kt

수 신 처: 중앙선거관리위원회 위원장
시행일자: 2011.11.01
보 기: 정보화담당관
제 목: 중앙선거관리위원회 홈페이지 접속장애 조치내역 송부

1. 관련

가. 정보화담당관-2344 ('11.9.29) 하반기 재보궐선거 관련 통신회선 증속 및 정보통신망 운영 협조요청

2. 귀 위원회의 무궁한 발전을 기원합니다.

3. 위 관련 2011. 10.26일 실시한 하반기 재보궐선거 관련 중앙선거관리위원회 홈페이지 접속장애 발생건에 대한 조치내역을 아래와 같이 송부하오니 관련 업무에 참조하시기 바랍니다.

가. 장애내역 : 중앙선거관리위원회 홈페이지 접속장애

나. 발생일시 : 2011. 10.26 05:50 ~ 08:32

다. 발생원인

- ㅇ 중앙선거관리위원회 홈페이지 DDoS공격(1G)으로 접속불가
  - DDoS공격 시간 : 2011. 10.26 05:50 ~ 11:20
- ㅇ 국내 250여개 IP에서 세션 및 대역폭 고갈 복합공격

라. 대응내역

- ㅇ 비정상트래픽 인지 후 공격자 IP차단
- ㅇ KT웹클린존 트래픽 우회 차단 후 홈페이지 정상(회복)
  - KT 웹클린존 우회차단 (08:32)후 웹클린존에서 DDoS공격 차단하며 정상서비스 개시
- ㅇ 중앙선거관리위원회 회선 증설지원 (1G * 1회선, 155M * 2회선절체)

마. 홈페이지 접속불가원인 검토의견

- ㅇ 중앙선거관리위원회 총 대역폭 300M를 초과한 총 1G DDoS트래픽이 발생하여 퍼브넷 AR라우터에 병목현상 발생
- ㅇ AR라우터에서 1G트래픽이 버퍼링되면서 중앙선거관리위원회로 300M 정도의 DDoS 트래픽이 지속적으로 발생되어 홈페이지 접속불가

바. 재발방지 대책(안)

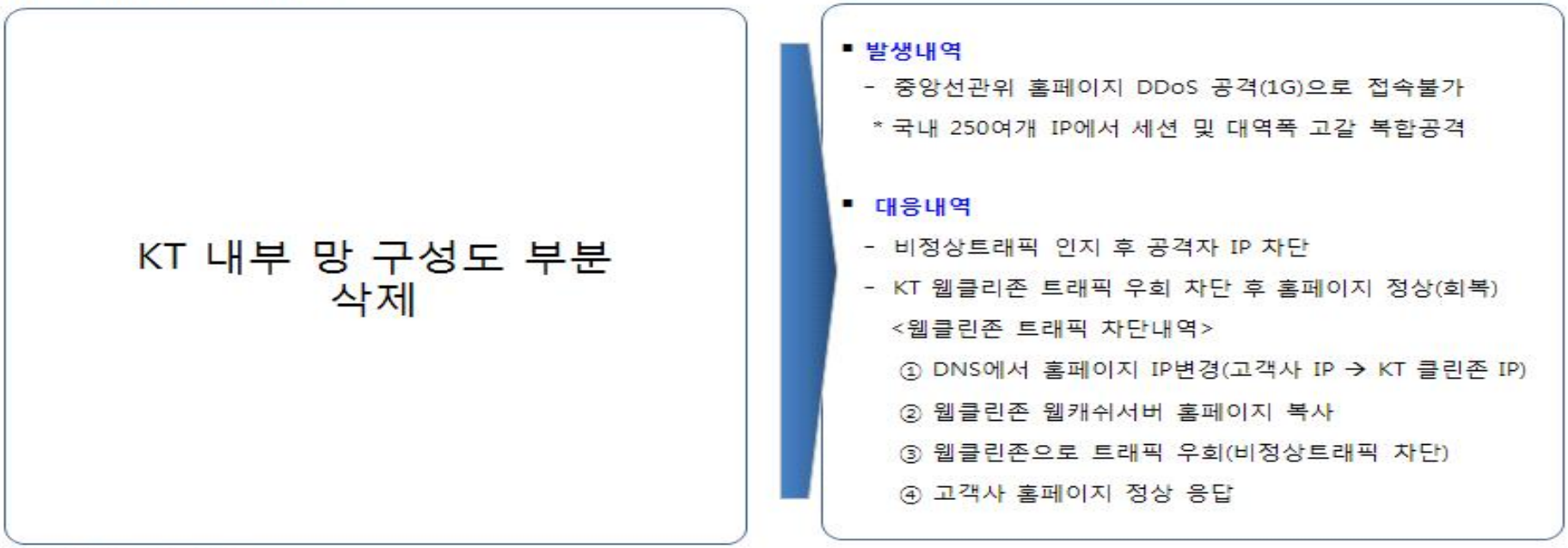
- ㅇ 2012년 총선 및 대선관련 KT 웹클린존 도입검토 필요
- ㅇ 선관위 자체 DDoS 사이버 대응체계 구축 등 필요

붙임 : 1. 중앙선거관리위원회 홈페이지 접속장애 조치내역. 끝.

주식회사케이티 Public고객본부장

중앙선거관리위원회 홈페이지 접속장애 조치내역

□ DDoS 보안침해 공격 개략도



□ 보안침해 조치내역

- 발생일시 : 2011. 10. 26(수) 05:50 ~ 08:32
- 공격방법 : UDP Flooding, Ping Flooding, UDP Tear Drop
- 침해내용 : 250여개 IP 세션에 의한 1G DDoS 공격 발생, 중앙선관위 155M*2 회선 대역폭 고갈 → 중앙선관위 홈페이지 접속 불가
- 조치내역
  - 공격 IP 차단 : 1차(06:30) 등 14 개 IP 차단, 2차(07:15) 등 8 개 IP 차단
  - KT 웹클린존 서비스 수용 조치(08:32) : 중앙선관위 홈페이지 IP 변경) → 홈페이지 접속 정상화

※ 중앙선거관리위원회 회선 증설 지원 : 1 G * 1회선(13:11 155M*2회선 트래픽 절체)