처리하지 못했고,

○ 홈페이지 웹서버가 재기동(reboot)되어 메모리 포화 상태가 해소되자, 5분 뒤인 07:00부터는 그동안 무난하게 트래픽을 처리하던 상황에서 KT망 2회선을 단절하고 LG U+망 1회선으로 모든 트래픽이 몰림. 더욱이 선관위 라우터 스위치가 계속 꺼졌다/켜졌다(link up/link down)를 반복해 선관위로 트래픽이 오고가기 어렵게 되었음.

○ 08:30에 KT망 2회선을 다시 연결하여 정상화된 것으로 보임.

5. 풀리지 않는 의문

1) 06:58 왜 KT망 2회선을 단절했는가

○ 3개 회선(KT2 + LG1)으로 처리하던 상황에서 1개 회선에만 의존해야 하는 상황을 초래

- 3회선 용량(465M)의 47% 규모의 트래픽(221M)
- 1회선 용량(155M)의 142% 규모의 트래픽(221M)

○ 회선을 자르면 트래픽이 사라지는가

- 남아있는 회선으로 트래픽 집중 : 병목 현상 유발

○ KT는 공격PC의 ip에서 오는 트래픽을 자체 차단(LG는 차단 없이 목적지까지 통과시킴)

○ “긴박한 상황” “최후 수단”의 의미

- 유입 트래픽이 줄어드는데?
- 1시간34분 동안 긴박?

2) 07:10~07:35 사이 KT망#1회선을 복구했는데 왜 다시 단절했나

“KT망 공격여부 확인을 위한 일시적 회선 복구로 트래픽 유입” (디도스 보고서 p11)

○ KT망 공격 - 50M미만 트래픽으로 <망>을 공격하는 것이 가능한가?

○ 회선 복구(link up)해 보니, 공격트래픽이 거의 없었음.

○ 별 공격도 없고, 40M 수준의 정상트래픽이 유입되는 사실을 25분간 확인하고 왜 다시 단절했는가.

○ KT망 #2는 왜 복구하지 않았나

3) 2011.11.26에 나온 LG 엔시스 기술보고서의 대한 대응은 왜 없었나

○ “정상적인 서비스가 이루어지지 못한 이유는 Router와 LG망과의 BGP Down으로 인한 것” - 엔시스 보고서 <3.1 종합의견>

○ “KT와 LG U+에 BGP Down/Up 발생에 대한 자료를 받아 분석할 것”

- LG엔시스 보고서 <2-2 총평>

토론 1

공공기관의 정보공개 관점에서 본 중앙선관위의 정보공유 방식

김유승 / 중앙대 문헌정보학과 교수, (사)투명사회를위한정보공개센터 이사

1.

이제 이 자리에 토론하고자 하는 사건의 이름부터 고쳐 불러야 할 것 같다. 10월 26일 서울시장보궐선거 당일 일어난 일련의 사건을 DDos 사태라 부르는 것 자체가 사건의 본질을 가리는 것이기 때문이다. 이는 전방위적 선거방해 행위이며, 민주주의 근간을 뒤흔든 엄중한 사건이다. 하지만, 그동안 일반 시민들의 사건의 실체적 진실에 다가설 수가 없었다. 모든 관련 정보가 숨겨지고 가려져왔다. 도대체 그날 아침 무슨 일이 일어난 것인지, 국민 모두가 궁금해 했지만 누구도 속 시원한 대답을 주지 않았다. 그러는 사이 의혹은 더 부풀어갔고, 헌법기관인 선거관리위원회에 대한 안타까운 불신 또한 커져 갔다.

사건의 시작부터 이제까지 선거관리위원회는 나름의 노력을 하였다 주장하지만, 시민들의 시각에는 실체를 투명하게 드러내고 알리고자 하는 노력이 보지 않았다. 그리고 너무도 뒤늦게 부분 공개된 한 보고서를 가지고 이 자리에 모였다.

2.

지난 2011년 12월 23일, 참여연대는 10.26 재보궐선거일 사이버 선거방해행위 사태와 관련하여, 선관위와 선거관리시스템 공급 업체간 재발 방지 및 원인규명을 위한 자료를 정보공개 청구하였다. 이에 선거관리위원회는 신속하게, 너무도 신속하게 12월 27일 정보공개청구에 대한 비공개결정을 통보한다.

비공개 사유는 <공공기관의 정보공개에 관한 법률> 제9조 제1항 제4호였다. “진행중인 재

판에 관련된 정보와 범죄의 예방, 수사, 공소의 제기 및 유지, 형의 집행, 교정, 보안처분에 관한 사항으로서 공개될 경우 그 직무수행을 현저히 곤란하게 하거나 형사피고인의 공정한 재판을 받을 권리를 침해한다고 인정할 만한 상당한 이유가 있는 정보"가 4호에 규정하는 비공개 대상 정보이다. 실상 10.26 선거방해행위에 대한 다수의 정보공개청구에 대한 비공개 사유 역시 같은 법 같은 조항이었다.

정보공개센터를 통해 다수의 정보공개청구 사례를 접했던 터라 크게 놀랄 일도 아니었다. 사실 조금 예상했던 대로였다. 제1항 제4호는 고무줄처럼 늘었다 줄었다 하는 전가의 보도와 같은 비공개사유이기 때문이다.

특정 사건의 수사 또는 재판에 관한 정보가 악의적으로 유출되고, 이에 대해 아무도 책임지지 않았던 기억은 그리 멀지 않다. 노무현 대통령, 한명숙 총리, 그리고 곽노현 교육감. 하지만, 정작 온 국민의 관심을 모았던 이 사건에는 그 엿가락 같은 잣대를 다시 들이밀었다. 그것도 전광석화의 속도로 말이다.

3.

어쨌든 현행법이니 4호가 존재할 만한 "상당한 이유"가 있다고 치자. 참여연대 정보공개청구한 정보가 정말 4호의 비공개대상 정보일까? "사태재발 방지와 원인규명 논의 자료가 어떻게 사법당국의 직무수행을 '현저히' 곤란하게 하고 피고인의 권리를 침해하는지" 모를 일이다. "선관위가 로그 기록 전체도 아닌, 당시 상황 통계 기록까지 공개 못할 이유는 없었으며, 오히려 선관위가 발벗고 나서 투명한 공개를 해야 할 사안"이었다. 로그 파일 공개의 경우도, IP 주소 등 개인정보보호 차원에서 일부 정보의 공개가 어렵다고 한다면, 그 부분만 가리고 공개했어야 한다.

이런 판단 아래 비공개 결정에 대한 이의신청이 제기된다. 첫 번째 정보공개청구에서 신속한 비공개결정을 내렸던 선과위가 이번에는 이의신청결정기간을 연장하기까지 한다. 연장사유는 해당 자료가 선관위와 관련 업체에서 관리하고 있는 중요 시스템 정보 및 개인정보가 포함되어 있어서, 관련 업체에서 보유한 정보의 공개여부에 관한 협의가 필요하다는 것이다.

관련 업체라니 이게 웬 말인가? 정보공개법 제12조는 정보공개여부를 심의하기 위하여 정보공개심의회를 설치, 운영한다고 규정하면서, 정보공개심의회의 구성원을 법에 따라 지명 또는 위촉하도록 되어 있다. 제3자에게 협의하라고 되어 있지 않다.

그럼 그 관련 영리 업체가 헌법기관인 선거관리위원회의 정보공개심의 위원인가? 정보공개업무의 주체는 헌법기관인 선거관리위원회, 그리고 선거관리위원회 정보공개심의회이다. 그 판단에 있어 제3자의 협의 또는 허락을 얻어야 한다는 것은 납득하기 어렵다. 제3자의 개인정보나, 영업비밀 등의 보호를 위해서라면 그 부분만 비공개하면 그만이다. 협의할 일은 아니다.

결국 2012년 2월 11일 유지보수업체 분석보고서가 부분 공개되었다. 최초 정보공개청구를 한 지 거의 2달만의 일이다.

4.

이번 사건의 의혹을 증폭시킨 선거관리위원회의 불성실한 정보공개 사례는 이것만이 아니다. 지난 2011년 11월 4일 서울시 선거관리위원회 투표소 현황에 대한 정보공개가 청구되었다. 하지만, 서울시 선관위는 투표소 변경 사유에 관한 자료가 존재하지 않아 공개할 수 없다고 했다. 그런데 11월 15일 강남구에서 변경 사유를 기재하여 보내왔다. 25개구마다 공개와 비공개가 들쭉날쭉이다. 게다가 공개한 자료의 범위, 형식이 각각 다르다.

표 1) 각 구 선관위별 투표소 현황 정보공개 현황

지역구	공개 여부	파일 형식	비고
강남	O	excel	
강동	O	pdf	
강북	O	pdf	
강서	O	excel	
관악	X		
광진	X		
구로	X		
금천	X		
노원	O	excel	
도봉	X		
동대문	X		
동작	X		
마포	O	excel	
서대문	O		교육감 선거 투표소 현황만 공개, 변경사유는 문서 부존재
서초	O	excel	
성동	O		무상급식 주민투표, 6.2 지방선거, 교육감 선거 투표소 현황만 공개, 변경 사유 없음
성북	O		무상급식 주민투표, 6.2 지방선거, 교육감 선거 투표소 현황만 공개, 변경 사유 없음
송파	X		서울시에서 기통지함 것으로 대체
양천	X		서울시에서 기통지한 것으로 대체
영등포	O	excel	
용산	O		무상급식 주민투표, 6.2 지방선거, 교육감 선거 투표소 현황만 공개, 변경 사유 없음
은평	O		서울시장 보궐선거, 무상급식 주민투표, 6.2 지방선거 투표소 현황만 공개, 변경 사유 없음
종로	O	pdf	무상급식 주민투표, 6.2 지방선거, 교육감 선거 투표소 현황만 공개, 변경 사유 없음
중구	O		
중랑	O		무상급식 주민투표, 6.2 지방선거, 교육감 선거 투표소 현황만 공개, 변경 사유 없음

5.

유권자자유네트워크는 현재 중선관위 회의록 비공개처분취소 행정소송 중이다. 지난 10·26 재보궐 선거 직후, 유자넷은 선관위에 '2011년 1월부터 10월까지 개최된 선관위 회의의 개최 일시, 참석자, 안건, 결정사항, 회의록 내역'에 대해 정보공개청구했다.

그러나 선관위는 회의록에 대해서만 유독 비공개 결정을 통지했다. 비공개 사유는 정보공개법 제9조 제1항 제5호 "의사결정과정 또는 내부검토과정에 있는 사항 등으로서 공개될 경우 업무의 공정한 수행이나 연구·개발에 현저한 지장을 초래한다고 인정할 만한 상당한 이유가 있는 정보"라는 것이다.

하지만 유자넷이 법원에 제출한 소장을 통해 밝혔듯이, 중앙선관위가 공정성과 투명성을 지키고자 했다면, 회의록을 통째로 비공개하는 것은 납득할 수 없는 결정이다.

6.

현재 헌법학자인 강경근 교수가 중앙선거관리위원회 상임위원인 것으로 안다.

강경근 교수는 우리나라 최초의 정보공개법을 만드는 데 참여하신 분이다. 10여 년 전 한 신문과의 인터뷰에서 비밀행정주의 관행을 지적하며 "비공개정보의 개념규정이 너무 광범위하고 용어가 포괄적·자의적"이라고 안타까움을 토로하신 기사가 기억난다. (한겨레신문 1996.11.18)

선관위가 이번 사건에 대한 정보공개에 대해 이와 같은 전향적인 자세를 취했더라면, 지난 3개월여 동안의 의혹과 불신으로 빚어진 사회적 비용은 필요 없었을지도 모른다. 시민들이 이 사건의 실체에 접근할 알권리가 보장되었을 것이다. 이제부터라도 이 사건의 그리고 업무 전반의 정보공개에 대한 선관위의 변화를 기대해본다.

토론 2

10.26 DDos관련 새로운 의혹제기에 대한 설명자료

제출 박혁진 중앙선관위 정보화담당관

(설명 유훈옥 중앙선관위 정보화담당관실 전산사무관)

10. 26. DDoS관련 새로운 의혹제기에 대한 설명자료

2012. 2.

중앙선거관리위원회
(정보화담당관실)

○ 홈페이지 웹서버 재기동 의혹에 대하여

- 중앙선관위가 참여연대의 정보공개청구에 의해 제공한 LG엔시스의 『중앙선거관리위원회 2011년 10월 26일 재보궐선거 서비스 장애 분석 및 보고서(2011.11.26)』 중 첨부3. 의 '3.6 홈페이지 웹서버 #1 상세 분석 내역' 및 '3.7 홈페이지 웹서버 #2 상세 분석 내역'에 따르면 홈페이지(www.nec.go.kr) 웹서버 #1과 #2 각각 점검결과 항목에 '이상없음. 메모리 증가 현상으로 인한 장애방지 차원에서 06:54분에 사용자에 의해 재기동됨' 이라는 내용이 기재되어 있습니다.
- 이 내용을 근거로 '나꼼수 봉주6회('12.2.22 방송분)'에서는 당일 12시부터 웹 서버 메모리가 100%에 이르러 리부팅을 해야 하는데 오전 6시 52분 내지 54분까지 조치를 하지 않고 버티다가 리부팅을 하자마자 KT 회선 2개를 끊어버려 서비스를 의도적으로 차단한 것이라고 주장하고 있습니다.
- 김기창 교수는 오픈웹 사이트에서도 다음과 같이 '나꼼수'와 유사한 의혹을 제기하고 있습니다.
  · 당일 0:00(또는 그 이전) 부터 6:54까지는 홈페이지 웹서버 RAM 메모리가 (어떤 이유에선가) 포화 상태로 내내 있었기 때문에 접속 요청을 제대로 처리하지 못했다.
  · 홈페이지 웹서버가 reboot되어 메모리 포화 상태가 해소되자, 5분 뒤인 7시 부터는 그동안 널널하게 트래픽을 처리하던 상황에서 KT망 두개를 자르고 LG망 하나로만 모든 트래픽이 몰리도록 한 다음, 누군가가 선관위 스위치 라우터를 계속 장난질쳐서 선관위로 트래픽이 오고가기 어렵게 만들었다가 8시 반에 KT망 두개를 다시 연결하여 정상화 된 것으로 보인다.
- 또한 시스템개발자 barry_lee씨는 다음과 같은 의혹을 제기하고 있습니다.
  · 디도스 공격이 시작되었는데, 디도스에 대한 대응을 먼저 하지 않고 한가하게 홈페이지 서버 재시작이나 하고 있었다.
  · 서버의 재시작은 뭔가 설정을 변경했을 때 하기도 하므로 의혹의 여지가 있다.
  · 디도스로 트래픽이 꽉 차있는데 IDC에 있는 선관위 웹서버에 접근을 해서 재기동 한다는 것은 말이 안된다.

➔ 이러한 주장은 10.26. 디도스 공격으로 06시부터 08시30분경까지 중앙선관위 홈페이지 접속장애가 있을 당시 홈페이지 웹서버가 메모리가 포화되어 서비스 처리가 제대로 되지 않았고, 이 장애는 KT 회선 절체와 서로 연관을 가지고 누군가에 의해 의도적으로 이루어졌다는 가정에 근거하고 있지만, 이는 기술적 부분

및 기초적인 사실에 대한 오해에서 비롯된 것으로 사실과 다름

1) 당일 06시 52분과 06시 54분에 메인 홈페이지 서버를 재기동한 것은 시스템 재기동(reboot)이 아니라 웹서버 데몬을 재기동한 것입니다. 웹서버 재기동하는 동안 웹서비스가 중단되지 않으며, 또한 rebooting이 아니므로 설정 변경도 없었음

○ 아래 표와 같이 재기동시간은 서버의 종류마다 다르며, OS를 reboot 하려면 최소 15분 정도 걸림. 따라서 두 대의 서버를 reboot 하려면 총 약30분 정도 소요되었을 것이며, 2분 간격으로 두 대의 웹서버를 재기동 했다는 것만으로도 보고서의 재기동은 데몬 restart임을 알 수 있음

구분	종료소요시간 (명령어)	기동소요시간 (명령어)	총 소요시간
웹서버 (WebToB)	약 3초 이내 (wsdown)	약 3초 이내 (wsboot)	약 6초 이내
WAS서버 (JEUS)	약3~5분 (jdown)	약3~5분 (jboot)	약 10분 이내
H/W (유닉스서버)	약 5분	약 5~10분	약 15분 이내

★ 중앙선관위 웹서버 구성 : 웹서버 WebtoB, WAS는 Jeus, H/W는 유닉스 서버 사용.

○ 데몬 재기동 시 이중화된 두 대의 웹서버 데몬을 차례로 재기동했기 때문에 재기동하는 동안 서비스 중단이 발생하지 않았으며, 심지어 서버 reboot를 했다고 할 지라도 두 대의 웹서버를 차례로 재기동할 경우 서비스 중단이 발생하지 않았을 것임

2) 웹서버의 memory saturation 현상은 WebtoB 소프트웨어의 버그 때문임

○ 10.26. 당시 선관위 웹서버 버전은 WebtoB 4.1.0.2 버전으로, PipeLine Request 시 memory leak 버그, 즉 PipeLine Request의 응답이 304 또는 hth cache 일 경우 memory를 해제하지 않는 버그가 존재함 (티맥스 WebtoB 릴리즈 노트)

○ 선관위의 웹서버 담당자는 이 버그를 10.26. 전에 인지하였으나, 선거기간 중 시스템 패치작업은 서비스 중지 등 예기치 못한 위험이 발생할 수

있기 때문에 티맥스소프트 엔지니어에게 문의한 결과 해당 버그는 서비스에 미치는 영향이 심각하지 않다는 회신을 받고 선거 후에 패치하기로 협의하였으며, 10.26. 당일 memory saturation 현상은 웹서버 데몬 재기동으로 조치한 것임

○ 메인 홈페이지 뿐 아니라 선거정보 웹서버(info.nec.go.kr) 5대의 메모리 사용율 그래프도 유사한 패턴을 보이는 것 역시 WebtoB의 버그 때문이며, 이 또한 메모리 증가 현상으로 인한 장애 방지 차원에서 20시 28분에 재기동(데몬 restart)한 것임

3) 메인 홈페이지 웹서버의 memory saturation 현상으로 인한 서비스 장애는 없었음

○ 선거 당일 홈페이지는 평소 운영하는 홈페이지가 아니고 선거정보(info.nec.go.kr) 사이트로 안내하기 위한 약 7KByte 크기의 intro page로 교체됩니다. 이 페이지는 DB와 연결되는 동적 페이지는 없고 html 코드만 정적(static)으로 보여주는 화면입니다. 따라서 동일한 요청(request)에 대해 caching이 되므로 메모리가 추가로 소요되지 않음

○ 00시부터 웹서버 데몬을 재기동한 07시까지 메인홈페이지 웹서버 중 1대는 16GByte 메모리 중 98.4%를 사용하고 약 260MByte의 가용 메모리를 가지고 있었으며, 다른 한 대의 웹서버는 약 2.32GByte의 가용 메모리를 가지고 있어 총 2.58GByte의 가용 메모리를 가지고 있었으며, 당시 담당 엔지니어는 비록 메모리의 사용율이 높기는 하지만 서비스에 문제가 없다고 판단되어 계속 모니터링만 하고 있었음. 그런데 디도스 공격으로 인해 홈페이지 접속 장애가 생기자, 만약의 경우에 대비하여 7시경 웹서버 데몬을 재기동하여 웹서버 한 대는 260MByte에서 4.85GByte로, 다른 한 대는 2.32GByte에서 4.56GByte로 총 5.97GByte의 여유 메모리를 확보한 것임

○ 선거정보(info.nec.go.kr) 웹서버 5대는 총 메모리 30.19GByte를 확보하여 정상적으로 작동하였음

4) 선관위의 시스템은 통신서비스 사업자의 IDC에 입주해 있지 않고, 자체 전산실을 보유하고 있음

○ 디도스로 모든 회선이 막힌 상태에서 선관위 서버 담당자가 어떻게 원격에 있는 웹서버에 접근하는 것은 불가능하며 누군가에게 지시를 내렸다는

의혹을 제기하는 것은 선관위 시스템 구성에 대한 오해에서 비롯된 것임. 웹서버 재기동은 서버 담당자가 전산실에서 직접 작업하였으며, 또한 서버 담당자와 통신, 보안 담당자가 서로 다르기 때문에 각자 자신이 맡은 역할을 수행한 것이지, 디도스에 대한 대응을 뒤로하고 한가하게 웹서버 재기동을 한 것이 아님

❑ 결 론

- ❍ 중앙선관위 메인 홈페이지(www.nec.go.kr) 웹서버의 재기동은 시스템 rebooting이 아닌 웹서버 데몬 restart로 KT회선 절체와 직접적인 관련이 있는 것이 아니며, 웹서버 재기동으로 인한 서비스 중지가 발생하지 않았음
- ❍ 메인 홈페이지 웹서버 메모리 포화시에도 약 2.58G의 가용 메모리가 확보되어 있었으며, 실제로도 웹서버로 인한 서비스 장애는 발생하지 않았음

○ 세개의 회선으로 넉넉하게 처리하던 상황(회선 총용량의 절반에도 못미치는 트래픽을 처리하던 상황)에서 회선 두개를 끊은 이유는?

➜ KT 2회선을 차단하고, LG U+ 1회선을 유지하는 결정을 하는 당시의 상황은 우리위원회 홈페이지 접속장애 현상에 대한 원인 파악과 조치단계에서 KT 2회선으로 대량의 패킷이 유입되는 DDoS로 공격으로 인지 한 후, 우리위원회가 2011. 3. 제정하여 운영 중인 『분산서비스거부(DDoS)공격 대응지침』 중 DDoS공격 대응절차의 3단계 초동조치에 의거 공격으로 사용되는 좀비 PC를 차단하는 조치를 취하며, KT와 공조를 통해 KT측에서도 접속차단 하도록 조치를 취하고 있었음.

➜ 당시 LG U+ 1회선의 사용량은 경미한 상태였고, KT측으로 들어오는 DDoS 공격을 ACL등록 방법으로 완화시키는 조치에 한계가 있는 것으로 판단하여 KT 2회선을 차단하는 결정을 하게 되었음

➜ 이러한 결정은 『분산서비스거부(DDoS)공격 대응지침』 중 DDoS공격 대응절차의 5단계 차단조치에 의거 조치한 사항임

다. 3단계 : 초동조치

○ DDoS공격으로 판명되면, 정보보호담당실무자는 기술대응절차서에 따라 장비별 담당실무자로 하여금 피해규모를 최소화하기 위하여 공격IP주소 차단, 장비 임계치 조정 등 기본조치를 수행하도록 한다.

(중략)

마. 5단계 : 차단조치

(중략)

○ 정보보호담당실무자는 DDoS공격에 대한 지속적 차단조치에도 불구하고 피해범위가 계속 확산되고 방어조치가 원활히 이루어지지 않는다고 판단되면, 정보보호책임관 및 정보보호책임자에게 보고하고 네트워크 케이블의 일시단절 및 서버 재부팅 등 강력한 대응조치를 수행할 수 있다.

○ 10. 26. 당시 총 465Mbps(KT : 310Mbps(155Mbps 2회선), LG U+ :155Mbps 1회선)의 회선 용량에 263Mbps 또는 221Mbps의 사용량을 계산하여 56% 정도 사용하였다는 견해에 대하여

➜ 최소 경로를 배정받는 라우팅 경로상 KT회선으로 들어오는 경로가 최소경로임에 따라 (LG회선에 연결된 라우터의 BGP정책에 따라서 사용자는 KT회선으로 최소경로를 배정받아 들어옴) KT회선으로 유입된 패킷이 많았음

➜ DDoS공격 발생 상황이 아니더라도 평시에도 KT회선을 주로 많이 사용하고 있으며, LG U+에 가입된 가입자의 경우 LG U+ 회선이 연결된 구간을 이용하게 됨

➜ 따라서 모든 사용자에 대해 KT 2회선과 LG U+ 1회선 총 3회선 즉 465Mbps를 적정하게 이용할 수 있도록 하는 것이 아니며, 사용자가 가입된 통신사업자의 중앙선관위 접속경로 중 최소경로를 배정받아 접근하는 방법이 적용됨에 따라, KT 회선의 이용률이 LG U+보다 상대적으로 많게 됨

➜ KT회선의 310Mbps이고 이것을 기준으로 하여, 선관위에 연결된 라우터 인터페이스가 ATM모듈임에 따라 이더넷으로 변환 시 Data패킷이 차이가 발생함 (ATM header를 Ethernet header로 변환하는 과정을 거치므로 약 85%의 속도를 지원하는 것으로 되어 있음. OC-3 155Mbps의 경우 약 130Mbps의 속도를 낼 수 있음)
(KT와 LG U+의 공식적인 입장임)

※ LG U+를 제외한 KT, SK Broadband, 기타 통신사업자의 경우 KT회선을 주로 이용하게 됨 (통신사업자의 공식적 의견 임)

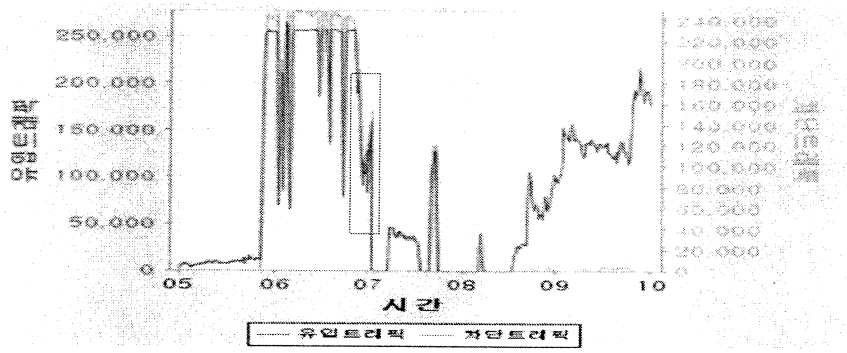
※ LG U+ 회선에 연결된 라우터 Config 내역

```
router bgp 3XXXX
 no synchronization
 bgp router-id 210.XXX.XX.XX
 bgp log-neighbor-changes
 network 58.XXX.XX.XX mask 255.255.255.0
 network 210.XXX.XX.XX
 network 210.XXX.XX.XX  mask 255.255.255.192
 neighbor 58.XXX.XX.XX remote-as 9950
 neighbor 58.XXX.XX.XX  soft-reconfiguration inbound
 neighbor 58.XXX.XX.XX  route-map permit_subnet_prepend out
 neighbor 58.XXX.XX.XX  filter-list 1 out
 neighbor 172.XXX.XX.XX  remote-as 3XXXX
 neighbor 172.XXX.XX.XX  next-hop-self
 neighbor 172.XXX.XX.XX  soft-reconfiguration inbound
 no auto-summary

 route-map permit_subnet_prepend permit 10
 match ip address prefix-list permit_subnet
 set as-path prepend 3XXXX 3XXXX 3XXXX
```

○ KT망을 끊기 전 06:58 상황은 긴박하지도 않았고, 유입트래픽은 회선 용량 절반에도 훨씬 못 미치고, 디도스 방어장비는 공격트래픽을 말끔히 걷어내고 약 10M bps 규모의 정상 트래픽을 통과시키고 있는 상황이었다는 견해에 대하여

➜ 06:46경 KT회선 #1을 차단(Sub interface down)함으로써 KT회선 #2를 통해 유입된 패킷에 대한 용량이며, DDoS 장비에 유입된 패킷은 2개의 회선을 유지시킬 당시보다 감소한 현상을 보이고 있는 것임




```
Oct 26 06:39:55: %BGP-5-ADJCHANGE: neighbor 172.XXX.XX.5 Down BGP Notification sent
Oct 26 06:39:55: %BGP-3-NOTIFICATION: sent to neighbor 172.XXX.XX.5 4/0 (hold time expired) 0 bytes
Oct 26 06:42:40: %BGP-3-NOTIFICATION: sent to neighbor 172.XXX.XX.5 passive 2/8 (no supported AFI/SAFI)
3 bytes 000101
Oct 26 06:46:04: %BGP-5-ADJCHANGE: neighbor 172.XXX.XX.1 Down Interface flap
Oct 26 06:46:33: %SYS-5-CONFIG_I: Configured from console by console
Oct 26 06:47:22: %BGP-5-ADJCHANGE: neighbor 172.XXX.XX.1 Up
Oct 26 06:47:24: %BGP-3-NOTIFICATION: sent to neighbor 172.XXX.XX.5 passive 4/0 (hold time expired) 0
bytes
Oct 26 06:47:39: %SYS-5-CONFIG_I: Configured from console by console
Oct 26 06:49:00: %SYS-5-CONFIG_I: Configured from console by console
Oct 26 06:49:28: %BGP-5-ADJCHANGE: neighbor 172.XXX.XX.1 Down BGP Notification sent
Oct 26 06:49:28: %BGP-3-NOTIFICATION: sent to neighbor 172.XXX.XX.1 4/0 (hold time expired) 0 bytes
Oct 26 06:49:40: %SYS-5-CONFIG_I: Configured from console by console
Oct 26 06:49:48: %BGP-5-ADJCHANGE: neighbor 172.XXX.XX.1 Up
Oct 26 06:51:24: %BGP-5-ADJCHANGE: neighbor 172.XXX.XX.1 Down BGP Notification sent
Oct 26 06:51:24: %BGP-3-NOTIFICATION: sent to neighbor 172.XXX.XX.1 4/0 (hold time expired) 0 bytes
Oct 26 06:51:42: %BGP-5-ADJCHANGE: neighbor 172.XXX.XX..1 Up
Oct 26 06:53:47: %BGP-5-ADJCHANGE: neighbor 172.XXX.XX.1 Down BGP Notification sent
Oct 26 06:53:47: %BGP-3-NOTIFICATION: sent to neighbor 172.XXX.XX.1 4/0 (hold time expired) 0 bytes
Oct 26 06:54:05: %BGP-5-ADJCHANGE: neighbor 172.XXX.XX.1 Up
Oct 26 06:56:16: %BGP-5-ADJCHANGE: neighbor 172.XXX.XX.1 Down BGP Notification sent
Oct 26 06:56:16: %BGP-3-NOTIFICATION: sent to neighbor 172.XXX.XX.1 4/0 (hold time expired) 0 bytes
Oct 26 06:56:24: %SYS-5-CONFIG_I: Configured from console by console
Oct 26 06:56:34: %BGP-5-ADJCHANGE: neighbor 172.XXX.XX.5 Up
```

○ 6시부터 오후 1시까지 LG 망이 이상 증상을 보였다. (경로를 못 찾고 헤매는 현상)견해에 대하여

➜ 07:00경 KT회선 단절 후 LG U+망을 이용하였으며, KT 사이버대피소로 이동한 후 08:53 ~ 13:11 까지는 LG U+망을 이용하지 않음

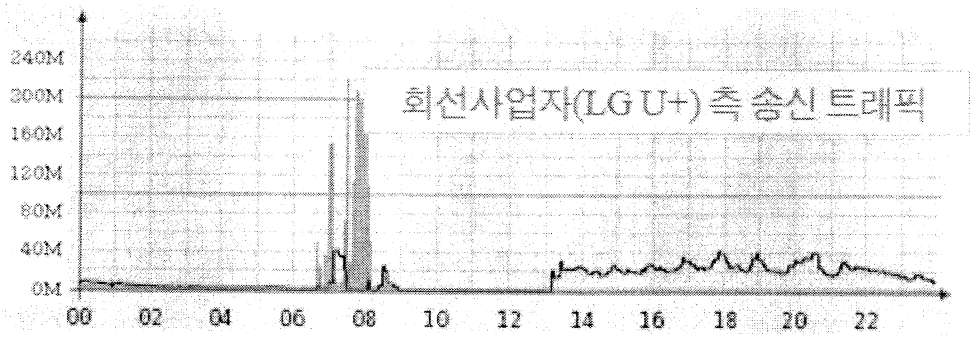
○ 이 보고서만으로 판단할 때, 선관위 라우터에 디도스 공격이 도달한 시점은 5:50부터 7:00 뿐이다. 7:00에서 8:32 까지는 KT 망이 끊어졌기 때문에 선관위 라우터에 도달한 디도스 공격이 없었다는 견해에 대하여

➜ KT회선이 연결된 라우터의 Sub interface를 down하여 LG U+회선으로 패킷이 유입되었으며, 디도스 대량 패킷이 유입되어 라우터의 BGP가 up/down되는 현상이 발생하여 정상적인 서비스가 어려운 상황이었으나, 이 상황에서도 DDoS패킷이 유입되었음

```
Oct 26 07:00:56: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:00:56: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:01:28: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:01:41: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:01:41: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:02:13: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:02:25: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:02:25: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:02:57: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:03:10: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:03:10: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:03:42: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:03:55: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:03:55: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:04:27: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:04:38: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:04:38: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:05:11: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:05:23: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:05:23: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:05:55: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:06:11: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:06:11: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:06:43: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:06:56: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:06:56: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:07:28: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:07:40: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:07:40: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:08:12: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:08:24: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:08:24: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:08:56: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:09:08: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:09:08: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:09:40: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:29:38: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:29:38: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:30:10: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:30:22: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:30:22: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:30:54: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:31:06: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:31:06: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:31:38: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:31:59: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:31:59: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:32:31: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:32:44: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:32:44: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:33:16: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:33:28: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:33:28: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
```

○ LG U+망이 제대로 작동하지 않은 이유는 BGP Down으로 인해 트래픽이 제대로 전달되지 않았다고 되어 있다. 이는 원래 155MBps의 회선 대역폭이 있는데 여기에 200MBps가 유입되었고, 이 과정에서 30MBps 만 전달되고 나머지는 아예 상호 전송이 안되는 이상현상이 발생됐다는 의미다. 하지만 아래 그래프 만으로는 LG U+망에 200MB가 유입된 흔적을 찾기 어렵다는 견해에 대하여

➜ LG U+로부터 제공된 MRTG 그래프에 의하면 약 200M의 트래픽이 선관위로 유입되었음.



중앙선거관리위원회 DDoS관련 기술분석 보고서 中 12페이지 (3-2. DDoS장비 등 분석결과(5)

○ LG U+망은 왜 비정상 동작했는가?

➜ 대량의 DDoS 공격패킷에 기인하여 BGP up/down현상이 지속적으로 발생하여 정상적인 작동이 어려운 상황이었음

```
Oct 26 07:00:56: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:00:56: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:01:28: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:01:41: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:01:41: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:02:13: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:02:25: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:02:25: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:02:57: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:03:10: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:03:10: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:03:42: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:03:55: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:03:55: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:04:27: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:04:38: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:04:38: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:05:11: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:05:23: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:05:23: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:05:55: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:06:11: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:06:11: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:06:43: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:06:56: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:06:56: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:07:28: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:07:40: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:07:40: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:08:12: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:08:24: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:08:24: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:08:56: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:09:08: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:09:08: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:09:40: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:29:38: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:29:38: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:30:10: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:30:22: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:30:22: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:30:54: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:31:06: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:31:06: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:31:38: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:31:59: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:31:59: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:32:31: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:32:44: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:32:44: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
Oct 26 07:33:16: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Up
Oct 26 07:33:28: %BGP-5-ADJCHANGE: neighbor 58.XXX.XX.161 Down BGP Notification sent
Oct 26 07:33:28: %BGP-3-NOTIFICATION: sent to neighbor 58.XXX.XX.161 4/0 (hold time expired) 0 bytes
```

O KT의 사이버 대피소(클린존) 서비스는 이미 2009년에 시작된 서비스다. 즉, 몰랐다면 직무 유기고, 알았다면 내부자 조력이 되는 셈이다라는 견해에 대하여

➜ KT의 사이버대피소 서비스는 KONET에 가입된 기업을 상대로 하는 서비스임. 선거관리위원회는 PUB넷이라는 국가 및 공공기관이 이용하는 망에 가입되어 있으며, PUB넷은 사이버대피소 서비스를 제공하고 있지 않음. 따라서 10. 26. 당시 디도스 공격상황이 발생했을 때 KT에서 긴급하게 사이버대피소를 이용할 수 있는 기술적인 협조를 받아 08:32경 서비스를 정상화하였음

○ The 서버관리자 to ISP : "여보세요? 아 예 저희 선관위 회선으로 다량의 UDP와 ICMP 공격이 들어와 문제가 생겼습니다. 일단 공격을 차단해 주시구요. 저희 회선 대역폭좀 늘려주세요. 네 감사합니다." 라는 견해에 대하여

➜ 위의 견해는 IDC(Internet Data Center)에 입주되어 있음을 전제로 하나, 선거관리위원회는 IDC에 입주해 있지 않고 자체 전산실을 운영하고 있음.

➜ 155Mbps가 연결된 라우터의 모듈은 ATM-155M모듈로서 155Mbps 이상으로 증속을 위해서는 라우터에 장착할 이더넷모듈이 필요하며, 대역폭 증속을 위한 작업은 다음과 같음.

1. 대역폭을 증속하기 위한 광전송로 확보
2. 광전송로 확보 후 ISP사업자의 라우터 장비에 연결하기 위한 작업
3. 선관위측 라우터장비에 광단자 연결 작업
4. 양측에 회선시험
5. IP셋팅 및 라우팅 작업

1~4. 작업이 사전준비가 되어 있는 경우 약 10~20분정도 소요되나
사전준비가 되어 있지 않은 경우 1~4. 작업을 완료하기 위해서는 수 시간 이상 소요됨
(KT 및 LG U+의 공식적인 입장임)

참여연대

정부지원금 0%, 참여연대는 회원의 회비로 운영됩니다
시민의 시민단체 참여연대 회원이 되어주세요
회원가입 02-723-4251 www.peoplepower21.org